A Trust-Based Adaptive Access Control Model for Wireless Sensor Networks

Htoo Aung Maw

This dissertation is submitted to the University of Hertfordshire in partial fulfilment of the requirements of the degree of Doctor of Philosophy (PhD)

Submitted: April, 2015

I would like to dedicate this thesis to my parents for their endless love, support and encouragement.

Acknowledgements

I would like to show my deepest gratitude and appreciation to my extra supervisory team who were willing to support me throughout my PhD studies. The encouragement and inspiration given to me by my principal supervisor Dr Hannan Xiao is second to none. She was able to identify my weakness early on and gently encourage and support these areas of my personal development. She has always shown a deep interest in my work and was always willing to talk about it. My second supervisor Prof Bruce Christianson has also provided me with exceptional support. He has the ability to make me view ideas from a different perspective which helped the overall development of this work. Last, but by no means least, I would like to thank my third supervisor Mr James A. Malcolm who also took the time to support me. He would instantly have ideas to discuss on regular occasions. I will always appreciate what they have done for me.

I would like to thanks my friends, gym buddies and colleagues in the research institute and school of computer science. I would also like to thank my Aunt's family especially my younger cousin Oliver who made me play games and made me laugh.

Finally, I would like to show my appreciation to my family for their never-ending love and always encourage me to work hard and to value education.

Abstract

Wireless Sensor Networks (WSNs) have recently attracted much interest in the research community because of their wide range of applications. One emerging application for WSNs involves their use in healthcare where they are generally termed Wireless Medical Sensor Networks (WMSNs). In a hospital, fitting patients with tiny, wearable, wireless vital sign sensors would allow doctors, nurses and others to continuously monitor the state of those in their care. In the healthcare industry, patients are expected to be treated in reasonable time and any loss in data availability can result in further decline in the patient's condition or can even lead to death. Therefore, the availability of data is more important than security concerns. The overwhelming priority is to take care of the patient, but the privacy and confidentiality of that patient's medical records cannot be neglected. In current healthcare applications, there are many problems concerning security policy violations such as unauthorised denial of use, unauthorised information modification and unauthorised information release of medical data in the real world environment. Current WSN access control models used the traditional Role-Based Access Control (RBAC) or cryptographic methods for data access control but the systems still need to predefine attributes, roles and policies before deployment. It is, however, difficult to determine in advance all the possible needs for access in real world applications because there may be unanticipated situations at any time.

This research proceeds to study possible approaches to address the above issues and to develop a new access control model to fill the gaps in work done by the WSN research community. Firstly, the adaptive access control model is proposed and developed based on the concept of discretionary overriding to address the data availability issue. In the healthcare industry, there are many problems concerning unauthorised information release. So, we extended the adaptive access control model with a prevention and detection mechanism to detect security policy violations, and added the concept of obligation to take a course of action when a restricted access is granted or denied. However, this approach does not consider privacy of patients' information because data availability is prioritised. To address the

conflict between data availability and data privacy, this research proposed the Trust-based Adaptive Access Control (TBA^2C) model that integrates the concept of trust into the previous model. A simple user behaviour trust model is developed to calculate the behaviour trust value which measures the trustworthiness of the users and that is used as one of the defined thresholds to override access policy for data availability purpose, but the framework of the TBA^2C model can be adapted with other trust models in the research community. The trust model can also protect data privacy because only a user who satisfies the relevant trust threshold can get restricted access in emergency and unanticipated situations. Moreover, the introduction of trust values in the enforcement of authorisation decisions can detect abnormal data access even from authorised users.

Ponder2 is used to develop the TBA^2C model gradually, starting from a simple access control model to the full TBA^2C. In Ponder2, a Self-Managed Cell (SMC) simulates a sensor node with the TBA^2C engine inside it. Additionally, to enable a full comparison with the proposed TBA^2C model, the Break-The-Glass Role Based Access Control (BTG-RBAC) model is redesigned and developed in the same platform (Ponder2). The proposed TBA^2C model is the first to realise a flexible access control engine and to address the conflict between data availability and data privacy by combining the concepts of discretionary overriding, the user behaviour trust model, and the prevention and detection mechanism.

Contents

List of Figures

List of Tables

Nomenclature

Acronyms / Abbreviations

ABE Attribute-Based Encryption

ACL Access Control List

ANSI American National Standards Institute

BAN Body Area Network

BS Base Station

BSN Body Sensor Network

BTG Break-The-Glass

BTG-AC Break-The Glass Access Control

BTG − RBAC Break-the-Glass Role-Based Access Control

CA Certification Authority

CA − RBAC Context-Aware Role-Based Access Control

CBAC Cryptography-Based Access Control

CP − ABE Ciphertext-Policy Attribute-Based Encryption

CSV Comma Separated Value

DAC Discretionary Access Control

DCs Distribution Centres

DFAC Distributed Fine-grained Access Control

DFG – AC Distributed Fine-grained Data Access Control

DH Diffie-Hellmen

DP2AC Distributed Privacy Preserving Access Control

DSA Digital Signature Algorithm

ECC Elliptic Curve Cryptography

EC – CBAC Elliptic Curve Cryptography-Based Access Control

FDAC Fine-grained Distributed Data Access Control

HCPs Healthcare Professionals

HIPAA Health Insurance Portability and Accountability Act

IBS Identity-Based Signature

IBE Identity-Based Encryption

KDC Key Distribution Center

KP – ABE Key-Policy Attribute-Based Encryption

MAC Mandatory Access Control

PDA Personal Digital Assistant

PDP Policy Decision Point

PEP Policy Enforcement Point

PKC Public Key Cryptography

PRICCESS Distributed PRIvacy-preserving aCCESS control

RBAC Role-Base Access Control

RFID Radio-Frequency Identification

RSA Rivest-Shamir-Adleman

SKC Symmetric Key Cryptography

SMC Self-Managed Cell

TBA^2C Trust-Based Adaptive Access Control

$TC-BAC$ Trust and Centrality degree-Based Access Control

TTDDP Two-Tier Data Dissemination Protocol

UPPAC Users' Privacy-Preserving Access Control

WASL WSN Authorisation Specification Language

WMSN Wireless Medical Sensor Network

WSNs Wireless Sensor Networks

XACML eXtensible Access Control Markup language

Chapter 1

Introduction

1.1 Introduction

Wireless Sensor Networks (WSNs) have attracted much interest in the research community because of their wide range of applications. An emerging application for WSNs involves their use in healthcare where they are generally termed as Wireless Medical Sensor Networks (WMSNs). In a hospital, outfitting patients with tiny, wearable, wireless vital sign sensors would allow doctors, nurses and other caregivers to monitor continuously the state of their patients. More importantly in an emergency scenario, the same technology would enable medics to care more effectively for large numbers of casualties. Moreover, unlike many sensor network applications, the healthcare application cannot make use of traditional in-network aggregation[1] [33] since it is not generally meaningful to combine data from multiple patients. In such a scenario, centralised data management cannot be effected.

Security policy violations in multi-user systems were categorised by Anderson [13] into three categories: unauthorised information release, unauthorised information modification and unauthorised denial of use. It is difficult to address the above violations in an access control policy for the healthcare application because an overly "loose" policy might permit access to inappropriate users, but an overly "tight" policy might prevent access from the appropriate users. To solve the problem of defining a flexible policy, we need a flexible approach in the access control engines to address all the possible access conditions.

The aim of this thesis is to present new ways to provide a flexible approach to access

[1] In-network aggregation deals with the distributed processing of data within the network. Data aggregation techniques are tightly coupled with how data is gathered at the sensor nodes.

control engine in WSNs and WMSNs.

The other main issues we study concern the enforcement of access permissions dynamically across healthcare organisations. They are:

- Who is designated to get access in emergency situations?
- What happens after a restricted access[2] is granted or not granted?

Let us consider the following example from a healthcare application to clarify the issues we aim to address in this dissertation. Alice is a doctor who takes care of a patient named Bob. Alice can access Bob's medical record but when she is away from work for some particular reason, such as sickness or on holiday, who has the right to access Bob's medical records in order to evaluate and treat him appropriately? Data availability is important: another doctor may need to access Bob's medical records to evaluate and treat his sickness. The healthcare system can provide data availability without security considerations but when patients are celebrities or high-profile people, how can we control and manage the privacy of these patients? The assumption is made that Bob is a celebrity who is in an emergency situation and Alice is not available at that time. The problem is who else has a designated access to Bob's medical records to give an effective treatment? Can other doctors or nurses from the emergency ward access Bob's medical record? If we consider the sickness of the patient, data availability is needed to give timely treatment, but what about the privacy of patient's medical record and information? In the healthcare industry, the assumption cannot be made that all the users are trustworthy enough to access data even in emergency situations because security breaches can happen at any time due to inappropriate usage. Additionally, a prevention and detection mechanism is needed to detect security policy violations and to take courses of action for any access especially when a restricted access is granted or not granted. The question is, how can we design an access control model to provide privacy, confidentiality and availability at the same time?

In this dissertation, new frameworks are developed to address the access control related issues such as how to provide a flexible approach in an access control engine for both defined and unanticipated situations, how to detect security violations, and how to address the conflict between data availability and data privacy.

[2]A restricted access means a data access request to sensitive or confidential data

1.2 Motivation and Problem Statement

In the healthcare industry, security is the degree of protection against danger, loss, damage and criminal activity. There are many problems concerning unauthorised information release of medical data in the real world environment. Based on the Health Insurance Portability and Accountability Act (HIPAA) enforcement report [140], unauthorised information release is the second highest (35 percent) cause of large security breaches in the healthcare industry. Another six percent is caused by hacking and IT incidents. There were several high-profile breaches of users' privacy and data confidentiality when the California Health Department reported on incidents involving patient medical records at UCLA medical Centre. It found that more than 100 hospital workers had been accessing the medical records of 1,041 patients. Some hospital workers were passing information of hospitalised celebrities to the tabloid media and in some cases to insurance companies.

According to another report [55], 1,754 separate Parkland Hospital employees viewed the medical record of a famous person whilst staying in Parkland Hospital. It is unknown how many of the hospital staff had a legitimate reason to view that patient's record but it would not be more than a few dozen. Wang *et al.* [137] mention that security breaches may be detrimental to patient health or even life threatening. At the same time, there is a need to access all the patient information in order to accurately evaluate patient health and provide better treatment. Normally, healthcare professionals want to meet emergency needs without security concerns; however, security must be addressed and included for a solution to be completed. Aside from the obvious security considerations with sensitive patient data, both data availability and data privacy need to be addressed.

In current healthcare applications [52], there is a lack of security incident responses and reports, and a lack of access control models. Ferreira *et al.* [12] reviewed a decade (2002-2012) of published literature on access control models for the medical industry. There are more than three dozen papers published on access control models for the healthcare industry; however, only a few of the proposed models have been implemented in practice. There are no well-considered threat models for the access control models that reside in both paper and electronic medical record systems for healthcare applications. Wang *et al.* [137] mentioned that, in theory, access control solved the problems of which users can or cannot access medical records. In practice, some large organisations still face problems when policy becomes unmanageable and consequently users circumvent controls.

In the healthcare industry, patients are expected to be treated in reasonable time. Therefore, an access control model should provide real-time access to comprehensive medical records. In emergency situations, a doctor or nurse needs to access data immediately. Any loss in data availability can result in further decline in the patient's condition or can even lead to death. Therefore, the availability of data is more important than security concerns. The overwhelming urgency is to take care of the patient; however, the privacy and confidentiality of that patient's medical records cannot be neglected. Thus, careful consideration in defining flexible policy is required to solve the conflict between data privacy and data availability in this real world application. Additionally, it should also detect unauthorised information release of patient medical records from both authorised and unauthorised users because security breaches can happen at any time.

Based on the above discussion, the question that motivates this research work to be carried out in WSNs and WMSNs is as follows:

How can the current access control framework be improved to provide a flexible approach in access control engine in order to make decisions effectively and help to address the conflict between data availability and data privacy for both defined and unanticipated situations?

To address the above research question, this research work developed new frameworks for access control engines to fill the needs and requirements of WSNs and WMSNs. The first part of the dissertation discusses an adaptive access control model that implements a discretionary overriding concept to address data availability issues in emergency situations. The second part presents an adaptive access control framework with a prevention and detection mechanism to control how security policy violations are handled and detected, and what the courses of action are when a restricted access is granted or denied. The third part of the dissertation integrates these concepts with a simple user behaviour trust model to provide a flexible approach in access control engines as well as to address the conflict between data availability and data privacy. The last part of the dissertation develops an existing access control model called Break-the-Glass Role-Based Access Control (BTG-RBAC) [38] in the same platform to enable a comparison with the proposed models. The evaluation criteria based on characteristics and features to compare with current WSN access control models are also studied.

1.3 Structure of this Dissertation

This section provides an overview of the subsequent chapters of this dissertation.

Chapter 2 gives an overview of the related work laying out the background to this research. This chapter primarily reviews research in the field of WSN access control models. The current ones are specifically categorised into three groups: role-based, cryptography-based and privacy preserving-based.

Chapter 3 gives an overview of the research that is presented in this dissertation. Firstly, the research gaps are identified based on the previous literature review of current WSN access control models, followed by a research question being posed for this dissertation. This chapter also introduces an overview discussion for the development of new frameworks in WSNs.

Chapter 4 discusses a simple access control model in Ponder2, which is a popular policy language to use in WSNs. This model is developed based on an existing authorisation policy in Ponder2 for enforcement of access decisions. Additionally, a medical scenario is developed and implemented to evaluate and validate the simple access control model.

Chapter 5 presents an adaptive access control model that extends the model in the previous chapter with an additional concept to make and adjust decisions regarding data access in WSNs for data availability purposes. To address the data availability issue in WSNs, the discretionary overriding concept is introduced for emergency and unanticipated situations. Development details are presented in this chapter with diagrams and figures. The proposed model is evaluated based on a medical scenario that is implemented and developed in Ponder2.

Chapter 6 adds a prevention and detection mechanism and introduces an obligation policy to the adaptive access control model proposed in the previous chapter. This enhancement addresses how security policy violations can be handled and detected, and what the courses of action are for a restricted access in emergency and unanticipated situations. The development details of this model in Ponder2 are discussed with figures and diagrams, followed by an evaluation of the proposed model with a medical scenario.

Chapter 7 introduces a simple behaviour trust model to define and calculate the total behaviour trust value of the user because we cannot assume that all the users are trustworthy enough to use the overriding facilities (introduced in the previous chapters 5 and 6) at any time. The main objective of developing the trust algorithm is to measure the trustworthiness of users based on information about their behaviour. Additionally, the trust value is considered for using with access control engines to make access decisions effectively and dynamically. Matlab is used to evaluate the proposed trust algorithm to show that how a user's behaviour information such as role, location, time, etc. can affect the calculation of behaviour trust value for each person.

Chapter 8 gives a description of the proposed Trust-Based Adaptive Access Control model (TBA^2C), which is an extended version of the model proposed in chapter 6, incorporating the simple user behaviour trust model from chapter 7. The main objective is to define a flexible access control policy based on behaviour trust values to make access decisions effectively in both defined and unanticipated situations. It also helps to address the conflict between data availability and data privacy in healthcare applications. In addition, the use of the trust value for authorisation decisions can detect an abnormal data access from authorised users by adding an extra condition in the authorisation policy. The development details of this model in Ponder2 are discussed with figures and diagrams, followed by an evaluation of the proposed model with a medical scenario.

Chapter 9 explains the step-by-step development of the Break-The-Glass Role-Based Access Control (BTG-RBAC) model in Ponder2 to enable a meaningful comparison with the proposed TBA^2C when both models are developed and implemented in the same platform. The redesigned BTG-RBAC model for medical data in WSNs is named the Break-The-Glass Access Control ($BTG-AC$) model. The development details of $BTG-AC$ in Ponder2 are discussed with figures and diagrams. Additionally, an evaluation of the $BTG-AC$ model is done based on the medical scenario for WSNs.

Chapter 10 compares Trust-Based Adaptive Access Control (TBA^2C) and Break-The-Glass Access Control ($BTG-AC$). These two models have similar structure but the main differences are that human interactions are still involved in the decision-making process and an additional policy is needed to define BTG operation in the $BTG-AC$ model. Additionally, TBA^2C can help to solve the conflict between data availability and data privacy in some situations. The comparison is made based on the network architecture model, concepts and

approaches, decision outcomes, access control policies, data confidentiality, data privacy and data availability.

Chapter 11 concludes this dissertation and reviews the contributions to the WSN research community. It also discusses some possible modifications based on the proposed concepts that could be applied to TBA^2C and outlines the corresponding future directions of research. Also, further concepts and extensions to apply in TBA^2C that could be beneficial for the research community are considered.

Chapter 2

Literature Review of Current WSN Access Control Models

2.1 Introduction

A Wireless Sensor Network (WSN) consists of hundreds or even thousands of distributed, autonomous, low power, low cost and small-sized devices, each with sensing, processing and communication capabilities to monitor the real world environment and collect information through infrastructureless ad-hoc wireless networks. Sensor networks are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring. From 2008, WSN technologies have been of interest to researchers and scientists in many areas because of their potential to change our way of life, with applications in entertainment, travel, retail, industry, medicine, care of dependent people, emergency management and many other areas.

Nowadays, a sensor node can capture pictures and multimedia data. The sensor node has the capability of sensing data from environments and storing data locally in a distributed fashion or in a centralised approach, transmitting to central storage. Stored data from sensor nodes are vulnerable and should be kept secret. In addition, access to the sensed and stored data needs to be protected through security measures against security policy violations from both authorised and unauthorised users. Data access control is a critical requirement for security-oriented applications such as healthcare and military in WSNs. In this section, security vulnerabilities and security requirements in WSNs are discussed. In addition, the published literature of current access control models for WSNs is reviewed and the state of art survey on these models is discussed.

2.2 Security Vulnerabilities in WSNs

A nature of WSN makes them vulnerable to various kinds of attacks. Vella [130] mentioned that data obtained by sensing nodes need to keep as private and confidential. Without security mechanisms or security primitives, the malicious users could intercept the private information or send false messages to the neighbour nodes in WSNs. Security attacks can be categorised into two; passive and active.

2.2.1 Passive Attack

The listening and monitoring over the communication channels by the unauthorised and the malicious users are named as passive attack. Sensor nodes can sense and collect data from the environments in WSNs; as a result the network becomes vulnerable to potential abuse of these data resources. Since collected data are stored in the sensor nodes without tamper-proof or tamper-evident equipment, the privacy and confidentiality of data become important issues to protect from the passive attacks. The malicious users can gather information by using passive monitoring and listening in anonymous manner. Some of the common passive attacks [120] in WSNs are explained as follows:

- *Eavesdropping and Passive Monitoring*

  One of the most common forms of attack on privacy of data is eavesdropping and passive monitoring. If data messages are not encrypted, the adversary can easily understand their content and obtain information.

- *Traffic Analysis*

  Traffic analysis can be performed to intersect data messages in order to analyse information from the pattern in a communication channel, even if these messages are encrypted with cryptographic keys. The greater the number of data messages has been observed and intercepted by a malicious user, the more he can infer from the traffic. Eavesdropping is more effective when it is combined with traffic analysis.

2.2.2 Active Attack

The monitoring, listening and modifying the data stream or message in the communication channel is known as active attack. In active attack, an adversary can maliciously disturb the communication channels between the sensors nodes. In harmful active attacks, the adversary can alter and spoof the data packets and messages. In addition, it can even interfere

with the wireless signals to jam the network. Ng et al [100] argued that even if the information is protected from eavesdropping by means of encryption, the attacker may blindly modify that encrypted information and turn the information into meaningless information. The following active attacks [135] are most common in WSNs.

- *Camouflage*

  A malicious user may try to compromise a sensor node and then use that masqueraded node as a normal sensor node in WSNs to advertise false routing information. The camouflage node tries to attract other sensor nodes regarding packets forwarding. After data packets start receiving at the camouflaged node, it will forward to other powerful sensor nodes to analyse systematically.

- *Sybil Attack*

  A particular harmful attack against sensor and ad hoc network is known as Sybil attack [99], where a node illegitimately claims to multiple identities. In Sybil attack, a malicious node presents multiple identities and sends incorrect information such as routing information, resource allocation, etc. to neighbour nodes in WSN. This means that a malicious user uses an identity of multiple nodes and routes multiple paths through a single malicious node. The sensor node authentication and encryption scheme can help to prevent that kind of attack in WSN [102].

- *Wormhole Attack*

  Since the sensor nodes use a radio transmission medium to send information, the malicious users can eavesdrop the packets, tunnel them to another location and retransmit them in WSNs [73]. This kind of attack can make false information that the original sender of the packets is in the neighbourhood of the remote location. There are two proposed countermeasures to detect wormhole attack in WSNs called MDS-VOW [135] and Wormhole Attack Defence Mechanism (WODEM) [147].

- *Replay Attack*

  A malicious user might use an old data message and attempt to send it at a later time for data access. When the sensor nodes receive that data message, they believe that it is an original message from the authorised user. Therefore, the malicious user can access to that data resource by using the old message. Freshness can be used in the query and request message to prevent replay attacks in WSN.

- *Hello Flood Attack*

  Hello Flood attack is introduced in WSNs by Karlof and Wagner [63]. In Hello flood attack, an attacker (laptop class user) uses high-power transmitter and advertises Hello message, which contains high quality route to the destination node or base station, to their neighbour nodes. It may cause a large number of sensor nodes to use that faulty routing information because the sensor nodes which receive Hello message, might attempt to transmit via that attacker node. In reality, the attacker nodes are out of the radio range of sensor network and far away from these neighbour nodes but the attackers use high-power transmitter to pretend that they are nearby.

- *Sinkhole Attack*

  A malicious node attempts to attract all the traffic from a particular area to go through it. A malicious node might use incorrect routing tables to attract all the traffic from neighbouring nodes or nodes from specific area. The result is that these nodes are chosen a malicious node as next hop node to route their data packets through. This type of attack makes a selective forwarding message and all the traffic in the sensor network should flow through a single malicious node [120].

- *Daniel of Service Attack*

  In WSNs, the attacks on availability of communication channels and data resources are referred to as Daniel of Service (DoS). WSNs are vulnerable for DoS attack due to resource limited and energy constrained. In DoS attack, an adversary usually attempts to disrupt, corrupt or destroy a network. Wood and Stankovic [141] discussed that DoS attack acts like an event that attempts to reduce a network's capacity, to perform its expected function. In the published literatures, most of the defence mechanisms for DoS attacks need high computational overhead. This means that the defence mechanisms from other wireless technologies are not suitable to apply in resource limited WSNs. There are several common techniques in the published literatures to cope with some of the common DoS attacks but the development of defence mechanism against DoS attack is still an open research issue in WSNs.

- *Node Replication Attack*

  In node replication attack, an attacker tries to add a new sensor node in the existing network in order to do that it replicates and copies node identity of current sensor node [120]. Node replication attack can cause several disruptions in the communication channels by forwarding and corrupting the data packets over incorrect routes. If a

malicious user gains physical access to a sensor node, it is possible for him to copy or replicate and use cryptography keys from that replicated node for message communication. The attacker can also place the replicated node in strategic locations in WSNs. Therefore, he could easily manipulate a specific segment of the sensor network.

Based on the above discussion, a WSN is vulnerable to a considerable number of attacks in all layers of TCP/IP protocol stack. Perrig [104] suggested that there might be other types of attacks that are not yet identified in WSNs. Securing WSNs against all the attacks and threats are the most challenging tasks for the WSN researchers.

2.3 Security Requirements in WSNs

A WSN is considered as highly distributed and ad-hoc manner because of that security requirements and goals should be well studied and provided. An aim of security is to protect the right thing in the right way. Gligor [49] discussed that "A system without an adversary definition cannot be insecure. It can only be astonishing". WSNs are vulnerable to many attacks because of its constraints such as limited resource, low computation capability, broadcast nature of transmission link and unprotected environments. Therefore, a careful consideration is needed for what things need to be protected against what threats, and how these attacks and threats can be detected and prevented. The security goals for WSNs are similar with other network technologies which are explained as below:

- *Confidentiality*: Sensed and collected data need to be stored and kept secretly from the unauthorised users. In WSNs, an issue of confidentiality should address the following requirements.
  - Key distribution should be extremely robust.
  - Public information such as sensor identities and public keys of the sensor nodes should be encrypted to protect against traffic analysis attacks.
- *Integrity*: The data should be genuine. An access control method should provide integrity protection of the user requests and query commands, otherwise a malicious user may try to modify these requests and commands which are constructed by authorised users.
- *Availability*: Whenever an authorised user tries to request data access, data should be always available in the sensor network. Therefore, the services of network should be

always available even if the sensor nodes are attacked by internal or external threats such as Daniel of Service (DoS).

- *Access Control*: Sensed and collected data from a sensor node should be accessible only to the authorise users. Access control should allow access to the authorised users and deny access to the illegitimate users.

- *Authorisation*: Authorisation ensures that only authorised sensors can be involved in order to provide information to the network services. On the other hand, only authorised users can access to data resources in WSNs.

- *Authentication*: Authentication checks the accuracy of message to identify its origin. A verification of user authentication is needed before data access is granted to that user.

- *Freshness*: Freshness ensures that a message is fresh and it prevents that no old messages have been replayed in the network. Sensor nodes may have capabilities of checking freshness in any user request and query command to prevent replay attack from a malicious user.

- *Secure Localisation*: Securing sensor node localisation is another security issue which needs to be considered in WSNs. If the attackers know the location of sensor nodes, a physical attack can be occurred at any time. Therefore, privacy of source location is important to provide in WSNs.

In WSNs, there are two additional requirements which need to be investigated for the security of sensor networks because there may be situations like new sensor nodes are joined or deployed and old sensor nodes are failed to operate in the networks. Based on these requirements, Wang et al [136] suggested that forward and backward secrecy need to be considered in WSNs.

- *Forward Secrecy*: An old sensor node should not be able to read any message after it leaves the sensor network.

- *Backward Secrecy*: A new sensor node should not be able to read any previous message from before it joins the sensor network.

Based on the above discussion, security services are required to provide in WSNs. There are several attacks and threats which try to violate above security services in WSNs. These

Security Properties	Security Threats	Possible Solutions
Confidentiality	Message Disclosure	Encryption, Access Control
Integrity	Message Modification	Digital Signature, Secure Hash Function
Availability	DoS, Wormhole, Sink-hole, Hello Flood	Intrusion Detection, Pair-wise Authentication
Access Control, Authori-sation	Unauthorised and Unau-thenticated Access	Access Control, Key Dis-tribution, Encryption
Authentication	Message Modification, Sybil Attack, Replay and Spoofing Attack	Random Key Distribu-tion, Digital Signature
Freshness	Replay and Spoofing at-tack	Time-stamp, One Way Secure Hash Function
Secure Localization	Node Capture and Note Replication Attack	Temper-proof and Temper-evident Equip-ment
Forward and Backward Secrecy	Message Disclosure	Key Distribution

Table 2.1 WSNs security properties, security attacks and possible solutions[73] ,[9], [103], [108],[100]

kinds of attacks and threats should be protected by using the security defence mechanisms. Table 2.1 lists the security attacks and threats which can violate security services, and the possible solutions to defences against them. The next section will discuss about access control mechanism which is one of the security mechanisms to protect from the unauthorised information release in WSNs.

2.4 Traditional Access Control Model

There are two types of access control model in information systems in use, which are Mandatory Access Control (MAC) [35] and Discretionary Access Control (DAC) [117]. MAC manages access control levels through an administrator in the organisation. It uses a hierarchical approach to control access to the objects, which represent data resource here. The administrator defines an access control policy that cannot be modified by the subjects.

Subjects mean users here. MAC is mostly used in systems where priority is placed on confidentiality, such as in military applications. In the DAC model, an owner of the object controls access to that object. It means that he or she has the power to create the permissions for data access. By default, subjects without permission cannot access the objects.

The concept of an access control matrix which defines the relationships between subjects, objects, and the actions that the subjects want to perform on the objects was introduced by Butler Lampson [67]. The subjects' identities are placed in rows and the objects' identities in columns. Each action, which a subject wants to perform on an object is placed in the intersection of the corresponding row and column. The size of the access control matrix is directly proportional to the number of subjects and objects. Samarati and Vimercati [115] suggest that there are three possible approaches to implement the access control matrix in electronic systems: authorisation table, access control list (ACL) and capabilities. Among these, ACL and capabilities are commonly used in the access control schemes. The three approaches of representing the access control matrix are explained as follows:

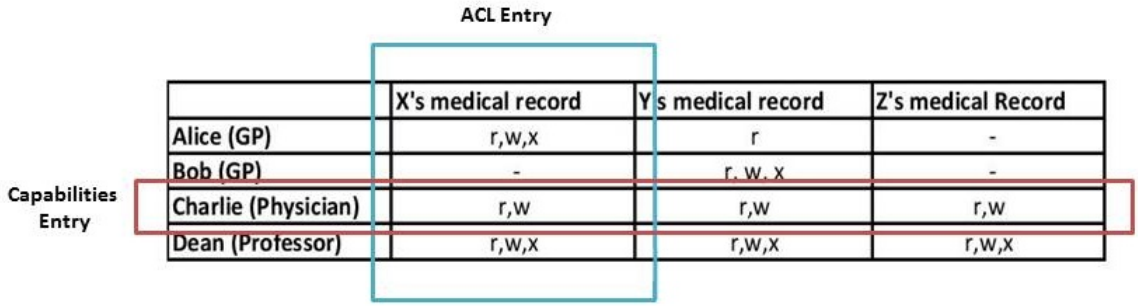


Fig. 2.1 Difference between ACL and Capabilities

- **Authorisation Table**

  An authorisation table is a three columns table: corresponding to subjects, actions and objects. Each tuple in the table corresponds with an authorisation.

- **Access Control List (ACL)**

  Each ACL contains the list of subjects and their access permission to the objects. When a subject tries to access an object, the ACL is used to verify the request from the subject. If the subject is in the ACL list, access will be granted. Otherwise access will be denied. In the ACL approach, the lists of subject and action pair are stored for

each object. The ACL is represented by columns in the access control matrix, as seen in Figure 2.1. In this figure, "r, w and x" stand for read, write and executable.

- **Capabilities**

  Capabilities are different from ACL for each object. Pairs of actions and objects are stored in a capability. In the capabilities approach, the subject can gain access to the object, when he presents his capabilities to the system. The subject's capabilities represents a row in the access control matrix.

The difference between ACL and capabilities can be seen in Figure 2.1. One of the drawbacks of using an access control matrix is when there are a large number of subjects and objects in the system, the administration of those subjects and objects becomes very difficult to handle. The Role-Based Access Control (RBAC) model [152] has been developed to model access control permissions in an organisation in a more manageable way than the access control matrix does. Detailed information of RBAC, and different types of access control models in WSNs, based on their architecture model, strengths and weaknesses will be explained in the next section.

2.5 Access Control Models in WSNs

A considerable number of access control models have been proposed for use in WSNs, though some of them are not yet implemented. In this section, those models are presented before the comparison is made in next section. The proposed access control models are grouped into three main categories based on the nature of their architecture: Role-Based Access Control (RBAC), Cryptography-Based Access Control (CBAC) and Users' Privacy Preserving Access Control (UPPAC).

2.5.1 Role-Based Access Control (RBAC) Model

Most of the access control models in WSNs and WMSNs are based on traditional RBAC, which has been widely accepted as a policy-based access control model. Applications based on RBAC have been implemented and deployed in commercial companies and education industries. The principle of the RBAC model is defined as an intermediary concept relating a group of subjects to a set of access permissions. Any member from the subject group role has all the permissions that are associated with that role. When a new subject is assigned to a group, he receives all the associated access permissions but these permissions are revoked

when the subject leaves the group or is removed from the system. The same procedure is used to add and remove permissions from the roles. When a permission is added to a role, all the members of the associated subject group will receive that permission. The permission will be revoked when it is deleted from the role. This feature helps to simplify system administration when there are many thousands of subjects and objects in an organisation.

In RBAC, the access decision is a choice between two outcomes: permitted access or denied access. The following access control models are proposed based on the RBAC model with different extensions to provide further security properties in WSNs.

- **Zhu's Model** [2009]

  Zhu *et al.* [155] proposed a light weight policy-based access control model, which used authorisation and obligation policies[1] to perform actions and make access decisions at the sensor nodes in a WMSN. The main idea of the proposed approach is to support sensor-level access control policy. A light weight policy system, which is known as Fingers [154], enables policy enforcement and interpretation on the distributed sensors to provide fine-grained access control. Each sensor manages its own policies to implement both Policy Decision Point (PDP) and Policy Enforcement Point (PEP). A PDP interprets policies and makes policy decisions while a PEP enforces the policy by permitting and denying permission for subjects to perform requested actions. A controller (perhaps a PDA) uses Diffie-Hellman (DH) key agreement to share keys with the sensor nodes. The sensor nodes can communicate between each other in a WMSN by using secret keys from the controller. An authentication process is used to prevent malicious nodes and users from joining the network. Only sensor nodes which have keys from the same controller, can communicate with each other. If a user has access to the network controller, he or she can request it to perform some actions at the sensor nodes. As an application, this approach can be used in WMSNs to prevent unauthorised access to actuators, such as insulin or other drug pumps that may harm patients.

- **Context-Aware Role-Based Access Control (CA-RBAC)** [2010]

  Garci-Morchon and Wehrle [43] proposed the Context-Aware Role-Based Access Control (CA-RBAC) model based on a modular context structure for WMSNs. The aim of the model is to provide context awareness and adapt its security properties to

[1] An obligation policy specifies the event, the action and the condition under which the action must be performed.

ensure the users' safety in WMSNs. Wehrle *et al.* [97] points out that the RBAC model is not good enough to use in a WSN because in the traditional RBAC model, the roles and policies must be predefined. In the proposed model, the decision making process is divided into three modular context situations: critical, emergency and normal condition. Based on these situations, access privileges to sensed data will be different. The access control decision will be made based on contextual information such as time and location and access control policies of the three different modules. In a WMSN, sensor nodes are attached to the human body to sense and check medical information for a healthcare service. In normal cases, an authorised doctor needs to verify his or her access control role in order to access the medical data of a patient, but a nurse may not have the same level of privilege. When the system declares a critical or emergency case based on the modular context information, the doctor or nurse can perform any action and can access data even though they may not be able to access data at normal condition. One of the disadvantages of this model is that there is no prevention or detection mechanism as well as no verification process to check user's data access, when the critical situation occurs.

- **Break-the-Glass Role-Based Access Control (BTG-RBAC)** [2011]

  Ferreria *et al.* [38] proposed the Break-the-Glass Role-Based Access Control (BTG-RBAC) model based on the RBAC model. The main idea of this model is to gather necessary information from end users with their collaboration for a usable access control policy that can perform BTG action in emergency situations. The Break-The-Glass (BTG) rule allows users to have emergency and urgent access to the system when a normal authentication does not perform or work properly. Ferreria *et al.* introduced BTG rules in order to override access policy whilst providing non-repudiation mechanisms for its usage. In a real environment, unanticipated situations may occur because it is impossible to predict all access permissions in advance for all situations. BTG extension is used for emergency and important cases whenever a user wants to access data urgently and immediately. When the user tries to perform BTG actions, the system will ask him or her if he or she actually wants to perform that action on a specific object. If the user answers affirmatively, the system will activate the BTG operation and trigger the associated obligations such as alarms and log file. The BTG-RBAC model has made the system much more flexible than normal RBAC but one of the disadvantages is that human processes are needed in order to define additional role and policy regarding BTG actions.

- **Trust and Centrality degree-Based Access Control (TC-BAC)** [2013]

  TC-BAC is proposed by Duan *et al.* [32] to allow access of a trusted node to a network. This model utilises trust to ensure that only legitimate nodes are permitted to join a WSN and then centrality degree[2] to assess continually for risk of access. The concept of centrality degree is used to analyse the relations among the sensor nodes in the network for evaluation of risk. The trust records of other nodes' behaviour are stored in each node for a local trust evaluation along with a centrality degree that represents its importance in the network. In the proposed model, the risk function mainly depends on the node's centrality degree and average trust degree in the network. The main contribution of this model is the introduction of trust and centrality degree attributes into RBAC engine to grant access control.

- **Maerien's Model** [2013]

  Maerien *et al.* [79] proposed an access control infrastructure based on RBAC for multi-party WSNs. In this model, an authorisation proxy acts as both the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP). The proxy retrieves the user's current roles from the small database on sensor nodes to check and verify whether the user's role is sufficient for the access requests. The advantage of this model is that the proxy also monitors the behaviour of the users in the system to detect potential intrusion attempts and keeps a log for sensor node usage caused by the users. There is a lack of flexibility in the proposed infrastructure because the defined roles on sensor nodes only allow for certain evaluation of access rights.

- **Gaurkar's Model** [2013]

  Gaurkar *et al.* [45] proposed an access control model with intrusion detection for security in WSNs. They proposed a new framework for low-level intrusion detection at sensor nodes with access control. The main contribution of the proposed model is that it prevents a malicious node from joining the sensor network. The proposed model extends traditional access control to consider the problem of authorisation not only at the time of access to a resource. The concept of Reference Monitor (RM) is used to enforce data access but there is no detailed information of how the access control is performed in the proposed model.

[2] A node's centrality degree in the network is composed of the rank of the access roles and the number of the node's neighbours.

2.5.2 Cryptography-Based Access Control (CBAC) Model

Cryptography-Based Access Control (CBAC) is another form of access control model for information systems. Ghani *et al.* [48] mentioned that CBAC mechanism is designed for untrusted environments, where lack of global knowledge and control are defining characteristics. It absolutely relies on cryptography to control data access and to ensure data confidentiality and integrity. The main idea is to use a unique key for each data resource. Users who are allowed to access that data resource are assigned the key for data access [7]. Cryptography methods in WSNs should meet the constraints of sensor nodes such as limited power, limited resources and memory shortage. As a result, choosing a suitable cryptography method is important in WSNs. There are two types of cryptographic method: asymmetric encryption, known as Public Key Cryptography (PKC), and symmetric encryption, known as Symmetric Key Cryptography (SKC). PKC based schemes provide better data access security than SKC in the open multi-user environment [144]. The nature of PKC is the use of two keys: one for encryption and one for decryption. In PKC, the data encryption is usually targeted to only one recipient or one group. Any message encrypted by using a public key, can be decrypted only with the corresponding private key.

Many researchers considered that PKC schemes, such as Rivest-Shamir-Adleman (RSA) [111] and DH key agreement scheme [80], were unsuitable for applications in WSNs because of large code size, message and data, long processing time and high power consumption. Sen [120] suggests that public key algorithms are computationally intensive and usually execute many multiplication instructions to perform a single-security operation. Therefore, one-to-one encryption is not efficient to be used in WSNs because the overhead of encryption and size of cipher text are directly proportional to the total number of authorised users. Broadcast encryption [22] is an alternative solution to providing a one-to-many encryption method but it requires the users to present their keys and other information individually. However, recent studies [53], [44], [132] argue that it is feasible to employ PKC in WSNs by using the right selection of algorithms and associated optimisation, parameters, and low power methods.

Many researchers in WSNs are interested in SKC schemes because of its lower computation overhead. SKC uses the same key for both encryption and decryption between two communicating hosts who share the secret key. SKC seems to be suitable for low-end devices such as sensor nodes because of the low overhead [153]. One major issue of using the SKC methods is how to securely distribute the key between communication nodes. It is

a major problem of using SKC because pre-distribution of keys is not always feasible and reliable in WSNs. Key management in WSNs has received much attention from researchers. Key management is an essential mechanism to ensure security in network services and applications when cryptographic schemes are applied in the sensor networks. The main idea is to establish keys between nodes, trusted authorities, and users in a secure and reliable manner. There are three different tasks in key management: key establishment, key revocation, and key update. Key management is a significant challenge in WSNs because the sensor nodes can be deployed in any location and they know nothing about their neighbour nodes before deployment.

Choosing a suitable cryptography method is important in WSNs. In this section, two different types of CBAC models will be explained: Attribute-Based Encryption (ABE) based fine-grained access control and Elliptic Curve Cryptography (ECC) based access control.

Attribute-Based Encryption (ABE) based Fine-Grained Access Control

Sahai and Waters [50] proposed the ABE scheme to model and design a scalable and flexible access control system. ABE is a public key cryptography primitive generalising Identity-based Encryption (IBE) [47] that is associated with user identity in a single user message. In ABE, a group of users is described by the combination of several descriptive attributes and access structures, which is also called an attribute policy. In ABE, the public key encryption is based on one-to-many encryption. There are two different types of ABE, which are proposed by Sahai and Waters [50]: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In KP-ABE, data which is sensed and stored in the sensor node is encrypted with a set of attributes: the user's private key is associated with an access structure that specifies which types of ciphertext the key can decrypt. Only the users that have the right access structure and the key can access and decrypt the sensed data. In CP-ABE, the ciphertext is associated with an access structure. The user's private key is associated with the attributes that specify which type of the ciphertext the key can decrypt. Some ABE-based fine-grained access control models use ECC for key management and distribution.

The ABE [20] method is commonly used in access control models for data encryption and storage in WSNs. Li *et al.* [71] suggests that ABE is a highly promising approach to realise scalability and fine-grained access control, where the flexible access permissions and rights are assigned to each individual user. Fine-grained access control facilitates different kinds of access permissions to a number of users. The sensors may collect information that

belongs to different security levels. Fine-grained access control is a security requirement to protect sensitive information from unauthorised access. One alternative method of providing fine-grained access control in WSNs is using an ABE scheme. Three access control models which use ABE-based encryption to provide fine-grained access control are discussed next.

- **Fine-grained Distributed Data Access Control (FDAC)** [2011]

  Yu *et al.* [144] proposed the Fine-grained Distributed Data Access Control (FDAC) model based on ABE. The main idea of their approach is to provide a distributed data access control which is able to support fine-grained access control over sensor data and is resilient against attacks such as user collusion[3] and node compromise[4]. A network controller which stores access structures, acts as a central distribution centre and distributes keys to users in FDAC. Only users with the right access structure and the right key can access data at the sensor nodes. The access structures will be different for each user depending on the access privileges of users.

  Regarding a battlefield example from the paper, the sensor nodes may be responsible for collecting different types of data such as vibration, smoke, etc in different locations (village, forest). Therefore, attributes such as - location = village; data type = vibration, smoke; owner = explosion experts, officers - are used to specify data access privileges of users. Based on the above example, the access structure of a user is designated as "(location is village) AND (type is vibration)" which allows the user to obtain the vibration data within the village area. More sophisticated access structures can be defined based on the application requirements. If the network controller is compromised by a malicious user, there will be no security provisioning in the system anymore. User revocation can be done by updating the master secret key that is embedded in the user secret key via broadcasting. User revocation may be one of the following: the service subscription is expired, the user changes group intentionally, or the user or group key is compromised. In this approach, CP-ABE based selective broadcast is used for user revocation but there are no details on how to use it.

- **Distributed Fine-grained Access Control (DFAC)** [2011]

  Ruj *et al.* [113] proposed a fully Distributed Fine-grained Access Control (DFAC) scheme using multi-authority ABE [26] to prevent a single point of failure. Instead

[3] Unauthorised users may collude to compromise the encrypted data.

[4] Sensor node could be compromised by a malicious user due to lack of compromise-resistant hardware.

of using one authority as FDAC does, several Distribution Centres (DCs) are used to store and distribute different access structures, sets of attributes and cryptographic keys to users and sensor nodes. All DCs are disjoint from each other. Each DC has its own access subtree, which contains attributes at the leaf nodes of that subtree, for each sensor node. Users who want to access data at the sensor node need to activate their ID with each DC to obtain access structures, access subtrees and keys. All the subtrees from each DC are ANDed together to build a complete access structure for a single user but the user has to store all the access structures in order to access different types of data from the sensor network. This model facilitates modification and secret key distribution when the access rights of a user are changed but the communication overhead of the user's revocation process is higher than with FDAC.

- **Distributed Fine-grained Data Access Control for Distributed Sensor Networks (DFG-AC)** [2011]

  Hur [56] proposed an access control model called Distributed Fine-grained Data Access Control (DFG-AC). It uses both a network controller and a data aggregator for central key management and central storage. The collected data from sensor nodes are transferred to the data aggregator by using a distributed sensor data collection protocol such as Two-Tier Data Dissemination Protocol (TTDDP) [143]. The main idea of using the data aggregator as central storage is to allow more complex data encryption. Additionally, the users can obtain all the information by accessing the data aggregator. The data aggregator is more powerful than the sensor nodes and it can use complex encryption methods. The advantage of the proposed model is that it considers the stateless receiver problem[5]. To solve this problem, key revocation is done with a stateless group key distribution mechanism using a binary tree. One of the disadvantages is that transmitting data from sensor nodes to data aggregator consumes considerable battery power and energy. In addition, there might be a single point of failure because of the centralised data storage. This model provides user revocation by using a KP-ABE scheme with the attributes for distributed WSNs.

Elliptic Curve Cryptography-Based Access Control (EC-CBAC)

Elliptic Curve Cryptography-Based Access Control (EC-CBAC) models [133], [153], [8] use ECC to authorise and grant users access to data. They prevent malicious nodes from

[5]Practically, users may miss a key update message. Therefore, they cannot keep their key states up-to-date. This problem is known as the stateless receiver problem.

joining the sensor network. ECC has became popular as the solution for WSN due to low computational overhead and small key size. The similarity of the proposed models is simply that they use ECC-based encryption.

- **Wang, Sheng and Li Model** [2006]

  Wang *et al.* [133] proposed an access control model based on ECC. The main objective of the proposed model is to use an ECC scheme for granting user access rights to the collected data. Different users may have different levels of data access due to restrictions of access implied by the data confidentiality and privacy. ECC is used in key distribution and sharing information between the users and in a Key Distribution Centre (KDC). In this approach, the KDC is responsible for generating all security primitives such as random numbers, access lists and hash functions, and maintains a user list with associated user identifications. The users have to request access permission from the KDC. Access lists, which comprise user identity, group identity and user privilege mask, define the user's access privileges. The user access privilege mask consists of a number of bits and each bit represents a specific information or service. Therefore, users who possess the same mask and access privileges are put in the same group.

- **Zhou, Zhang and Fang Model** [2007]

  Zhou *et al.* [153] proposed an access control protocol based on ECC to accomplish node authentication and key establishment for new nodes whenever they join a sensor network. The proposed access control model uses node identity and node bootstrapping time for the node authentication procedure. They introduced node bootstrapping time into authentication procedures to differentiate malicious nodes from legitimate new nodes. In this model, the authors are mostly looking at node deployment to prevent malicious nodes from joining the network. A Certification Authority (CA) is used to generate a certificate, which includes ID information and bootstrapping time, to authenticate the identity of a new node. Also the node certificate is signed with the CA's private key. Because of this, adversaries cannot alter ID and bootstrapping time. When a new node is deployed in a WSN, it shows its certificate to the neighbour nodes in order to verify its identity via the CA's public key. This access control protocol enforces to control sensor node deployment and prevents malicious nodes from joining sensor networks.

- **Al-Mahmud and Morogan Model** [2012]

  Al-Mahmud and Morogan [8] proposed an identity-based authentication and access control model in WSNs. The main idea of the proposed model is to use Identity-Based Signature (IBS) [122] for providing both user authentication and data access control in WSNs. This protocol is based on an IBS scheme where ECC-based Digital Signature Algorithm (DSA) [61] is used to sign and verify a message. A Base Station (BS) is responsible for generating the private keys of both users and sensor nodes in the network. For the key distribution, a one-pass key establishment protocol [138] is used to share session keys between sensor nodes and users. Users are required to register with the BS. Based on the access request from the users, the BS generates a private key and access structure for each user. The sensor nodes are preloaded with the hash value of user identities and the private key, which will be used for the authentication process. After the authentication process, the sensor node will check whether the user is authorised to access the data.

- **Chatterjee, Das and Sing Model** [2013]

  Chatterjee *et al.* [27] proposed a user access control scheme for Wireless Body Area Network (WBAN). This schemes is used an ECC based crypto system to ensure that a particular legitimate user can only access the information for which he/she is authorised. This model uses an access list composed of a user identity, a user access privilege mask and a group identity for each user regarding data access. A user access privilege mask is a binary number where each bit represents specific information or services that can be accessed by an authorised user. The group identity represents a unique number to identify a particular access group. This model is similar to Wang, Sheng and Li Model [133]. The main difference is that ECC based crypto system is used in this proposed model.

2.5.3 Users' Privacy-Preserving Access Control (UPPAC) Model

Most of the access control models in WSNs are to provide data privacy and data confidentiality. Privacy of users and sensor nodes in WSNs is different from data privacy and has received less attention in the literature. In user privacy, users aim to hide their ID and other information. Therefore, no one in the network knows the real ID of a user except the network authority and the user himself. Recently, there are two schemes proposed for the privacy-preservation of users' information in WSNs: Distributed Privacy Preserving Access

Control (DP2AC) [150] and Distributed PRIvacy-preserving aCCESS control (PRICCESS) [54]. The PRICCESS model is related to the RBAC model. The main reason the PRICCESS model is presented under UPPAC is that it provides user privacy preserving distributed access control in WSNs.

- **Distributed Privacy Preserving Access Control (DP2AC)** [2009]

  Zhang *et al.* [150] proposed a Distributed Privacy Preserving Access Control (DP2AC) scheme. The owner of the sensor network generates the token by using a blind signature [107]. Users need to buy tokens from the network owner before entering the sensor network. The tokens can be verified by any sensor node in the network but no one can tell the identity of the token holder including the network owner. There is no relationship between user identities and tokens, so privacy preservation for users is achieved. Once the token is validated by a sensor node, it provides the user with a certain amount of requested data which is equivalent to the denomination of the token. The main objective of the proposed DP2AC model is that the network owner can prevent unauthorised access to sensed data, while users can protect their data access privacy.

  However, a recent study [72] points out that DP2AC is not a fine-grained access control because each anonymous user has the same access privileges. Furthermore, the network user cannot sign a query command because of the blind signature. As a result, an adversary can easily intercept tokens and impersonate authorised users to access data at the sensor nodes. A disadvantage of using tokens in a WSN is that the sensor nodes need more storage for the token detection mechanism. Additionally, all the used tokens have to be recorded and stored in the sensor nodes to prevent the tokens being reused by malicious and unauthorised users.

- **Distributed PRIvacy-preserving aCCESS control (PRICCESS)** [2011]

  He *et al.* [54] proposed the PRICCESS protocol for WSNs. The main contribution to the research community of this protocol is that it provides user privacy preserving distributed access control in a single-owner multi-user sensor network. A ring signature [18] is used to protect the anonymity of users by using a group ID and a group signature. Each group of users has different access privileges, ID, and key for signature. Users have to activate their information with a network controller to receive group ID and keys for data access. Users with the same access privileges are likely to be put in the same group by the network controller. The PRICCESS model uses an ACL

approach to store the access list of the group for data access control in the network controller. Any user from the group can use a group key when he or she signs the message for a data access request. The network controller verifies that the message has been signed by one of the group members without knowing who the actual signer is. Therefore, the use of ring signature can preserve the user's privacy and at the same time the network controller is satisfied that the singer is an authorised user.

2.6 Comparison of WSN Access Control Models

To make meaningful comparisons of the current access control models in WSNs, the evaluation framework is defined to compare and contrast current access control models by using the following features and characteristics [48], [90], [114], [85].

1. *Support Data Privacy*

   The need for data privacy is growing among all the real world applications in WSNs. Data privacy becomes more and more important in WSNs, when data are to be released to only authorised and legitimate users. The more data being disclosed, the more the owner of that data loses his own privacy.

2. *Support User Privacy*

   The need for user privacy is important in some applications. Sometimes a user, who tries to access data from the network, does not want to share his detailed information with other users in the network. It means that the users' privacy preservation is needed to protect the privacy of user information in the network.

3. *Flexibility*

   No matter how perfect an access control system is, if it does not support accommodation to changes, such as insertion and deletion of new application systems, the access control model is not feasible to use in the real world. In WSNs, the user characteristics and the access context are changing continuously. Therefore, the access control decisions must be synchronised with continuously changing security conditions. It is desirable for the access control model to handle the dynamism of users and environments. Therefore, the access control model needs to be flexible enough to support changes and synchronise with the access control decisions.

Access Control Models	Support Data Privacy	Support User Privacy	Flexibility	Support For Emergency Access	Context Sensitivity	Granularity
Zhu's Model [155]	Yes	No	No	No	No	Coarse-Grained
CA-RBAC [43]	Yes	No	Yes	Yes	Yes	Fine-Grained
TC-BAC [32]	Yes	No	Yes	No	No	Coarse-Grained
Maerien's Model [79]	Yes	No	No	No	No	Coarse-Grained
Gaurkar's Model [45]	Yes	No	No	No	No	Coarse-Grained
$BTG-AC$ [84]	Yes	No	Yes	Yes	No	Coarse-Grained
FDAC [144]	Yes	No	Yes	No	Yes	Fine-Grained
DFAC [113]	Yes	No	Yes	No	Yes	Fine-Grained
DFG-AC [56]	Yes	No	No	No	Yes	Fine-Grained
Wang, Sheng and Li Model [133]	Yes	No	No	No	No	Coarse-Grained
Zhou, Zhang and Fang Model [153]	Yes	No	No	No	No	Coarse-Grained
Al-Mahmud and Morogan Model [8]	Yes	No	No	No	No	Coarse-Grained
Chatterjee, Das and Sing Model [27]	Yes	No	No	No	No	Fine-Grained
DP2AC [150]	Yes	Yes	No	No	No	Coarse-Grained
PRICCESS [54]	Yes	Yes	No	No	No	Coarse-Grained
TBA^2C	Yes	Yes	Yes	Yes	Yes	Fine-Grained

Table 2.2 Comparison of Access Control Models based on Features in WSNs

4. *Support Emergency Data Access*

An ideal access control model needs to support data access not only in normal situations but also in an emergency situation. Many applications will benefit from such

provision.

5. *Context Sensitivity*

   An access control model is context sensitive when context information plays a role in making the appropriate access decision. It means that the contextual information (such as location and time) is used in defining policies for making access control decision dynamically.

6. *Granularity*

   There are two different types of granularity in access control, which are fine-grained and coarse-grained. Fine-grained means that the access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users [51]. Coarse-grained means that groups of users and collections of objects often share the same access control requirements. The access control system should then offer support for authorisation specific to the groups of users, objects and possibly actions.

These six supporting features listed above are used to evaluate the current access control models in WSNs. Table 2.2 shows a comparison of current access control models based on these features and characteristics. The first row of the table describes evaluation criteria and the first column lists access control models. Each cell in the table shows whether the model of that row has the feature of that column.

All the access control models in WSNs provide data confidentiality and data privacy in normal condition but users' privacy preservation is only supported in DP2AC and PRICCESS. The access control models which use ABE and contextual information to make access decisions, provide flexibility in the system. Based on Table 2.2, all the access control models in WSNs support authorisation decisions and allow for changes like roles, users, policy, etc. Among them, CA-RBAC and $BTG-AC$ support emergency and immediate data access. There are few access control models that make authorisation decisions based on context information. Approximately equal numbers of access control models support coarse-grained and fine-grained. As a summary, the authorisation policy for each scheme is different, that means all models are proposed to solve different problems and look from different point of view to address the issues in WSNs area. As a summary, the authorisation policy for each scheme is different, that means all models are proposed to solve different

problems and look from different point of view to address the issues in WSNs area.

Regarding Table 2.1, the role-based access control models in WSNs are aimed to protect a message disclosure and an unauthorised information release. Cryptography-base access control models are not only to protect a message disclosure and unauthorised information release but also to provide data confidentiality and data integrity by using different cryptographic methods. For the proposed Trust-Based Adaptive Access Control (TBA^2C), we only consider a message disclosure and unauthorised information but additionally, we address the conflict between data availability and data privacy in WSNs.

The proposed TBA^2C model introduces a user behaviour trust model with an adaptive access control engine to address the conflict between data availability and data privacy. In the adaptive access control engine, an overriding policy is introduced to override an access permission with role, contextual information and behaviour trust value when the system needs for emergency and unexpected situation. Unlike other WSN access control models, the proposed TBA^2C is considered to address the conflict between data availability and data privacy that is an essential issue to be provided in any application or system. Therefore, the proposed TBA^2C is only access control model that considers and addresses the conflict between data availability and data privacy in WSNs. The step-by-step development of a TBA^2C model will explain in later chapters.

2.7 Conclusion

Overall, this section has categorised and briefly discussed a range of WSN access control models. A more comprehensive comparison between current WSN access control models can be seen in a work of Maw *et al.* [85]. The details of WSN applications, access control roles and policies for Healthcare Professionals (HCPs), and deployment tools such as simulators and emulators are explained in Appendix B of this dissertation. Based on the above discussion, it becomes clear that access control has been neglected by the WSN research community. There are potential research issues that need to be addressed regarding data access control in WSNs. None of the current WSN access control models addresses the conflict between data availability and data privacy. In the next chapter, the research gaps are identified based on the state-of-art survey of WSN access control models in this chapter. This is followed by a brief discussion of the proposed frameworks to address these gaps.

Chapter 3

An Overview of the Research Problem

3.1 Introduction

Most of the current WSN access control models are based on a traditional Role-Based Access Control (RBAC) [152] model to control data access based on roles. The decision is binary: deny or permit access. The RBAC model has been widely accepted as a policy-based access control model and it is suitable for most commercial applications but roles and policies need to be predefined before the system can make decisions. Some WSN access control models used cryptographic methods for data storage and data access control but the systems still need to predefine attributes, roles and policies before deployment. It is, however, difficult to determine in advance all the possible needs for access in real world applications because there may be unanticipated situations at any time.

Many potential situations cannot be predefined in traditional RBAC or cryptography-based systems. For example, the roles and policies for emergency and unexpected situations cannot be defined in advance. When the system faces these kinds of situations, what will the system do? Does the system wait until the authorised user comes and logs in? Alternatively, in the medical scenario, does a nurse wait for a doctor who takes care of a patient, in order to retrieve that patient's medical record? In most of the emergency and unanticipated situations, the users cannot wait until someone else comes in order to retrieve the necessary data. Given this, what are the possible methods to provide a flexible approach in the access control engine? For real world applications, the system needs to be flexible enough to make decisions regarding data access based on unusual situations in addition to normally defined situations. Using the RBAC model often cannot fulfil the requirements of real world applications in WSNs. Therefore, a new access control model is needed for WSNs that will

provide a flexible policy to make access decisions dynamically in both defined and unanticipated situations.

The structure of this chapter is as follows: Firstly, the identified research gaps are presented followed by a statement of the research question that is addressed in this dissertation. Finally, the step-by-step development of the research is briefly discussed.

3.2 Research Gaps

Based on the survey and analysis of WSN access control models from the previous chapter, the following research gaps are identified.

- **Lack of Flexibility**

  Current WSN access control models use predefined policies and roles to make access decisions on user requests. However, it is impossible to predict in advance all the possible policies and roles that may be needed for unexpected and unanticipated events. Some access control models proposed for sensor nodes to perform some actions but there is a lack of capability to make decisions regarding data access locally at the sensor nodes for emergency and unexpected situations. Current WSN access control models need much more flexibility to make access decisions on unanticipated events. In the WSN content, flexibility is important in an access control engine to make decisions on user requests quickly and efficiently, when unanticipated situations occur. Therefore, a flexible access control model is important and desirable in terms of providing efficient, accountable and immediate data access for emergency and unanticipated situations.

- **Conflict between Data Availability and Data Privacy**

  Current WSN access control models suffer from a conflict between data availability and data privacy, especially in emergencies. There is a lack of data availability when data privacy is the first priority. Conversely, data privacy is easily breached when data availability is the first consideration. There are two WSN access control models that consider decision-making processes in emergency situations. The Context-Aware Role-Based Access Control (CA-RBAC) model [43] was proposed to provide an effective access control decision when the users need to access data in emergency situations. The CA-RBAC model tried to reduce communication time for emergencies.

In it, the encryption, decryption, and verification of the digital certificates are not involved in emergency situations. In CA-RBAC, it is assumed that immediate patient welfare is more important than privacy and confidentiality of patient information and medical records in emergency situations. There might be some cases, however where privacy is of primary importance. For example, a user does not want to give access to his or her medical record to other doctors and nurses apart from his or her personal or private doctor and nurse. Generally, privacy and confidentiality of data still needs to be maintained even in emergency situations.

Ferreira introduced the Break-The-Glass Role-Based Access Control (BTG-RBAC) [38] model to make access decisions for emergency situations based on the BTG role; however, there is no provision to defect security policy violations. This means that both CA-RBAC and BTG-RBAC are considered to provide data availability when the users need data access for emergency situations but there is no prevention or detection mechanism and no verification process to check the user's data access such as identification, contextual information, etc. Therefore, data privacy and confidentiality of patients' information and medical record can be circumvented easily. This conflict between data availability and data privacy is a central issue to address, whenever a new access control model and security mechanism is proposed and developed for security-oriented applications such as medical and military. The question is how an access control model and security mechanism can provide both data availability and data privacy at the same time.

- **Prevention and Detection Mechanism**

  One of the proposed access control models [43] in Wireless Medical Sensor Networks (WMSNs) used RBAC with modular context information for medical applications. In that approach, when a patient is in emergency or critical situations, anyone in the system can access the patient's medical record without involving any authentication process. From a user's aspect, the system needs to provide some kind of prevention and detection mechanism to protect the privacy of patient information and confidentiality of medical records even in emergency situations. As well, current WSN access control models do not check any recorded or log files to see who has tried to access sensed and collected data with or without authorised access and when or where this situation has happened. Auditing of data usage and data access have been neglected by researchers in WSNs. Therefore, a prevention and detection mechanism to keep

records of access requests needs to be introduced for auditing purposes in WSNs.

- **User Behaviour Monitoring and Trust**

  In current WSN access control models, users with access privileges can access data at any time. The assumption that all users are trustworthy to access needed data at any time, however, is unsupported by experience. It is impossible to predict a user's intention for accessing data at a particular time. For example, in a medical scenario, a doctor can be a researcher at an organisation. He or she may try to access his or her patient's data at different times and locations for research purposes or his or her benefit. Normally, WSN access control models will allow doctors to access data because of their access right and privilege. However, when doctors misuse patient data for their own benefit, how can those situations be detected? How can such situations be prevented?

  One method of preventing this kind of situation is to apply a user behaviour-monitoring model to check user actions, location, time, etc., whenever a user attempts to access data. In addition, trust management can be applied with the users' behaviour-monitoring model to provide a flexible approach and to monitor the user behaviour patterns. Therefore, the user behaviour trust model can be another important research aspect in WSNs. Using a behaviour trust value in decision-making processes regarding data access is new in WSNs and other wireless technologies and will be a challenge.

- **User Privacy and Sensor Node Privacy**

  Among current WSN access control models, few address user privacy and sensor node privacy. There is no access control model that provides both user privacy and data confidentiality in WSNs. The privacy of users is important to provide in WSNs because of their broadcast and distributed nature. In some cases, users may want to hide their identity and information because they do not want to share it with other users in the network. Some privacy-preserving access control models such as Distributed Privacy Preserving Access Control (DP2AC) [150] and distributed PRIvacy-preserving aCCESS control (PRICCESS) [54] used blind or ring signatures to provide privacy of user ID and information. DP2AC provides privacy preserving for users but there might be problems in a WSN storing all used tokens for the token detection mechanism because of limited resources and storage.

The location privacy of a sensor node is another research issue in WSNs because sensor nodes are deployed in a great variety of locations with neither tamper-evident nor tamper-proof equipment. If a malicious user can capture the location of sensor nodes, he or she can physically attack those nodes. Consequently, all possible problems and solutions for user and sensor node privacy need to be considered when being designed for WSNs.

The discussion reveals that there is much research work needed in WSNs especially on access control related issues. Most of the current WSN access control models are focused on the authentication process, neglecting authorisation and policy management. Therefore, we focus on how a flexible approach can be provided in access control engines to handle both defined and unanticipated situations based on policy management. In this dissertation, we address all the above research gaps except for sensor node privacy. A possible solution to provide sensor node privacy in WSNs is using Attribute-Based Encryption (ABE).

3.3 Research Question

A research question that motivates us to carry out this research work is:

How can the current framework be improved to provide a flexible approach in the access control engine to make decisions effectively and help to address the conflict between data availability and data privacy for both defined and unanticipated situations?

3.4 Research Agenda

To address the above research question, this dissertation is divided into four parts to show the step-by-step development of our proposed new access control framework and how it is improved in each part. These four parts of the dissertation are briefly explained here.

The first part of the dissertation (Chapter 5) is focused on the following questions:

- How can data availability be provided in emergency and unanticipated situations?
- How can the concept of discretionary overriding be used to improve the decision-making process in an access control engine?

To address the data availability issue, a discretionary overriding concept [110] is introduced for WSNs. Many applications in WSNs are designed for medical or military scenarios where emergency and unanticipated situations can occur at any time. The question is, how can access decisions be made efficiently and immediately when an access control engine at the sensor node faces unanticipated events. The discretionary overriding process can make access control engine much more flexible than normal access control models because it may have the capability to override decisions regarding data access in emergency and unanticipated situations. Therefore, we shall investigate the extent to which the introduction of the discretionary overriding concept in WSNs can achieve the flexibility of access control engine providing data availability issue in emergency and unanticipated situations.

Following on from the work on the above-mentioned questions, the second part of the dissertation (Chapter 6) addresses the following questions:

- How can security policy violations be detected and handled?
- What are the courses of action for restricted access in emergency and unanticipated situations?

To address the above questions, the prevention and detection mechanism and the obligation policy are applied and extended in the access control framework in chapter 5. Firozabadi *et al.* [41] mentioned that a preventative control mechanism prevents a user from violating the policies, whereas a detective control mechanism does not guarantee that violations are prevented, but will ensure that a violation is detected in a reasonable time. In this model, the prevention and detection mechanism is applied to keep a track record of the user's requested information in an audit log to detect security policy violations but an administration process needs to be involved for checking the log. Alongside with the prevention and detection mechanism, the obligation policy [39] is introduced to deal with what are the courses of action when a restricted access is granted or denied.

The third part of the dissertation (Chapters 7 and 8) investigates potential ways to improve the previous access control frameworks by studying the following questions.

- How can a flexible policy be defined that is not too permissive or too strict, to make access decisions effectively and efficiently?
- How can access control model be improved in decision-making processes regarding data access by using a behaviour trust value?

- What kind of algorithm should be used to calculate and evaluate user behaviour trust value?
- To what extent can this approach be used to address the conflict between data availability and data privacy in WSNs be addressed?

To address the above questions, a simple user behaviour trust model based on weighted-running average [14] and geometric mean [88] is applied in the proposed access control framework to make and adjust access decisions dynamically. The main issue we study is that there is no way to predefine all the access policies regarding data access in the real world application for unanticipated and emergency situations. The introduction of a user behaviour trust model can make an access control engine much more flexible as it can monitor the user behaviour patterns to detect security policy violations from both authorised and unauthorised users. Additionally, the behaviour trust value is used as one of the defined thresholds to override access policy for data availability purpose and it can protect data privacy because only the user who satisfies these thresholds including trust value, can get a restricted access in emergency and unanticipated situations. Therefore, the proposed Trust-based Adaptive Access Control (TBA^2C) model integrates the concepts that have been introduced so far with a simple user behaviour trust model to provide a flexible approach in access control engines and help to address the conflict between data availability and data privacy.

The final part of the dissertation (Chapters 9 and 10) develops in Ponder2 the Break-The-Glass Access Control ($BTG-AC$) framework that was originally proposed by Ferreira [38], but a few modifications have been made to better fit in WSNs. This model has similar structure to the TBA^2C framework. This part of the dissertation compares the TBA^2C and $BTG-AC$ models based on evaluation criteria and results from the healthcare application. The main advantage of the proposed TBA^2C over $BTG-AC$ is that no human effort is needed to override policy for emergency and unanticipated situations. Additionally, the conflict between data availability and data privacy can be solved in some situations unless the trusted users become untrustworthy in the system.

3.5 Conclusion

In this chapter, an overview of the research problems is given and the research question that motivates this research work is set out. The step-by-step development of the proposed

framework is briefly summarised; however, detailed information will be explained in later chapters. In the next chapter, a simple access control model for WSNs based on the existing features of Ponder2 is presented with its development details.

Chapter 4

A Simple Access Control Model

4.1 Introduction

Access control is one of the essential requirements in Wireless Sensor Networks (WSNs). To develop a lightweight access control model for WSNs, careful consideration of suitable development tools is essential. In this chapter, a simple framework based on the National Institute of Standards and Technology (NIST) [116] standard access control model with an existing authorisation policy in the Ponder2 [29] is developed and explained to act as a starting point before we address the research issues for WSNs in later chapters. In this way, the reader can clearly see the step-by-step improvement of the access control model from the beginning until all of the research issues have been addressed by the end of this dissertation.

Firstly, the Ponder2 policy language is briefly discussed, then detailed information of the simple access control model in Ponder2 is presented with figures and diagrams. In addition, a healthcare application is developed in Ponder2 to evaluate and verify the proposed model. Finally, this chapter concludes with suggestions to address the data availability issue in WSNs as the next stage of development.

4.2 Ponder2

There are a variety of development tools for WSNs available in the current WSN research community. Two policy languages, Ponder2 [29] and WSN Authorisation Specification Language (WASL) [82], are designed specifically for resource and memory limited devices like sensor nodes. Ponder2 is a popular policy language to use in Body Sensor Networks

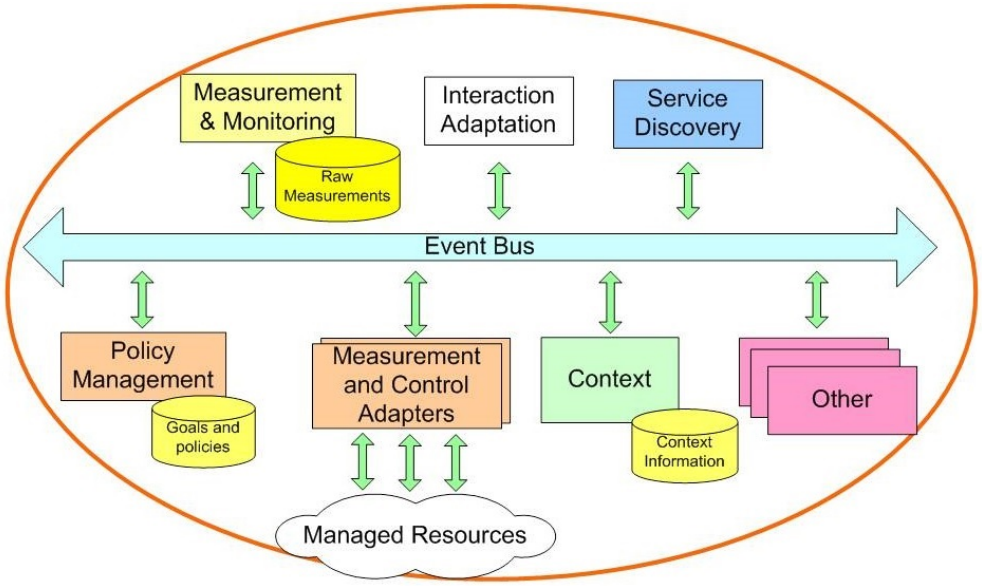


Fig. 4.1 The SMC Architecture Pattern

(BSNs) and much published literature on WSNs is based on Ponder2. It comprises a self-contained, stand-alone, general-purpose object management system with message passing between objects, incorporates an awareness of events and policies, and implements a policy execution framework.

Ponder2 has a high-level configuration and control language called PonderTalk and user-extensible managed objects that are programmed in Java. Ponder2 is implemented as Self-Managed Cell (SMC) [78], which is a set of hardware and software components forming an administrative domain. Figure 4.1 illustrates the architecture pattern of a SMC that manages a set of heterogenous components (i.e., managed resources) such as those in BSN, WSN or even a large-scale distributed application. Resource adapters are instantiated to provide a unified view for interaction with the resources as they may use different interfaces or communication protocols.

A SMC can load other components and services for detecting context changes, monitoring component behaviours or for security (authentication and access control). However, the event bus, the policy service, and the discovery service work in conjunction with each other and form the core functionality of a SMC that must always be present. As most pervasive system are event-driven, the services of a SMC interact using a common subscribe event bus, although we do not constrain all communication to be event-based. The event bus can

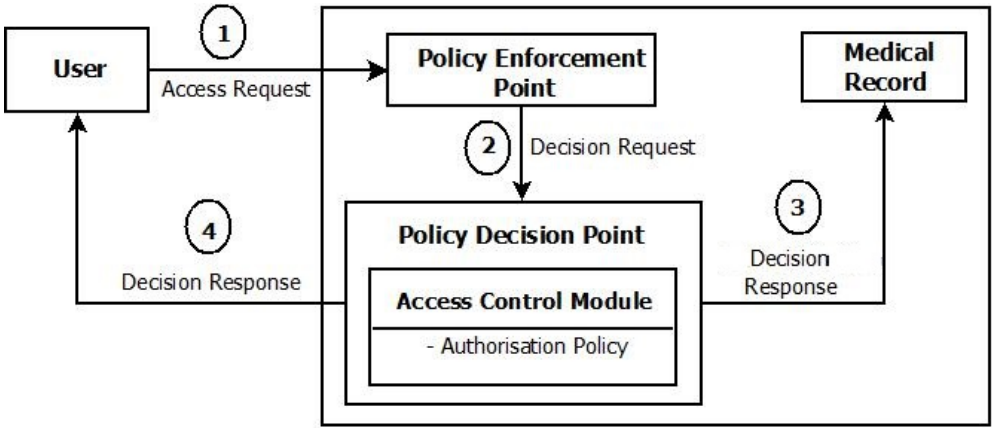


Fig. 4.2 A Simple Access Control Model

be used for both management and application data such as alarms indicating that threshold have been exceeded. The discovery service is used to discover new components which are capable of becoming members of the SMC, e.g., other SMCs in the vicinity. The discovery service also manages the SMC's membership as it is necessary to cater for transient failures, which are common in wireless communications and to detect permanent departure (e.g., device out of range, switched off, or failure).

The policy service implements a local feedback control loop to achieve adaption and self-management. It caters different types of policies which specify what actions are permitted on which resources and services. The policy management is a main element that we modify and add extra function to develop a new access control model for BSN and WSNs. Therefore, Ponder2 is capable of self management. Everything in Ponder2 is a managed object loaded dynamically into the SMC from a library, thereby producing the factory managed object (Java class). The proposed model is implemented in the Ponder2 policy language, which is suitable to use in small devices such as sensor node.

4.3 Development Framework

Figure 4.2 shows the high-level design of the proposed simple access control model based on the NIST standard access control framework in Ponder2. Brief discussion of Policy Enforcement Point (PEP) and Policy Decision Point (PDP) with its components is presented here.

4.3.1 Policy Enforcement Point (PEP)

PEP provides an authentication service between users and sensor nodes. Whenever PEP receives an access request, it authenticates the user by checking the user information such as user identity and cryptographic key before it forwards the decision request to the PDP. The assumption is made that Attribute-Based Encryption (ABE) based authentication service and key distribution are already provided in the PEP of the proposed model.

4.3.2 Policy Decision Point (PDP)

PDP is a main module in the proposed model inside which the access control module is implemented, and makes access decisions based on the existing authorisation policy in Ponder2. The PDP uses information such as users' role, action and context along with authorisation policy for the decision-making process. After the access control module has made decisions regarding data access, PDP sends back a response message to the user and forwards the decision internally to the targeted object.

Access Control Module

As shown in Figure 4.2, the access control module makes an access decision on a user request based on authorisation policies that are predefined in that module.

- Authorisation Policy

  An authorisation policy is used to force the access control module to check whether a subject is authorised to execute an action on a target. Based on the existing authorisation policy in Ponder2, subject, target, condition and action are used to define the data access. Subject means a user who is trying to access data from the target that stores information. Whenever the access control module receives a decision request, it checks the department that the user is from, which is defined in the condition of the policy. If the decision request meets the condition, the subject is allowed to perform the action at the target. The authorisation policy can be changed based on the requirements of the application. There may be several authorisation policies based on the users' access privileges. An example authorisation policy in Ponder2 is shown below:

  Def: Permit-Policy
  subject nurse
  action read
  target ob_1

condition department = Heart

The above permit-policy allows the nurse from "Heart" department to read the medical record (ob_1) of a patient from the same department.

4.3.3 Outcomes of the Decision-Making Process

In a simple access control model, there are two possible decision outcomes based on existing authorisation policy.

- Permitted Access: A user access request has been granted, if he or she has the right privileges to access data at sensor nodes. For example: A nurse has the right to access medical records of patients from the same department.
- Denied Access: A user access request has been denied. The user is not allowed to access the resources because he does not have the right to access data. For example: A nurse does not have the right to access medical records of patients from other departments.

4.4 Simulation Test Scenario

In WMSNs, each patient has his or her own BSN that consists of several sensors. Sensor nodes implanted in the patient's body continuously monitor glucose level, oxygen, etc. They transmit collected data to a local wireless PDA (data aggregator) or store it locally. The assumption is made that sensed data are stored in the data aggregator, as the medical record with other personal information in BSN.

Users such as doctors and nurses try to access medical records of patients via mobile, personal digital assistant or personal computer. For example, sensors can interact with each other via IEEE 802.15.4 wireless links and interactions with other mobile phones and personal digital assistants from users via Wi-Fi or Bluetooth. Each BSN manages its own policies relating to what kind of actions such as read, write, etc can be performed but for simplicity only read operation is discussed throughout this dissertation. The department that where the doctors or nurses are from, is used when the users try to interact with other BSNs or request to join a patient's BSN for data access. Figure 4.3 shows the architecture of a BSN based on the above discussion.

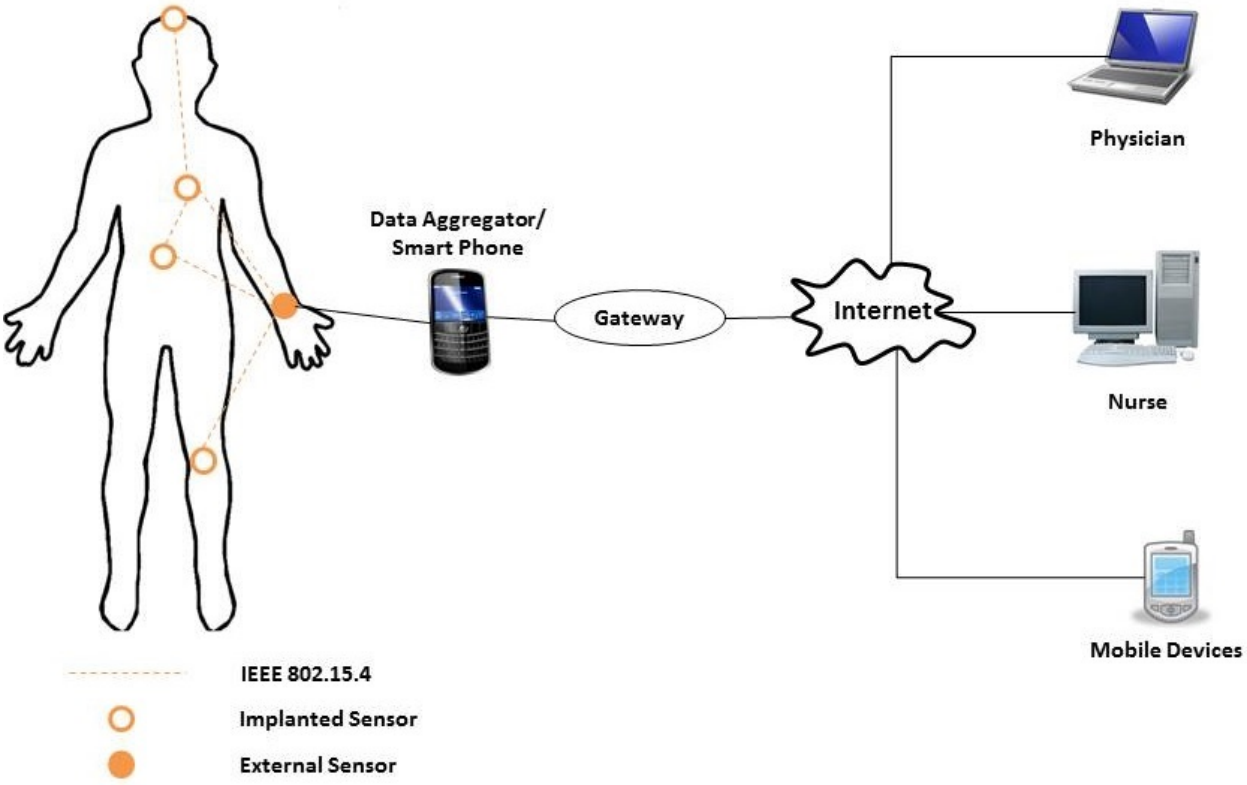


Fig. 4.3 An Example of BSN Architecture

We assume that all the users in this scenario are in a "Hatfield" hospital, and try to access the medical records of the patients. Based on the users' access privileges, data access to a patient's information and medical record will be different. Therefore, access control policies are different based on the users' responsibility, role and department. In this test scenario, the authorisation policies identified to evaluate the proposed simple access control model based on a medical scenario are shown in Table 4.1.

Policy	**Role**	**Department**	**Operation**	**Object**
1	Doctor	Heart	read	ob_1
2	Doctor	Heart	read	ob_2
3	Nurse	Heart	read	ob_1
4	Nurse	Cancer	read	ob_2

Table 4.1 Example of Defined Policy

In policy 1, the doctors from "Heart" department have the right to access the medical record of patient (ob_1), which stores collected data from implanted sensors and personal information, from the same department ("Heart"). Policy 2 allows the doctors to access the medical record of the patient (ob_2) from "Cancer" department. Policy 1 and 2 for the doctors are needed regarding data access to the medical records of patients from both "Cancer" and "Heart" departments. The policies for nurses are slightly different. In policy 3, the nurses from "Heart" department can access the medical record of a patient (ob_1) who is in their department. Unlike doctors, the nurses can only access the medical record of the patient from the same department. Policy 3 and 4 are different. Policy 4 is for the nurses who work in "Cancer" department to access their patients' medical records.

Many other circumstances could have been developed and evaluated, but development of policies is deliberately limited to reduce the experimental results reported in this dissertation to a manageable number. More policies might be needed to check the consistency and accountability of the proposed model in WSNs. In general, other circumstances or other policies may have more or less similarity to the above four policies. However, the above four policies have the essential properties for the evaluation of the simple access control model.

4.5 Experimental Results

The evaluation of the proposed simple access control model using the above medical scenario are presented with screen shots. The interface of the users and decision outcomes can be different based on users' access privileges such as roles, and departments.

Figure 4.4 shows a user interface and decision outcomes for a doctor. In this interface, the doctor needs to provide the patient's path for access to the patient's medical record. In this figure, it shows that the doctor "Maw" has the right to access the medical records of patients from both "Cancer" and "Heart" departments based on decision outcomes. By looking at the path of patients, it shows that these patients are from two different departments: "Heart" department (/patient/heart/bob) and "Cancer" department (/patient/cancer/alice). Based on this figure and decision outcomes, policy 1 and 2 are achieved by showing that the doctor has permission to access medical records of patients from both departments.

A different policy is applied to a nurse. For policies 3 and 4, a user interface for the

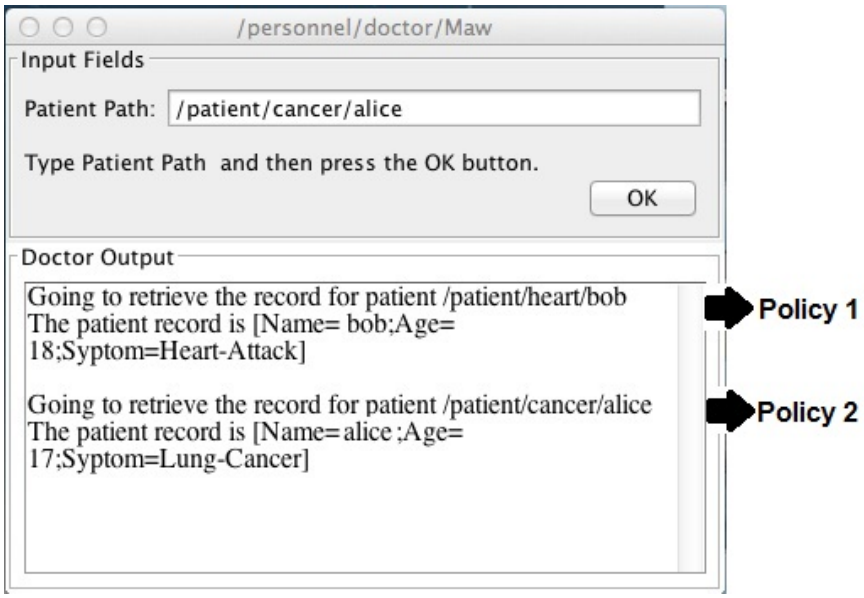


Fig. 4.4 Interface and Decision Outcomes for a Doctor

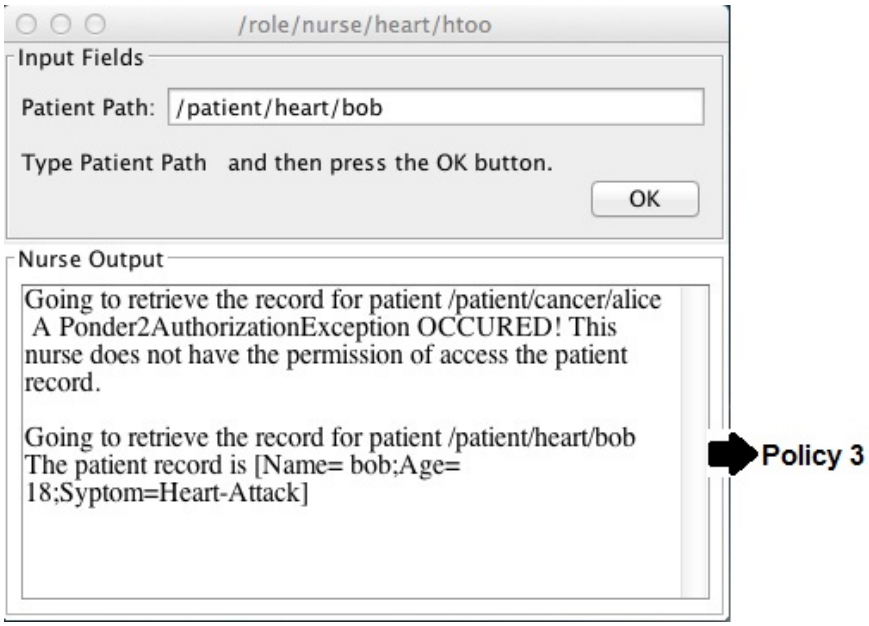


Fig. 4.5 Interface and Decision Outcomes for a Nurse

nurse is developed. As with the interface for the doctor, the nurse needs to provide the patient's path or targeted objects for data access. Figure 4.5 shows an example interface and decision outcomes for the nurse from "Heart" department. Additionally, it shows that the nurse "Htoo" from "Heart" department can access the medical record of the patient (Bob) from the same department but he does not have permission to access the medical record of

the other patient (Alice) in “Cancer” department. Therefore, his data access to that medical record will be rejected. Policy 4 has the same properties as policy 3. Based on the decision outcomes from Figure 4.5, it shows that policies 3 and 4 are achieved by applying different authorisation policies for the user (nurse).

4.6 Conclusion and Next Step

In this chapter, the proposed simple access control model based on the NIST standard with the existing authorisation policy in Ponder2 is discussed and evaluated using a medical scenario. However, there are limited decision-making processes that rely on predefined authorisation policies. This means that the access control engine cannot make decisions regarding data access for emergency and unanticipated situations because there is a lack of data availability in the simple access control model. Therefore, a flexible access policy to address this data availability issue must be provided in the access control engine for emergency and unanticipated situations. For example, a nurse "Htoo” from “Heart” department may need to access the medical record of a patient from “Cancer” department in emergency situations. To address data availability issue in WSNs, the proposed simple access control model is extended with the discretionary overriding concept, namely an adaptive access control model for WSNs in the next chapter.

Chapter 5

An Adaptive Access Control Model

5.1 Introduction

In this chapter, the issue of data availability is addressed by introducing a discretionary overriding concept to the previous simple access control model to evaluate the access decision dynamically for Wireless Sensor Networks (WSNs). This concept can be used to update access-level permissions but also to provide data availability in emergency situations, thereby providing a flexible approach in access control engines regarding access decisions. To address the data availability issue, an adaptive access control model is developed to dynamically adjust and evaluate access decisions for emergency and unanticipated situations.

The structure of this chapter is as follows: firstly, the motivations behind the proposed adaptive access control model are explained, followed by its development details. Additionally, a medical scenario is developed with several defined policies to evaluate the proposed model. Finally, this chapter concludes with suggestions to address how the security policy violations need to be handled and detected as further development.

5.2 Motivations

Many manually administrated procedures are flexible enough in allowing people to expand the roles and alter the rules within the boundary of the special needs. In contrast, access control models in WSNs do not allow similar flexibility. An inflexible access control can cause frustration or prevent people from doing their job. In any security-oriented applications such as healthcare and military, data availability is important to provide for immediate

data access. For example, in a medical scenario, a doctor has the authority to access medical records of patients from any department but a nurse does not have the same permission because of data confidentiality and privacy. The nurse can only access the medical records of patients from his or her department. If the doctor is away or sick, who can access the important or confidential medical data? The nurse is unable to access any important information without approval from doctors or other administrative persons. However, someone who does not have access privileges to access data must retrieve a confidential medical record for that patient, who is in an emergency situation. In this case, a nurse might need to override access policy for emergency data access even though normal access privilege does not allow him or her to do so. Therefore, the question is how the nurse can obtain a confidential medical record while a doctor is not available. These kinds of situations need to be considered for data availability purpose.

A possible method of solving the flexibility problem regarding data availability is to use delegation [119], [89], [28]. This means that a user who has access privileges to certain data can delegate the required power and permission [40] to someone else so that another person can gain necessary access to data. Delegation helps to improve system flexibility to a certain extent when the users know the situations in advance; however, the system needs to define extra situations in advance for the delegation to occur. To address the question of "*How can data availability be provided in emergency and unanticipated situations?*", the discretionary overriding concept is introduced in WSNs to provide a flexible approach in the access control engine.

5.2.1 Discretionary Overriding

The adaptive access control model is proposed and designed based on the concept of discretionary overriding [110], [109] to address the data availability issue. It is introduced to make and adjust decisions locally for emergency and unanticipated situations. Another question that we study in this chapter is "*How can the concept of discretionary overriding provide data availability for emergency situations?*". Overriding of access control is one approach for handling such hard-to-define and unanticipated situations where data availability is critical [10].

Rissanen *et al.* [110] proposed extending the access control model with a possibility-with-override concept to increase the flexibility in hard-to-define or unanticipated situations.

They proposed to explicitly distinguish in the security policy between, what it is *permitted* to do, what it is *forbidden*, and what a principal *can* do. The importance of these distinctions in computer security is argued in [40]. They referred to the solution of intersection between *can* and *forbidden* as possibility-with-override. This means that users may be able to override the denial of access within predefined access control policies. Rissanen *et al.* [110] suggest that there are three possible outcomes to an access request from users: denied access, permitted access and possible-with-override access. These outcomes are explained as follows:

- Permit access: Users have permission to access data.
- Denied Access: Users do not have permission to access data.
- Possibility-with-override: The access is denied to a user but the user may request to override the denial access and gain access to data.

Based on the above three possible outcomes, a system may define the permitted access and the denied access policies for normal situations and leave the possibility-with-override for emergency and unusual situations. The discretionary access control is already developed and implemented in eXtensible Access Control Markup language (XACML) [10], [11] which is a powerful policy language for distributed systems but it is not suitable to use in WSNs. Garcia-Morchon and Wehrle [43] state that the composition of the access control policies in XACML are not efficient due to the high memory requirements of the language or composition complexity. Therefore, the adaptive access control model is designed to address data availability issue for WSNs by introducing the concept of discretionary overriding in Ponder2.

5.3 Adaptive Access Control Framework

Figure 5.1 shows the high-level design of the proposed adaptive access control model with its components. Compared with Figure 4.1, the overriding policy is introduced and defined inside the access control module. Apart from the overriding policy, all the properties such as Policy Enforcement Point (PEP) and an authorisation policy, work the same as in the previous model. Therefore, only the details of the overriding policy are presented in this section.

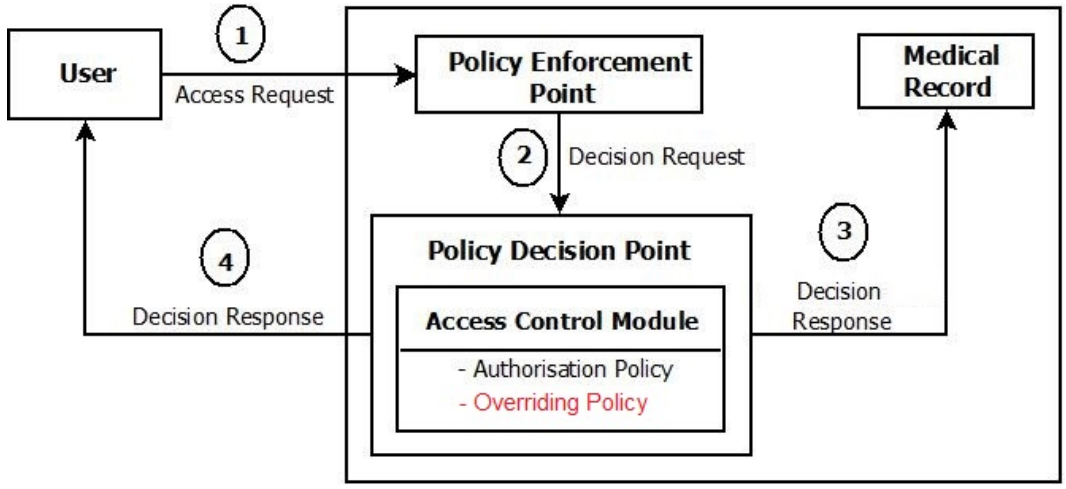


Fig. 5.1 An Adaptive Access Control Model

5.3.1 Overriding Policy

An overriding policy is introduced into the access control engine to override the access policy to support flexibility of access control engine and to address the data availability issue. This means that an access control engine has the capability of overriding a denial of access for emergency situations. Therefore, a simple overriding policy is introduced based on users' role and the contextual information such as department (which department the users are assigned to) and time for policy overriding in decision-making process at the access control engine. An example overriding policy is shown below.

Def: Overriding-Policy
subject nurse
action read
target ob_1
condition Department = Cancer
and time is between 9am to 15pm

Based on the above overriding policy, the nurse from "Cancer" department is allowed restricted access to the medical record of a patient from another department (ob_1 is for a patient from "Heart" department) in emergency situations but he needs to satisfy the above conditions defined for department and time.

5.3.2 Outcomes of the Decision-Making Process

In this model, the policy evaluation for decision-making processes regarding data access relies on both authorisation and overriding policies. The introduction of the discretionary

overriding process can extend the existing two decision outcomes into three outcomes. These are permitted access, denied access and permitted access with overriding. Permitted access and denied access were explained in the previous chapter.

- Permitted Access with Overriding: A user does not have an access privilege to access the resources but his or her restricted access request will be granted if he or she overrides access policy within some constraints such as location and time. For example: a nurse tries to override access policy based on the contextual information for emergency data access to the medical record of a patient from another department.

5.4 Access Control Policy

In a medical scenario, data availability is important in both defined and emergency situations. The loss in data availability can result in further decline in patients' conditions or can possibly lead to death. To address data availability issue in emergency and unanticipated situation, the permitted access with overriding is explained here with example policies. The details of the medical scenario can be seen in the previous chapter. ob_1 is for a patient from "Heart" department and ob_2 is for a patient from "Cancer" department. The policies identified to evaluated the adaptive access control model are shown in Table 5.1.

Policy	**Role**	**Department**	**Time**	**Operation**	**Object**
1	Doctor	Heart	Any	read	ob_1
2	Doctor	Heart	Any	read	ob_2
3	Nurse	Heart	Any	read	ob_1
4	Nurse	Cancer	Any	read	ob_2
5	Nurse	Cancer	9am $<$ and $<$ 17pm	override^{read}	ob_1
6	Nurse	Heart	9am $<$ and $<$ 17pm	override^{read}	ob_2

Table 5.1 Example of Defined Policy

Policy 1 to 4 are the same as in the previous model. Policy 5 and 6 that have a similar property, are related to the overriding policy. Normally, a nurse from one department does not have permission to access the medical records of patients from departments other than

his or hers. In the policy 5, the nurse from “Cancer” department can override access policy to access the medical record of patient from “Heart” department when it is needed for emergency situations. This means that, he or she can override the access policy based on the contextual information, such as time and department, for emergency data access. The same concept is applied to policy 6 for the nurse from “Heart” department. The constraints we consider in this model are that the department of the user has to be the same as where he works for and the access is within the working schedule. Otherwise, the restricted access request will be rejected.

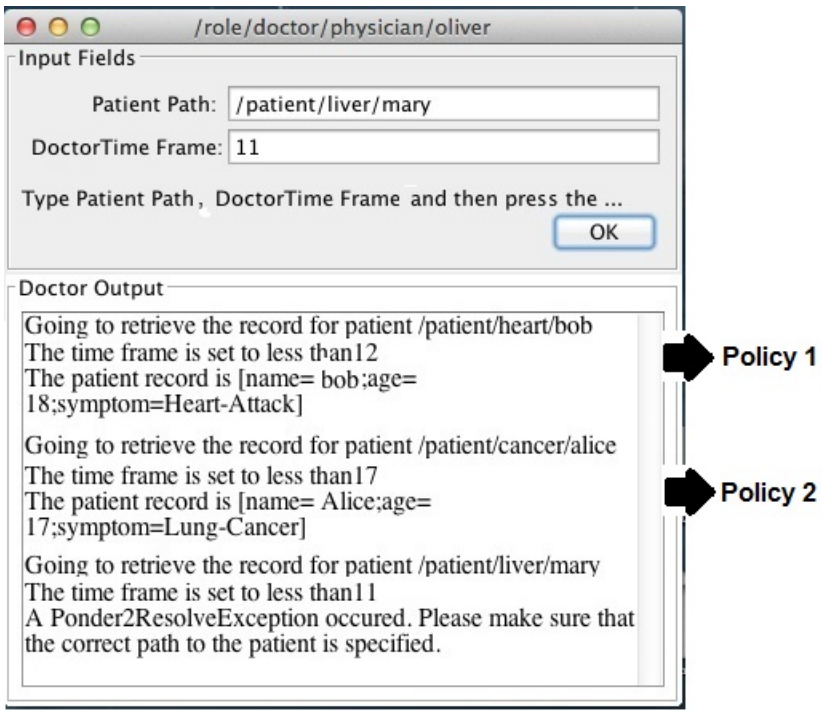


Fig. 5.2 Interface and Decision Outcomes for a Doctor

5.5 Experimental Results

Detailed information of how the proposed adaptive access control model is evaluated by developing a medical scenario in Ponder2 with the above policies is presented with screen shots. Although Policy 1 to 4 are the same as the previous model, the interface of the users is more advanced and more information is required regarding simulation purposes to access the medical records of patients.

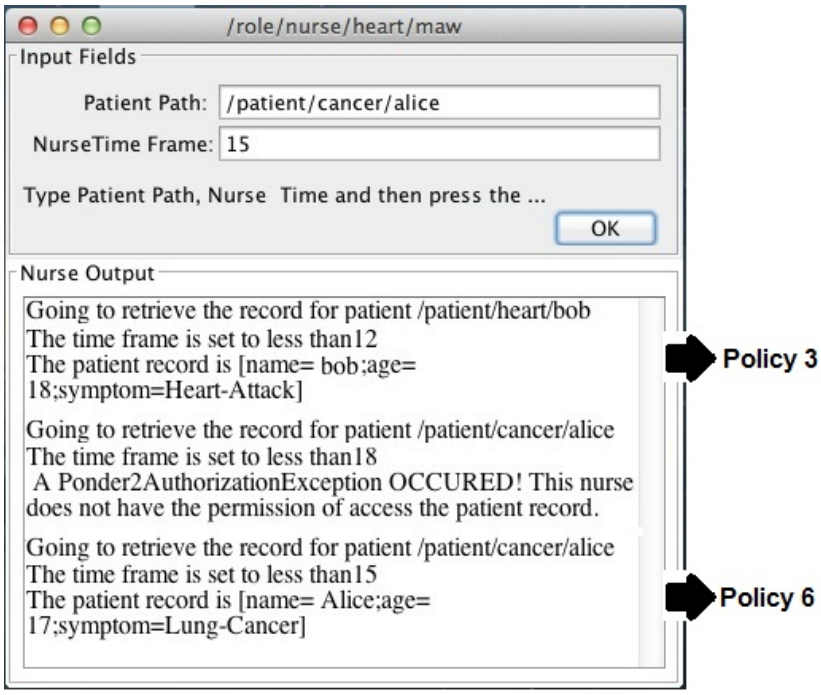


Fig. 5.3 Interface and Decision Outcomes for a Nurse

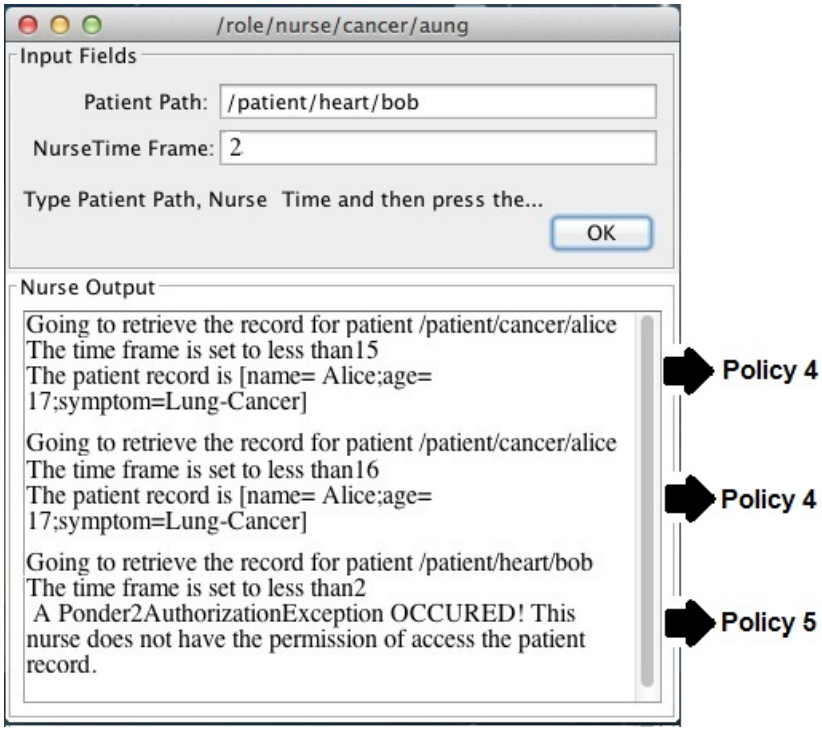


Fig. 5.4 Interface and Decision Outcomes for a Nurse

Figure 5.2 shows a user interface and decision outcomes for a doctor "Oliver". The patient's path and contextual information are required for the purpose of simulation. In the proposed adaptive access control model, the doctor needs to provide contextual information such as department and time for data access. Based on the decision outcomes, the doctor has the right to access medical records of patients from both "Heart" and "Cancer" departments. This means that, the policy 1 and 2 are achieved in the proposed model.

Figure 5.3 shows how the overriding process can be done in the proposed adaptive access control model. Based on the decision outcomes from Figure 5.3, the nurse (Maw) from "Heart" department can access medical records of patients from his department regarding policy 3. In the second case, his restricted access has been denied because he did not meet the time criteria from the overriding policy. In the last case, he tried to override his or her policy regarding access the medical record of the patient from another department: "Cancer". To override an access policy successfully and for access to be granted, the user needs to satisfy the defined thresholds such as role, department and time. Therefore, the final result shows that the nurse can access the medical record from another department by overriding the denial of access based on policy 5. Policy 6 has the same properties as policy 5 but it is aimed for nurses in "Cancer" department. Figure 5.4 shows the user interface of the nurse (Aung) from "Cancer" department but the expressions are the same as Figure 5.3.

Therefore, data availability is provided at some situations in the proposed model. The decision outcomes in the adaptive access control model are checked for consistency as well as to verify and test the overriding policy based on the different user interface.

5.6 Conclusion and Next Step

In this section, detailed information of the proposed adaptive access control model is presented with user interface and decision outcomes. The advantage of the adaptive access control model over the simple access control model is that it introduced the overriding policy to provide data availability service in emergency and unanticipated situations. One of the weaknesses of the proposed adaptive access control model is that there is no facility or mechanism to detect security policy violations such as unauthorised information release and unnecessary overriding process[1]. Therefore, data privacy is lost in security policy violations initiated by a malicious or unfaithful user. The questions that now arise are how can the sys-

[1]Unnecessary overriding process means misuse of overriding policy.

tem handle this kind of situation and what are the courses of action for restricted access in WSNs. Based on the above weakness in the adaptive access control model, an improved version of the model with a prevention and detection mechanism will be proposed in the next chapter.

Chapter 6

Adaptive Access Control Model with a Prevention and Detection Mechanism

6.1 Introduction

In this chapter, the framework of the previous adaptive access control model is extended with a prevention and detection mechanism to address how security policy violations are handled and detected in Wireless Sensor Networks (WSNs). An introduction of the overriding policy in the previous model can provide data availability in emergency and unanticipated situations but there is a weakness of applying it. The weakness is that the user may always try to override access policy whenever he or she desires data access. If there is no security mechanism to detect the security policy violations, security breaches can occur at any time. There is no prevention or detection mechanism in current WSN access control models for auditing purposes to detect the security policy violations. Sandhu and Samarati [118] mention that the role of auditing is to produce an analysis of data to discover or diagnose security violations. Therefore, a prevention and detection mechanism is extended to the previous adaptive access control model to detect security policy violations and misuse of the overriding facility from both authorised and unauthorised users. Additionally, an obligation policy is introduced to identify the courses of action when a restricted access is granted or denied in emergency and unanticipated situations.

The structure of this chapter is as follows: Firstly, the adaptive access control model with a prevention and detection mechanism is presented. Additionally, a medical application is developed under Ponder2 to evaluate and check whether the proposed adaptive access control model with the prevention and detection mechanism has achieved its objectives.

Finally, this chapter concludes with suggestions for the next step.

6.2 Adaptive Access Control model with a Prevention and Detection Mechanism

The overview diagram of the proposed adaptive access control model with the prevention and detection mechanism can be seen in Figure 6.1. Based on this figure, all the components such as PEP, authorisation policy and overriding policy, work the same as in the previous models. In the access control module, an obligation policy is added to use along with the authorisation decisions for auditing purpose. Details of the obligation policy and prevention and detection mechanism are explained below.

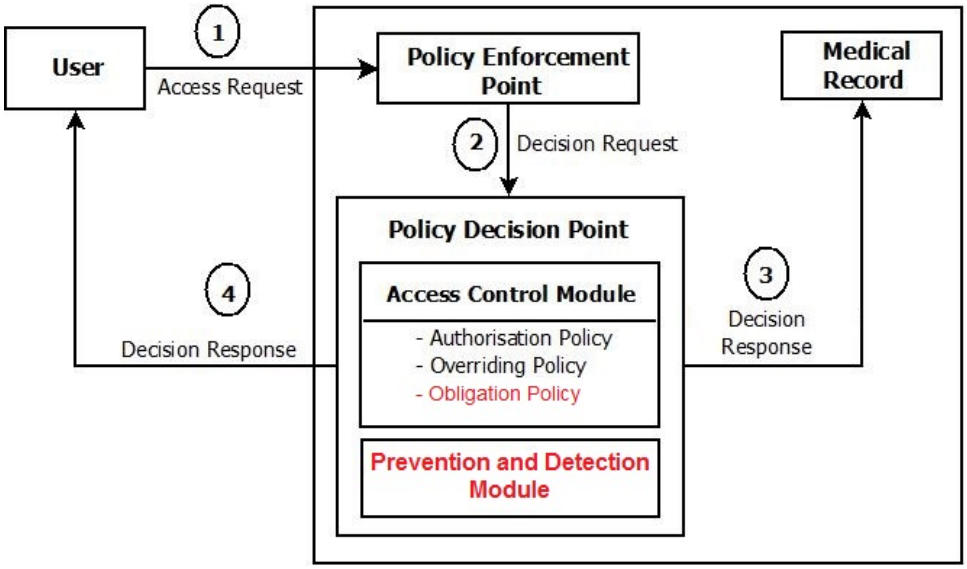


Fig. 6.1 An Adaptive Access Control Model with a Prevention and Detection Mechanism

6.2.1 Obligation Policy

Accorsi and Stocker [1] suggest that obligations are used as post conditions that must be fulfilled after the authorisation decisions. An obligation is introduced to take some courses of action regarding the issue that relates with the overriding process. This issue is "*What should happen if a restricted access is granted*".

To address the above issue, the obligation policy is used to perform a course of action that a user is required to take in emergency and unanticipated situations. The obligation

policy may "Trigger an Alarm", "Notification Message" and keep an audit log for further investigations that are related to audit purposes. After the policy has been evaluated, the specific obligations are sent automatically with the authorisation decisions to the management teams. Therefore, the obligation policy is used as post condition after the enforcement of authorisation decisions. The format of obligation policy is shown below.

Def: Obligation-Policy
condition policy type is override
target Em_{log}
do write.audit < subject, Time, Target, Department, Decision Outcomes >
and trigger-alarm
and notify-message

The above obligation-policy will activate when the overriding process is invoked. For example, if restricted access is granted or denied to a nurse based on the overriding policy, the obligation policy will be activated along with authorisation decisions to perform some actions.

6.2.2 Prevention and Detection Module

The main idea of introducing a prevention and detection mechanism [21], [19], [112] is to protect the privacy and confidentiality of data by storing users' information, actions, etc. as an audit log for the purpose of detecting security violations. For an audit log to be usable, it should:

- Be available through a usable interface for the auditors or the administrators.
- Contain sufficiently detailed information to get a picture of what has happened.

Regarding the above facts, the audit log is to record the event and specify 1) when it occurred, 2) the user information associated with that event and 3) the results of the decision-making process. An audit log can assist in detecting security violations and flaws in the system by detecting any suspicious access from users. In the audit log format, the subject is a user who tries to access a medical record from the targeted object with an authorisation decision. In the audit log, the contextual information such as time and department are also recorded. The format of the audit record is shown as follows:

Auditlog := [Subject + Time + Target + Department + Decision Outcomes]

There are two different audit logs in the proposed model. These are:

- Access Log - every time a medical record is opened an entry is created in the access log containing information about the users, the patient and the document being accessed.

- Emergency Log - an entry is created in this log whenever a restricted access is permitted or denied using the overriding process.

These two logs are stored as Comma Separated Value (CSV) extension, so it can be easily checked and monitored by system administrators. Therefore, the prevention and detection module is used in the proposed model to keep a record of all the users' access information as an audit log for detecting security policy violations.

6.2.3 Outcomes of the Decision-Making Process

In the proposed adaptive access control model with a prevention and detection mechanism, the decision-making processes regarding data access are based on the authorisation, overriding and obligation policies. There are five possible decision outcomes based on existing policies, two of which, permitted access and denied access, are already explained in chapter 4. Permitted access with overriding from the previous chapter is replaced with permitted access with overriding and obligation. Therefore, the remaining two different decision outcomes and permitted access with overriding, and obligation are discussed as follows.

- Permitted Access with Obligation - A user access request has been granted but the obligation policy is activated automatically to take some actions when data access is given to that user especially for important and confidential information.

- Denied Access with Obligation - A user does not have access privilege to the resources and his or her restricted access has been denied. Additionally, the obligation policy is activated to take a course of action after the authorisation decision is made.

- Permitted Access with Overriding and Obligation - A user does not have access privilege to the resources but the restricted access will be granted if he or she overrides the access policy within some constraints, such as contextual information. Additionally, the obligation policy is activated to detect unnecessary overriding processes by authorised users when the overriding policy is used for decision evaluation.

Policy	**Role**	**Department**	**Time**	**Operation**	**Oblg**	**Object**	**Obligations**
1	Doctor	Heart	Any	read	N.A.	ob_1	N.A.
2	Doctor	Heart	Any	read	Oblg	ob_2	Oblg [Notification Message]
3	Nurse	Heart	Any	read	N.A.	ob_1	N.A.
4	Nurse	Cancer	Any	read	N.A.	ob_2	N.A.
5	Nurse	Heart	9am $<$ and $<$ 17pm	override^{read}	Oblg	ob_2	Oblg [Notification Message and Trigger the Alarm]
6	Nurse	Cancer	9am $<$ and $<$ 17pm	override^{read}	Oblg	ob_1	Oblg [Notification Message and Trigger the Alarm]
7	Admin	Audit	Any	read	N.A.	Ac_{log}	N.A.
8	Admin	Audit	Any	read	N.A.	Em_{log}	N.A.

Table 6.1 Example of Defined Policy

6.3 Access Control Policy

Unlike the previous medical scenario, this scenario considers the provision of data availability with a certain degree of detection to detect security policy violations. In this test scenario, the following policies in Table 6.1 are identified and developed to evaluate the proposed model.

The policies 1, 2, 3 and 4 have the same policy definitions as those shown previously in chapters 4 and 5 but in policy 2, the obligation is added to take a course of action when the doctor tries to access a medical record of patients from another department. In addition, policies 5 and 6 are new policies to show that a combination of overriding policy, obligation policy and a prevention and detection mechanism is beneficial to healthcare application in WSNs. The policy 5 allows the nurse from "Heart" department to access the medical record of patient from another department, if he or she satisfies the defined threshold from the overriding policy but the obligation policy is activated to perform some courses of ac-

tions. The policy 6 is for the nurses from "Cancer" department to override access policy in unanticipated situations. Additionally, policy 7 and 8 allow the administrators from "Audit" department to read both access and emergency log for auditing purpose at any time.

6.4 Experimental Results

The evaluation of the proposed adaptive access control model with a prevention and detection module with a medical scenario is presented with screen shots. Firstly, user interface and decision outcomes for a doctor is discussed; followed by a nurse.

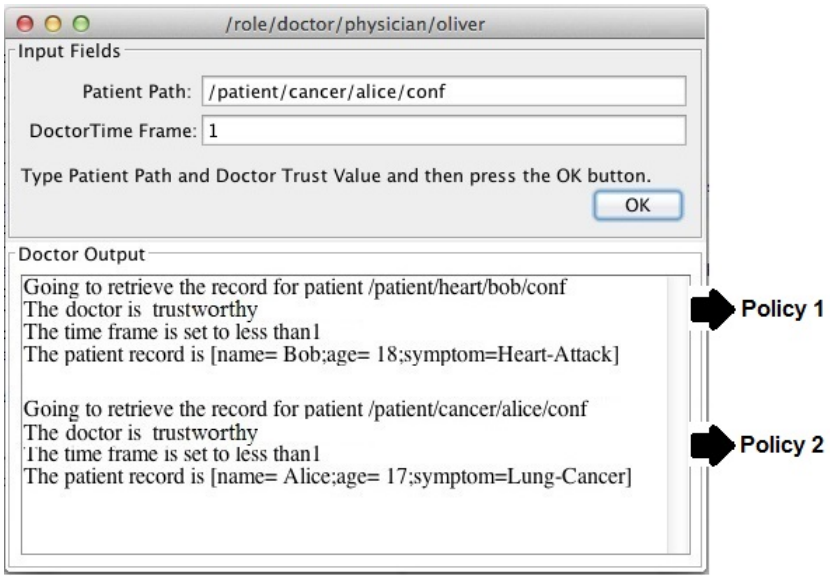


Fig. 6.2 Interface and Decision Outcomes for a Doctor

Figure 6.2 presents user interface and decision outcomes of a doctor "Oliver". Based on the decision outcome, the doctor can access the normal medical record of the patient from "Heart" department. When he requests data access to a confidential medical record of that patient, an obligation policy is activated along with an authorisation decision based on policy 2. This means that he can have access to both medical records but an obligation might be performed based on this content are how sensitive.

Figure 6.3 shows the interface of the nurse as well as decision outcomes. The first result shows that the nurse from "Cancer" department can access the medical record of the patient from that department. In the second case, access to the medical record of a patient

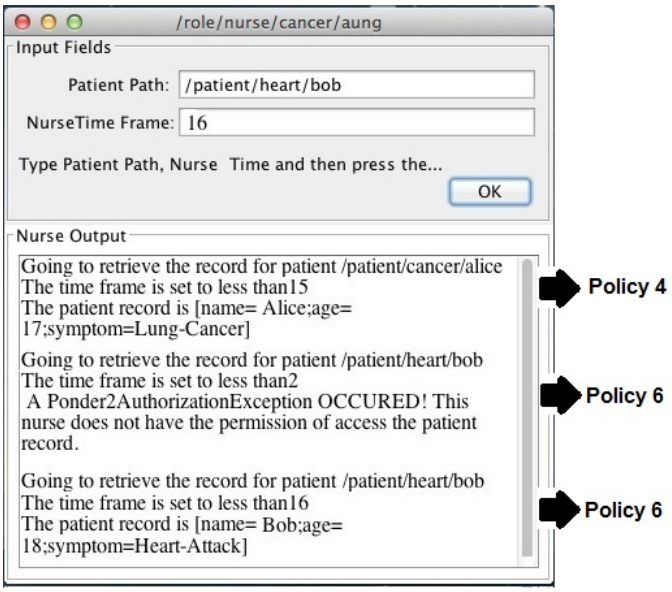


Fig. 6.3 Interface and Decision Outcomes for a Nurse

from "Heart" department is denied because the user does not satisfy the defined thresholds from the overriding policy, but the obligation policy is still activated to take some actions for auditing purpose. The final result shows that if a nurse satisfies the thresholds from the overriding policy, access for the normal medical record is granted to that user, but some obligations are triggered. Based on the decision outcomes and evaluation results shown in Figure 6.3, the properties of policies 5 to 6 are achieved in the proposed model.

Audit trails are used to detect security policy violations from both authorised and unauthorised users. All the users' requested accesses are kept as a log for auditing purposes. The access log can be seen in Figure 6.4. This log will keep all the user access information from all attempts to access data from the targeted objects. Figure 6.5 shows the emergency audit log that creates an entry of the users who uses the property of the overriding process. The audit logs are stored in the prevention and detection module.

6.5 Conclusion and Next Step

In this chapter, detailed information of the proposed adaptive access control model with a prevention and detection mechanism is presented with figures and diagrams. Both access and emergency audit logs are stored in the prevention and detection module to detect

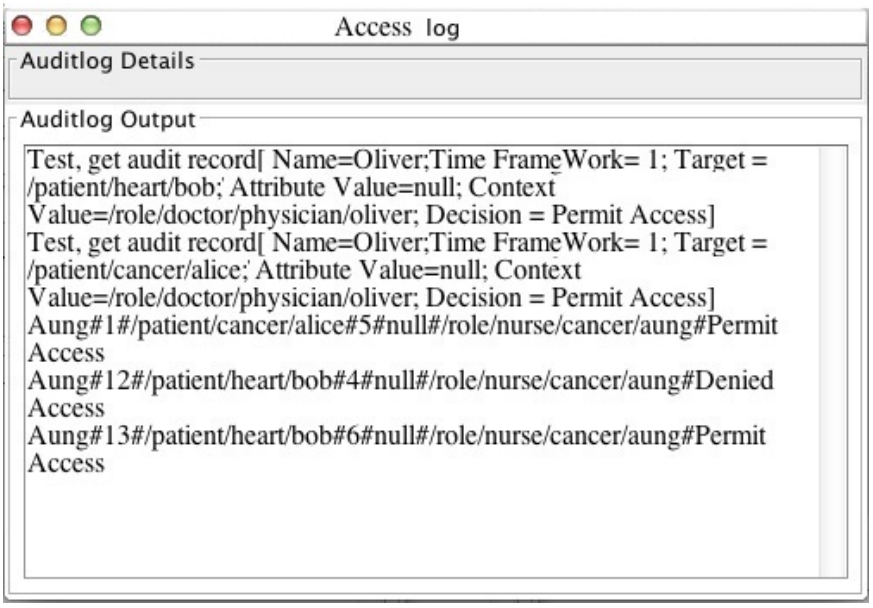


Fig. 6.4 An Interface for the Access Log

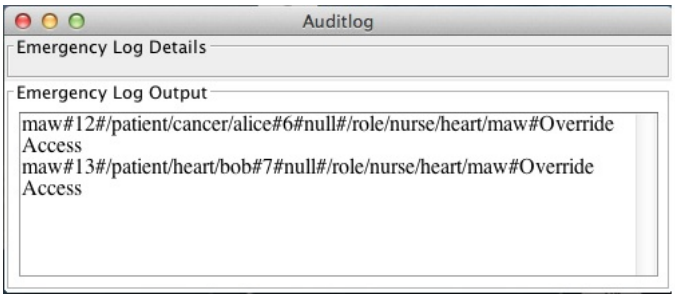


Fig. 6.5 An Interface for the Emergency Log

security policy violations. Along with authorisation decisions, the obligation policy is introduced to perform a course of action when the restricted access is granted or denied in emergency and unanticipated situations. Therefore, the proposed model can detect security policy violations and detect unnecessary overriding processes by taking courses of action alongside authorisation decisions. In this model, there is no way to detect an abnormal data access from authorised users because the normal authorisation policy allows the users to access the medical record at any time and from any department. On the other hand, we cannot assume that all the users are trustworthy enough to override access policy for the restricted access in unanticipated situations. Therefore, a trust model is considered to be included in the proposed model to check whether the users are trustworthy or untrustworthy based on the dynamic changes of their behaviour. Additionally, a trust model can enhance the capability of making decisions at the access control engine by using trust value as one of the

defined thresholds in the policy evaluation. To address the above issues in the next chapter, a simple user behaviour trust model is developed to integrate with the access control model.

Chapter 7

A Simple User Behaviour Trust Model

7.1 Introduction

In the previous chapters, the assumption was made that all the users are trustworthy enough to perform overriding on a denial of access in emergency and unexpected situations; however, in reality, users are not always trustworthy enough to give that kind of a flexible access. Based on that weakness in the previous model, in this chapter a user behaviour trust model for Wireless Sensor Networks (WSNs) is introduced and developed to evaluate user trustworthiness based on the highly dynamic and unpredictable characteristic of each user.

The structure of this chapter is as follows: firstly, trust in WSNs is discussed, followed by the proposed user behaviour trust model. The data flow diagram and algorithm for the proposed model are explained next. Additionally, the trust algorithm is evaluated based on numerical analysis in MATLAB to show the characteristic variations of the total trust value of the user based on their behaviour information. Finally, this chapter concludes with suggestions to integrate trust with the adaptive access control model from chapter 6 for making an effective access decision by providing a flexible approach to define policies that are not too permissive nor too strict.

7.2 Trust in WSNs

Trust plays an important role in networks and human life environments. In the context of a network, trust is used to help its components to decide whether another member, node or device from the same network is being inattentive, uncooperative or compromised.

Fernandez-Gago [34] states that trust becomes quite important in self-configurable and autonomous systems such as WSNs, Wireless Body Area Networks (WBANs) and Wireless Medical Sensor Networks (WMSNs). Having different definitions in security related literatures "trust" in this chapter is considered as the trustworthiness of users based on highly dynamic and unpredictable characteristic of their behaviour.

Trust in WSNs can be classified into different categories based on the needs of the application. The classification of trust [123] is explained as follow:

- Direct Trust: Direct trust is the trust that a subject holds of another service provider without any intermediate service provider or entity.
- Indirect Trust: Indirect trust is the trust that a subject holds of one service provider through some other service provider or entity.
- Full Trust: A subject is said to have full trust of a service provider if that subject trusts all the services provided.
- Partial Trust: A subject is said to have partial trust of a service provider, if that subject trusts some of the services provided.
- Recommended Trust: Recommended trust is the trust of one entity of another that is recommended by other entities.
- Authentication Trust: Authentication trust is the trust of an entity of the authenticity based on an identity certificate signed by a certificate authority.
- Communication Trust: Communication trust means that the trust is calculated between the sensor nodes based on their cooperation of routing messages to other nodes in the network [95].
- Data Trust: Data trust is the trust that is based on the actually sensed data of the sensors [92].

Regarding the above categorisation of trust, direct and indirect trust are commonly used in trust calculations of sensor nodes [94], [92] to check whether the nodes are trustworthy or not based on Bayesian network [25] and Naive Bayes classification algorithms [145]. For reputation-based trust calculation [93], [42], trust are used in key management and network management. Authentication trust is mostly used in policy-based trust management systems

Trust based Schemes in WSNs	
Trust-based Schemes	References
Trust-based routing management or protocol	[128], [16], [2], [75], [96], [142], [98]
Trust-based intrusion detection	[14], [15], [16]
Trust-based key management	[70], [76], [77], [81]
Trust-based malicious node detection	[64], [149], [59], [94]
Group-based trust management	[121], [148]
Reputation-based trust management	[93], [42], [125]

Table 7.1 A Taxonomy of Trust-Based Schemes in WSNs

[123]. The communication and data trust proposed by Momani [95], is used to calculate trust between sensor nodes. Therefore, trust can be divided in six groups regarding the aspects of requirements in WSNs: trust-based routing management or protocol; trust-based intrusion detection; trust-based key management; trust-based malicious node detection; and group-based and reputation-based trust management for networks. Table 7.1 shows the taxonomy of trust-based schemes in the published literatures for WSNs.

Trust can also resolve security related routing issues. Several trust management schemes [128], [16], [2], [75], [96] are proposed to detect suspicious transmission and identify malicious nodes for disseminating information in the network. For example, trust-based routing management only allows the trusted sensor nodes to participate in the routing. Direct trust and indirect trust are mostly used to evaluate each node's trustworthiness based on trust metrics (i.e. Quality of Service (QoS) characteristics such as data packets forwarded, control message forwarded, availability based on beacon or Hello message, etc.) and weight factors. One of the trust algorithms for routing management calculates the direct trust based on Geometric Mean [88] of the QoS characteristics. The indirect (second-hand) information may be particularly useful when there is no direct interaction, i.e. when the situation is risky, then the indirect trust plays major role in the formation of trust on any node.

Trust-based intrusion detection schemes such as [14], [15], [16] are used to effectively deal with selfish or malicious nodes and to improve QoS in WSNs. The trust-based intrusion detection schemes considered the effect of both social trust (such as honesty [1]) and QoS trust (such as competence, reliability and task completion capability) to detect malicious nodes.

[1]The honesty trust is the trust that measure through evidences of dishonesty such as false self-reporting and abnormal trust recommendations.

Trust-based key management schemes [70], [76], [77] based on cryptographic method are proposed to provide a secure communication channel in WSNs. Since sensor nodes collect personal medical data, security and privacy are important services in this kind of networks. It is aimed to securely and efficiently generate and distribute session keys based on biometrics (such as electrocardiogram [81]) or identity-based encryption [8] between the sensor nodes and the base station to secure end-to-end transmission.

The aim of trust-based malicious node detection is to minimise communication and storage overhead, and to improve reliability in WSNs. Direct and indirect trust are mostly used in malicious node detection methods to calculate the trust value of each node based on weighted running average approach [91]. Direct trust method [59] consists of the following steps:

- Behaviour of the node is monitored periodically.
- In each period the numbers of good and bad behaviour of the node are recorded.
- Based on the numbers of good and bad behaviour, trust is calculated periodically.

Indirect trust is calculated based on recommendation (second hand information) obtained from trustful neighbours. Additionally, the communication and data trust are also used to detect malicious node based on Bayesian network.

The group-based trust management schemes for clustered WSNs such as [121], [148] is aimed to detect and prevent selfish, faulty and malicious nodes, to minimise the memory overhead, and to reduce the communication overhead by making sensor nodes only communicate with the cluster head. The trust value calculation in cluster head is based on weighted running average, so that the recent trust value can be given more weight in the overall trust calculation.

Distributed Reputation-based Beacon Trust System (DRBTS) [125] are aimed at providing a method by which bacon nodes[2] can monitor each other and provide information so that sensor nodes can choose whom to trust, based on a quorum voting approach [124]. In order to trust a bacon node's information, a sensor must get votes for its trustworthiness from at least half of their common neighbours. Ganeriwal and Srivastava [42] propose a framework

[2]A beacon node assists other sensor nodes to determine their location.

where each sensor node maintains reputation metric representing past behaviour of other nodes, which are then used as an inherent aspect in predicting future behaviour. This approach is based on a Bayesian formulation, specifically a beta reputation system [62], for the algorithm steps of reputation representation, updates, integration and trust evolution. Overall, reputation-based trust management are employed in WSNs to deal with malicious and unreliable nodes based on first and second hand information from the neighbours.

Based on the above discussion, most of the trust schemes in WSNs are using weight factors, so that the direct trust or recent trust can be given more weight in the overall trust calculation. Direct trust, indirect trust and trust that based on QoS characteristics are commonly used in trust calculations of sensor nodes to check whether the nodes are trustworthy or untrustworthy based on Bayesian network, Naive Bayes and geometric mean. Regarding the above facts, there is no existing trust model that evaluates trust based on users' behaviour information. This means that none of the existing trust models can be readily related to the decision-making process in the access control engine. The evaluation of trust for users based on their behaviour information is significant in forming a trustworthy network and is a new research issue in WSNs. Therefore, we propose a user behaviour trust model to use in WSNs and WMSNs in order to measure behaviour trust of the user from the system perspective to enhance access decisions. Unlike existing trust models in WSNs, the proposed model is aimed at calculating the trust value of each user regarding whether the users are trustworthy or untrustworthy, based on highly dynamic characteristics of their behaviour information.

7.3 A User Behaviour Trust Model

A user behaviour trust model that uses current user behaviour information and previous trust values to calculate user trustworthiness from the system perspective is proposed and introduced in WSNs. The current trust value is the geometric mean [88] of information obtained from the user's current access requests to an object, such as user's role, location and time. The main reason of using the geometric mean is that it compares different attributes - finding a single "figure of merit" for these attributes - when each attribute has different numeric ranges. The concept of using geometric mean to calculate the direct trust based on QoS characteristics of a sensor node for routing management [124] motivates us to reproduce a simple calculation for current trust evaluation based on a user's behaviour information such as the role and the contextual information from the access request. The user's behaviour information can be considered as user's characteristic and calculated based on geometric

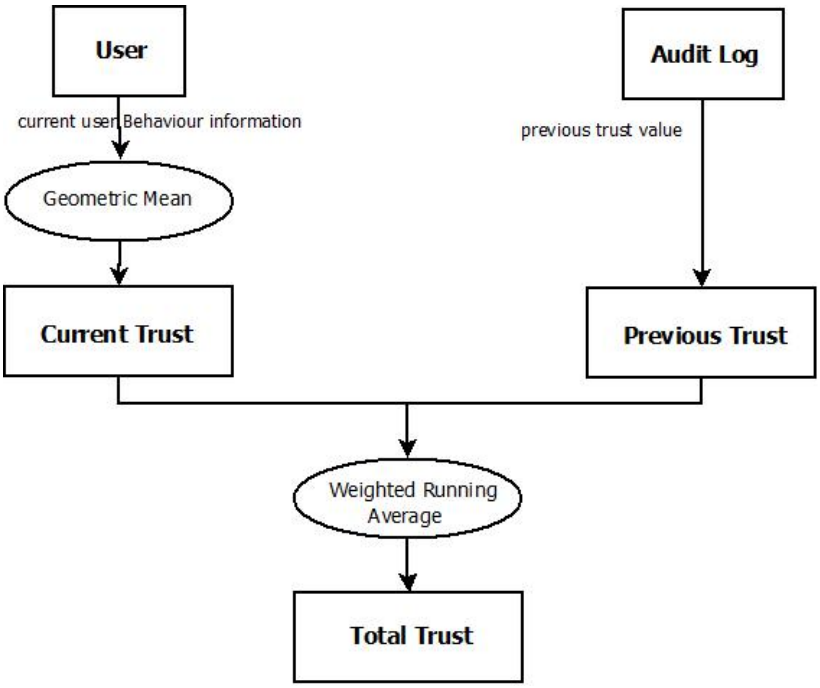


Fig. 7.1 Overview of the Trust Model

mean formula. The geometric mean equation can be seen as follow:

$$(\prod_{i=1}^{n} a_i)^{\frac{1}{n}} = \sqrt[n]{a_1 * a_2 * ..... * a_n} \tag{7.1}$$

For the previous trust value, the total trust value of the user from the previous transaction is used. This means that the total trust value of users does not rely completely on the evaluation of current trust. The traditional weighting approach [91] is used to calculate the total trust value of a user based on the current trust and the previous trust. The weight factor is commonly used in the trust calculation, so that the recent behaviour characteristics can be given more weight in the overall trust calculation. If total behaviour trust value is higher than the defined threshold, the user is trustworthy enough to perform an action on a certain object. When it goes under the defined threshold, the user becomes an untrustworthy person and the system may decline his access to a specific object. An overview of the user behaviour trust model can be seen in Figure 7.1. There are three sub-modules: current trust, previous trust and total trust.

7.3.1 Current Behaviour Trust Value (T^{cur})

A user's behaviour information (such as the role and the contextual information from the access request) is used to calculate the current trust value of the user. The formula for the evaluation of current behaviour trust based on geometric mean is shown below:

$$\mathbf{T}^{cur} = (\prod_{i=1}^{n} a_i)^{\frac{1}{n}} \tag{7.2}$$

where,
n = Number of Attributes
a = Attribute

Based on the user's behaviour information (such as location, role and time), the above equation is substituted as follow:

$$\mathbf{T}^{cur} = \sqrt[3]{T^{Lo} * T^{Ro} * T^{Ti}} \tag{7.3}$$

where,
T^{cur} = Current Trust Value
T^{Lo} = Trust Value for Location
T^{Ro} = Trust Value for User's Role
T^{Ti} = Trust Value for Time Range

Equation 7.3 shows that the current behaviour trust value is evaluated based on three different attributes: location; user's role; and user's time range. Each attribute has a defined value between 1 and 4 because we consider three different conditions in the proposed model. The defined value of each attribute is evaluated differently. Based on the geometric mean, the maximum value of current behaviour trust can be up to 4 and the lowest value can be 1.

In the proposed model, the physical location of a user (location of subject), which department that user is from (department of subject) and where is the targeted data that the user tries to access (department of object) are considered as the evaluation criteria for the location attribute. Table 7.2 represents an example data set to evaluate the trust value of location for a user.

Department of Subject	Department of Object	Location of Subject	T^{Lo}
A	A	A	4
A	A	B	3
A	B	A	2
A	B	B	1

Table 7.2 An Evaluation Criteria for Location Attribute

Based on Table 7.2, if the department of the subject, the location of the subject and the department of the object are the same (in this case "A" department), the trust value of location for a user is defined as 4 that is a maximum value. If the user works in department "A" and tries to access data which stores the same department "A" but his actual location is from another department ("B"), his trust value is set as 3. If the object is stored in "B" department but both department of subject and location of subject are from "A" department, the trust value is defined as 2 because the user tries to access data which is stored in the different department. In last case, the trust value of location for a user is the lowest 1 when the location of subject and the department of object are different compared to the department of the subject.

The defined trust value for a user's role is reflected based on their responsibility and duty. For the doctor, the trust value for user's role is set as 4 but for the nurses, it is defined as 2. The trust value can be different for other roles (such as administration staff, laboratory staff, etc.) but we only consider doctors' and nurses' roles. In general, if the current user's time range is within the system defined time frame, the trust value of the time criteria T^{Ti} is set between 1 to 4. In a medical application, some users work in the daytime and some in the night time. Therefore, the defined trust value for time criteria can change based on users' working schedule or time framework. Example conditions for time criteria can be seen in Table 7.3.

Ti	T^{Ti}
$12 \leq \text{Ti} < 18$	4
$6 \leq \text{Ti} < 12$	3
$18 \leq \text{Ti} < 24$	2
$0 \leq \text{Ti} < 6$	1

Table 7.3 An Evaluation Criteria for Time Attribute

Based on the above discussion, the evaluation for each criterion is considered separately based on the requirements of the application for the current behaviour trust. The proposed current trust module can easily be extended with additional attributes for extra criteria for evaluation of trust.

7.3.2 Previous Trust Value (T^{pre})

In the proposed model, the previous trust value is used as one of the supporting factors for total trust evaluation when the user requests at the next attempt. The user trust values from the previous transactions are used as the previous trust value of the users. T^{pre} is equivalent to the total trust value of users from the previous transactions.

7.3.3 Total Trust Value (T^{total})

The total behaviour trust value checks whether the user is trustworthy or untrustworthy to perform some actions based on his or her current and previous behaviour trust values. The total trust value is a function of current and previous trust values. The proposed model also uses the traditional weighting approach as in [91], [8] to combine current and previous trust to form the total trust per relation in the system, as shown in equation 7.4.

$$\mathbf{T}^{total}\mathbf{(n)} = (\ \alpha * \mathbf{T}^{cur}\mathbf{(n)}) + (\ \beta * \mathbf{T}^{pre}\mathbf{(n)}) \tag{7.4}$$

where,
T^{total}(n) = Total Trust Value of the nth Transaction
$T^{cur}(n)$ = Current Trust Value of the nth Transaction
T^{pre}(n) = Previous Trust Value of the nth Transaction
α = Constant Weighting Factor ($0 \leq \alpha \leq 1$) to the current trust
β = Constant Weighting Factor (1 - α) to the previous trust

α is a weighting given to the current trust and β to the previous trust where $\alpha + \beta = 1$ and $0 \leq \alpha, \beta \leq 1$. Weights can be assigned using different approaches. Depending on the application, sometimes the current trust may be given more weight and the previous trust may be given less weight i.e. $\alpha > \beta$, and vice-versa. Additionally, the traditional weighting approach is commonly used in the overall trust calculation in WSNs regarding direct and indirect trust. If there is no previous behaviour trust, the current behaviour trust value is used as the total behaviour trust value. Based on the evaluation of the total behaviour trust

value of a user, the levels of trustworthiness can be expressed as follows:

- A user is trustworthy if $T^{total} \geq T^{threshold}$
- A user is untrustworthy if $T^{total} < T^{threshold}$

Currently, a simple method is used to differentiate whether a user is trustworthy or untrustworthy based on the total trust. If the total trust value of the user is higher than or equal to the defined threshold ($T^{threshold}$) which is 2.5 based on the arithmetic mean[3] [31] of previous trust and current trust, he is a trustworthy person, but when the total trust value is under the defined threshold, that person is deemed an untrustworthy person. After the evaluation of total behaviour trust value for that user, that value will be forwarded to the access control module for decisions regarding data access. Using behaviour trust values can enhance the decision-making process at the access control module. The behaviour trust module assists the decision-making process regarding whether the user is trustworthy or un-trustworthy to perform some actions in the specific targeted objects.

7.4 Data Flow Chart

The data flow chart for the behaviour trust module can be seen in Figure 7.2. When the user behaviour trust module receives user requested information (U^{info}), the current behaviour trust module evaluates the current user's information. After that, the system checks whether the user has previous interaction by checking his previous behaviour trust value. If it is the first attempt for that user, where T^{pre}(n) is inapplicable, the current behaviour trust value is used as the total behaviour trust value.

If T^{pre}(n) is greater than zero, both current and previous trust values are forwarded to the main trust engine to calculate the total behaviour trust based on equation 7.4. The total trust value will be forwarded to the access control module for decisions regarding data access.

7.5 Evaluation of Trust Algorithm

The user behaviour trust algorithm is evaluated based on numerical analysis in MATLAB [83] to check and show how the total trust value of users vary given different users' be-

[3]The arithmetic mean is used as a good measure of central tendency, compared to $\alpha = \beta = 0.5$.

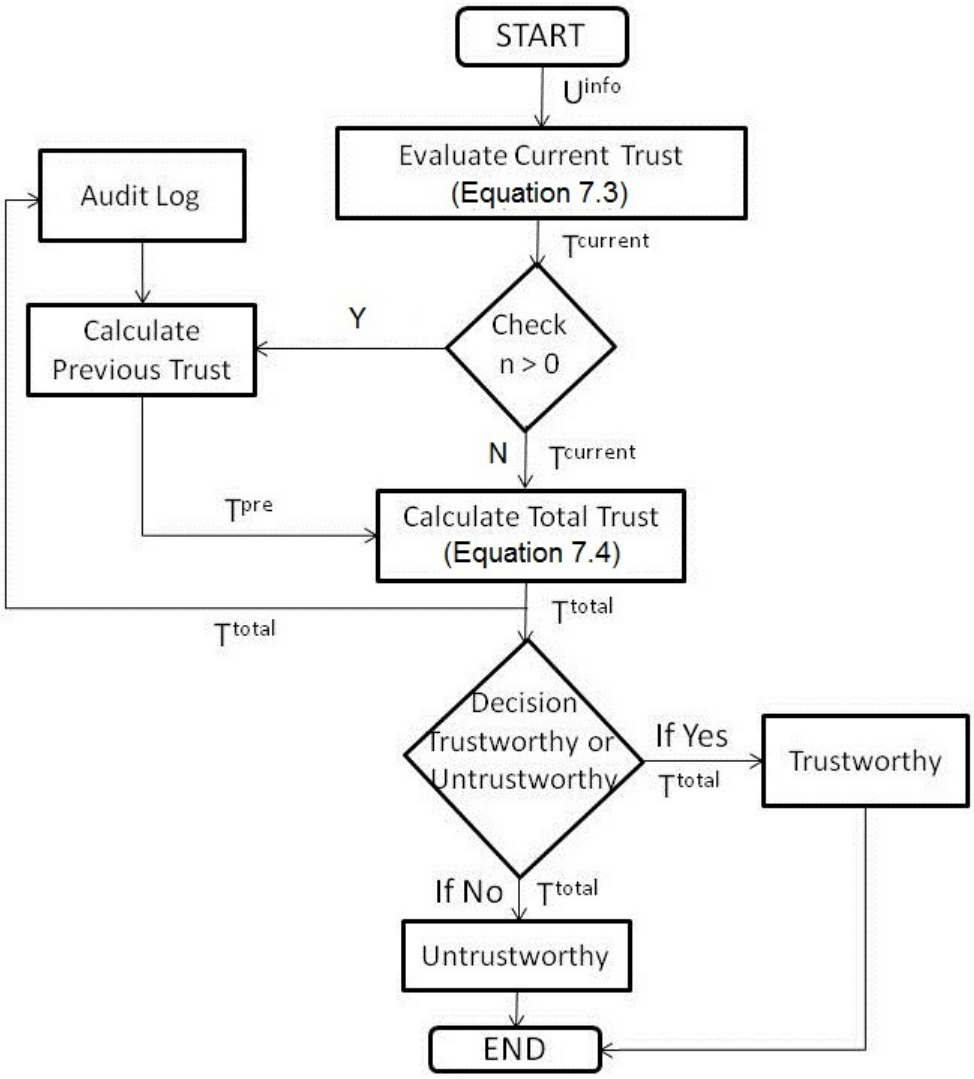


Fig. 7.2 Flow Chart of the Trust Model

haviour information or attributes. The trust algorithm is calculated with random variables[4] that represent the trust value of three different attributes such as trust value for location, users' role and time range. Random variables are useful when solving and complex problems related to probability (whether the users can be trusted or not trusted). The trust algorithm can be seen as follows:

Calculate Total Trust (T^{total}, T^{cur}, T^{pre}, T^{Lo}, T^{Ro}, T^{Ti}, α, β)
U^{info} = Current User Information
T^{total} = Total Trust Value

[4] A random variable is a process that assigns values of an attribute to different cases.

T^{pre} = Previous Trust Value
T^{cur} = Current Trust Value
T^{Lo} = Trust Value for Location
T^{Ro} = Trust Value for User's Role
T^{Ti} = Trust Value for Time Range
α and β = Constant Weighting Factor ($0 \leq \alpha, \beta \leq 1$)
For T^{Lo},
T^{Lo_u}= randi(4,1,10);
For T^{Ro},
T^{Ro}= randi(4,1,10);
For T^{Ti},
T^{Ti}= randi(4,1,10);
For Current Trust (T^{cur}),
$T^{cur}(n) = \sqrt[3]{T^{Lo} * T^{Ro} * T^{Ti}}$
For Total Trust (T^{total}),
if $T^{pre}(n)$ = NA,
$T^{cur}(n) = T^{total}(n)$
Return $T^{total}(n)$;
else $T^{pre}(n) = T^{total}(n-1)$;
$T^{total}(n) = (\alpha * T^{cur}(n)) + (\beta * T^{pre}(n))$
Return $T^{total}(n)$;

Figure 7.3 shows the numerical analysis of trust algorithm based on users' behaviour pattern in MATLAB. The green line presents the previous trust value of the user and the red line represents the total trust value of the users. The blue line represents the current behaviour trust of the user; the black lines represent the trust value of three different attributes such as location; user's role; and user's time range. These attributes were simulated by using the "randi" [83] function based on uniformly distributed pseudo-random integers to generate the random integers. This function generates different variables that are used as the defined trust value for location of user, value for location of targeted object, value for user's role and value for time range, for the current trust evaluation. "randi(4,1,10)" represents the numerical number between 4 to 1 for the transactions (10). Therefore, it shows that the current trust value of a user varies based on the dynamic changes of his or her behaviour information. Overall, it shows that the trust value of users can be evaluated and calculated based on highly dynamic characteristics of their behaviour information. Additionally, Fig-

ure 7.3 demonstrates that the total trust value of a user does not only rely on the current trust value that evaluate based on the users' behaviour information from recent transaction but also depends on the previous trust values.

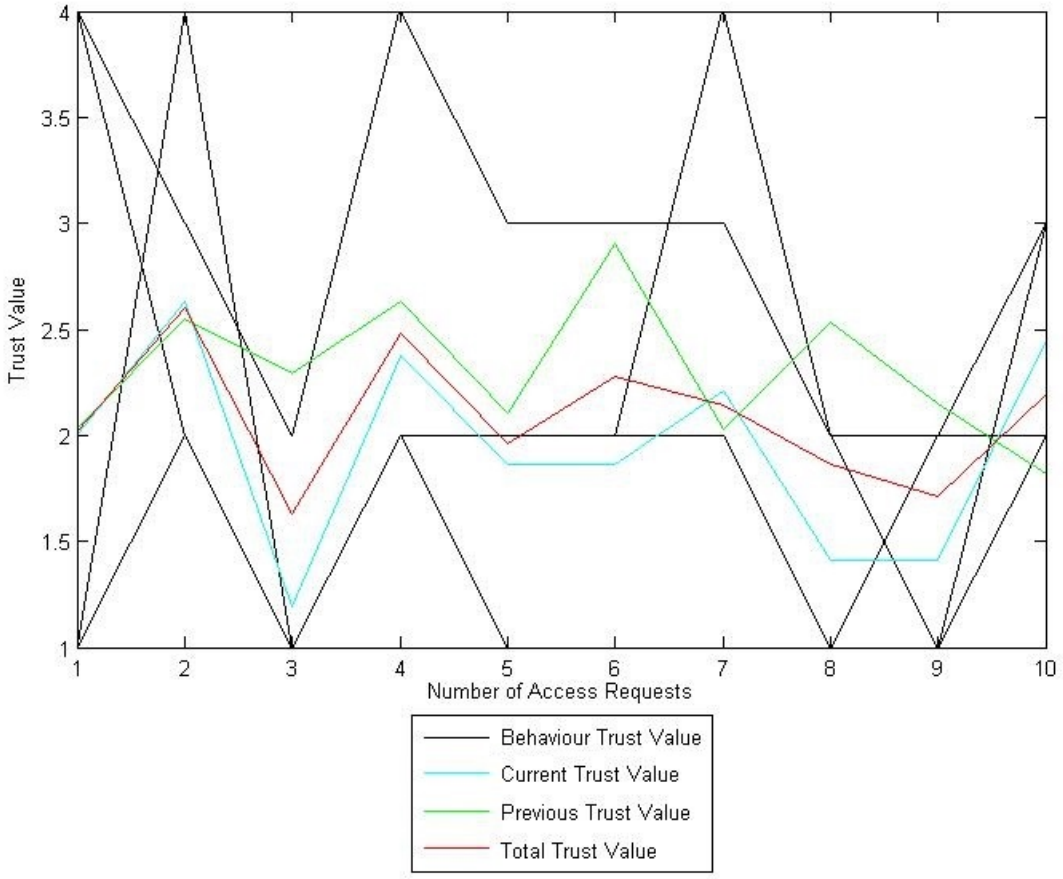


Fig. 7.3 Behaviour Trust Evaluation

7.6 Conclusion

This chapter discussed a simple user behaviour trust model with figures and diagrams. The proposed model is developed and designed based on the geometric mean and weighted running average to calculate the trust value of the user. The results obtained from the evaluation of trust algorithms based on numerical simulation in MATLAB show that the trust value of the users can vary based on the current users' behaviour information and the previous trust value. The proposed model is developed to cooperate with access control engines and to

be used as one of the policy evaluation criteria for making access decisions effectively and dynamically. The proposed model is designed based on the user behaviour information (such as location, role and time) that can be easily obtained from any data access request. This means that, there is no essential requirement regarding the behaviour information or attributes and it can be easily adapted in current access control engines. Additionally, the introducing of trust model in access control engines can help to address the conflict between data privacy and data availability because only the trusted users can get the restricted access in emergency and unanticipated situations. Therefore, we extend the adaptive access control model with prevention and detection mechanism from chapter 6 with the proposed behaviour trust model to create the Trust-Based Adaptive Access Control Model (TBA^2C) that will be explained in the following chapter.

Chapter 8

TBA^2C: A Trust-Based Adaptive Access Control Model

8.1 Introduction

In the healthcare industry, patients are expected to be treated in reasonable time and any loss in data availability can result in further decline in the patient's condition or can even lead to death. Therefore, the availability of data is usually more important than security concerns. The overwhelming priority is to take care of the patient, but the privacy and confidentiality of that patient's medical records cannot be neglected. In current healthcare applications, there are many problems concerning security policy violations in the real world environment. Additionally, we cannot assume that all the users are trustworthy enough to give a flexible access in both defined and emergency situations because there is no facility to detect abnormal data access from authorised users in current Wireless Sensor Network (WSN) access control models. Some WSN access control models address data availability issue for emergency situations but the privacy of the patients' information has been neglected.

To address the above issues, Trust-Based Adaptive Access Control (TBA^2C) is proposed which is an extended version of the model proposed in chapter 6 incorporating the simple user behaviour trust model from chapter 7. TBA^2C is aimed at protecting the privacy of the users' information and the privacy of the patients' information allowing only trusted users to have a restricted access in emergency and unanticipated situations. In addition, the trust value is used as an extra condition in the authorisation policy to detect abnormal data access from authorised users. Therefore, TBA^2C is an emerging concept that builds on the concepts of fine-grained access control [144], the user behaviour trust model, the prevention

and detection mechanism, and the possibility-with-override concept to provide a flexible policy that is not too permissive nor too strict in the access control engine and to adjust the access decisions effectively based on the user behaviour trust values.

Firstly, the development details of TBA^2C model are explained, followed by the simulation test scenario with its threat model. Additionally, a medical application is developed to evaluate and verify the proposed TBA^2C model. Finally, this chapter concludes with further suggestions.

8.2 A Trust-Based Adaptive Access Control Framework

Trust-Based Adaptive Access Control (TBA^2C) integrates the concepts that have been introduced in the previous chapters to provide a flexible approach in the access control engine and to address the conflict between data availability and data privacy in WSNs. The proposed model has incorporated the concepts of the possibility-with-override [110] into WSNs for hard-to-define and unanticipated situations. Possibility-with-override means users may be able to override the denial of access when unanticipated situations occur. It is combined with the simple user behaviour trust model to enforce access decisions effectively and efficiently at the access control engine. The user behaviour trust model is employed to evaluate the total behaviour trust value of the users based on their role, department, time, etc. The trust value is used as one of the policy evaluation criteria in the access control engine.

There are three main modules in TBA^2C: Policy Enforcement Point (PEP), Policy Decision Point (PDP) and the user behaviour trust module. The overview of TBA^2C can be seen in Figure 8.1. In the TBA^2C model, PEP has the same properties as the previous models but the policy definitions in the access control module are different because the trust value is introduced and used as one of the policy evaluation criteria. A brief discussion of the access control module and the user behaviour trust module comes next.

8.2.1 Access Control Module

The access control module is the main module in the proposed TBA^2C model. All the defined access policies such as authorisation, obligation and overriding are integrated with that module. An effective access decision can be made in any circumstances based on the defined access policies and user behaviour trust value.

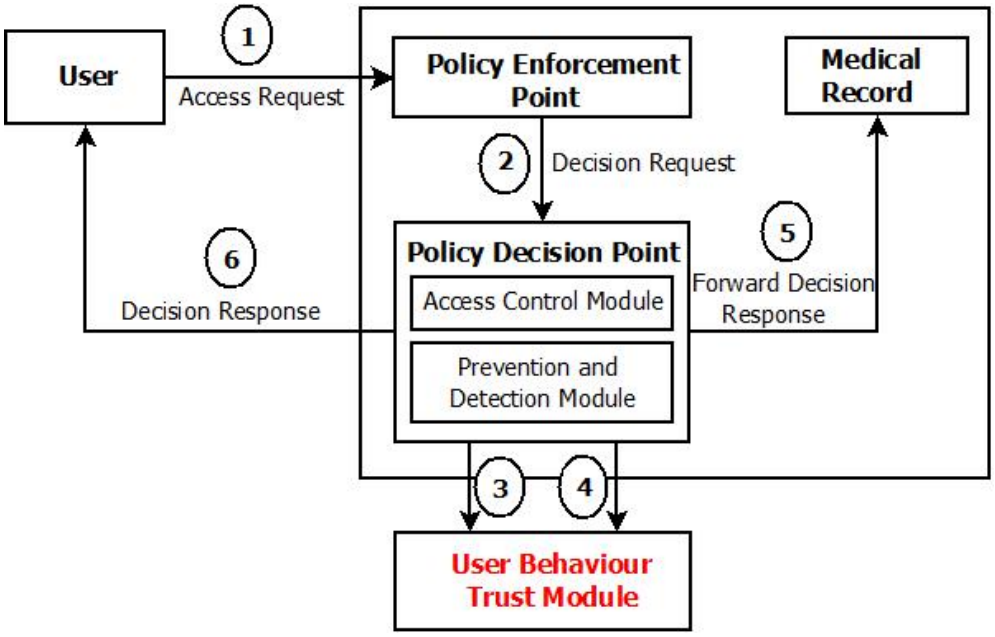


Fig. 8.1 Overview of the TBA^2C Model

- **Authorisation Policy** Authorisation policy is used for normal permitted and denied access in the proposed model. An example of authorisation policy is shown below:

Def: Permit-Policy
subject nurse
action read
target ob_2
condition department = Cancer
and time is between 9am to 17pm
if trust value is < 2.5
call obligation policy

The above permit-policy adds an extra condition (trust criterion) to detect abnormal data access from authorised users. It defines the nurse from "Cancer" department has the right to access the medical record of patient from the same department (ob_2). Unlike the previous models, the trustworthiness value of the user is checked as additional condition in the authorisation policy. The nurse still has an data access even if his trust value is lower than defined value but the system assumes an abnormal data access and performs a course of action by activating the obligation policy.

- **Obligation Policy**

  An obligation policy is used in some situations to perform a course of action alongside the authorisation decision.

  Def: Obligation-Policy
  Target Em_{log}
  if policy type is override
  do write.audit < subject, Time, Target, Behaviour Trust Value, Department, Decision Outcome >
  and Trigger-alarm
  and Notification Message

  Based on the above policy, if there is an overriding process, the obligation policy becomes active and keeps the user information as an audit log and some actions such as triggering an alarm and sending notification message to administrator are performed.

- **Overriding Policy**

  An overriding policy checks conditions for the decision-making process at the access control module. To override the denial of access, the subject has to meet the following policy criteria:

  Def: Overriding-Policy
  subject nurse
  action read
  target ob_1
  condition trust value is $\geq$ 2.5
  and department = Heart
  and time is between 9am to 17pm
  call Obligation-Policy

  Regarding the above policy, a nurse from "Heart" department may access the medical record of a patient from "Cancer" department (ob_1) but he needs to meet conditions such as trust, department and time to override the denied access. An important factor is that the user behaviour trust value has to be equal or higher than the defined value which is 2.5 to override it. Alongside the authorisation decision, the obligation policy will be activated whether the access has been granted or denied.

8.2.2 User Behaviour Trust Module

A user behaviour trust model from the previous chapter is used in the TBA^2C model. This module uses current user information and previous trust values to calculate the user trustworthiness value from the system perspective. The current trust value is obtained from the user's current access request to an object, such as user's role, department, time and targeted objects. The total trust value of the user is stored in a log as the previous trust value for the user's next attempt. The trust value is not only used in the overriding process but also in the normal authorisation process to detect abnormal data access from authorised users.

8.3 Simulation Test Scenario

A medical application is developed to show how the proposed model is fit and how the policy evaluation is done for overriding access based on user behaviour trust value and other information. The simulation test scenario for this TBA^2C is the same as in the previous chapters. The main difference is that the trust value is used in the decision-making processes.

Figure 8.2 expresses the overview diagram of how to apply the TBA^2C model in healthcare applications for Body Sensor Networks (BSNs) and WMSNs. Based on Figure 8.2, the step-by-step process of user access to the targeted object is explained as follows:

1. A user sends an access request to the targeted object in the system.

2. PEP authenticates the user and forwards users' attributes to a user behaviour trust module. Simultaneously it sends a decision request to PDP for decisions regarding data access.

3. The user behaviour trust module calculates the trust value of the user based on current trust and previous trust. Thereafter, it sends the behaviour trust value to PDP. We assume that the behaviour trust module is deployed in another sensor node that is centrally located to calculate the trustworthiness value of the users.

4. PDP calls the access control engine and passes through the details (such as the requested operation, the targeted object, the contextual information and the behaviour trust value) to make decisions regarding data access.

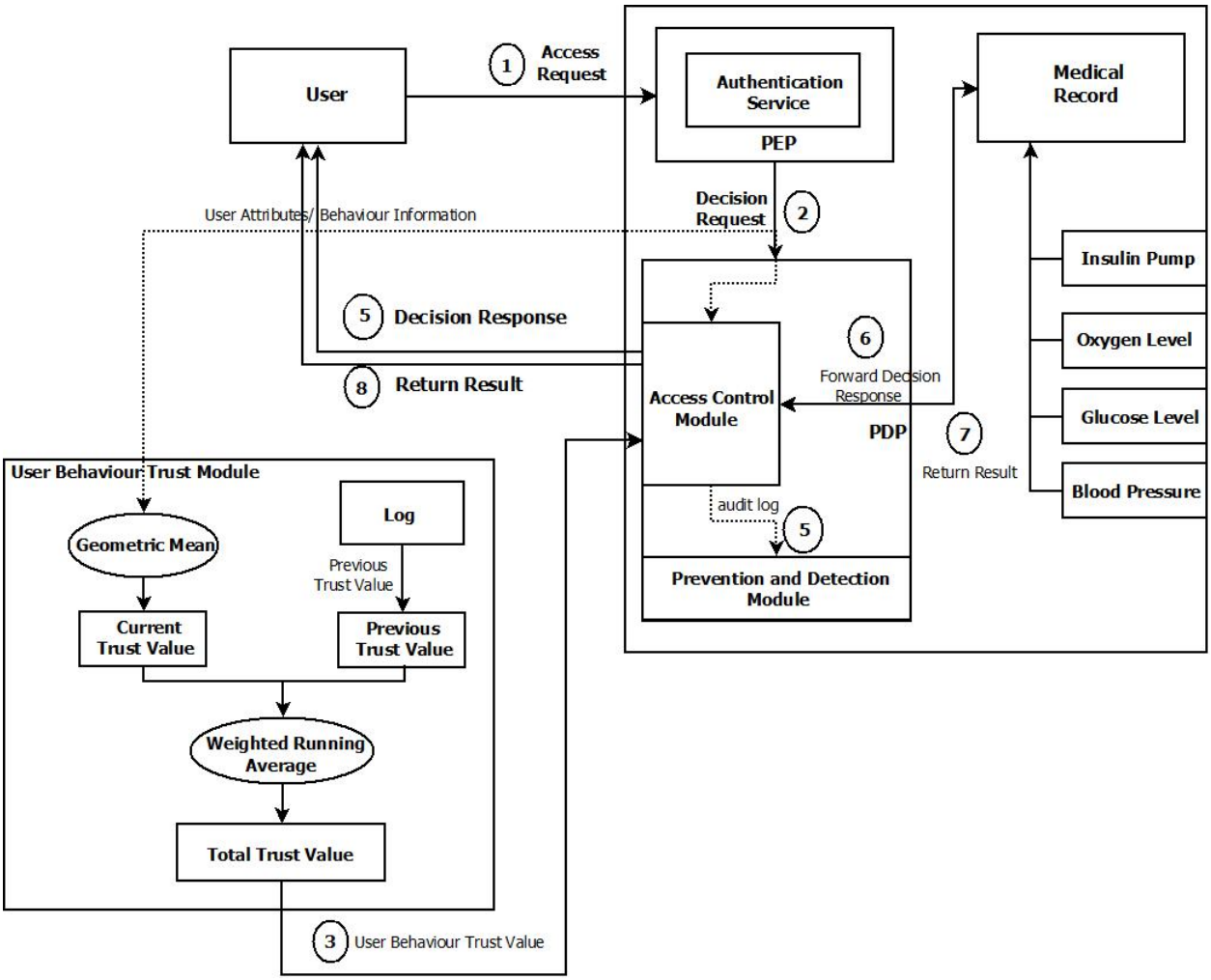


Fig. 8.2 Overview of TBA^2C with Medical Application in Body Sensor Network

5. The access control engine returns permitted access or permitted access with obligation or permitted access with overriding and obligation; (or denied access or denied access with overriding and obligation, in which case a denied message is sent from PDP to the user and the request terminates here).

6. PDP forwards the decision response to the targeted object.

7. The targeted object returns the results.

8. PDP returns the results to the user.

The following policies in Table 8.1 are identified and developed to evaluate the proposed model. In table 8.1, "ob_1" represents the medical record of a patient from "Heart" department and "ob_2" is the medical of the patient from "Cancer" department. "$Oblg_1$" performs a

Policy	**Role**	**Department**	**Time**	**Condition**	**Operation**	**Oblg**	**Object**
1	Doctor	Heart	Any	N.A.	read	N.A.	ob_1
2	Doctor	Heart	Any	N.A.	read	N.A.	ob_2
3	Nurse	Heart	Any	N.A.	read	N.A.	ob_1
4	Nurse	Cancer	Any	N.A.	read	N.A.	ob_2
5	Doctor	Heart	Any	(if T $<$ 2.5)	read	$Oblg_1$	ob_1
6	Doctor	Heart	Any	(if T $<$ 2.5)	read	$Oblg_2$	ob_2
7	Nurse	Heart	Any	(if T $<$ 2.5)	read	$Oblg_1$	ob_1
8	Nurse	Cancer	Any	(if T $<$ 2.5)	read	$Oblg_1$	ob_2
9	Nurse	Heart	9am $\leq$ and $<$ 17pm	(if T $\geq$ 2.5)	override^{read}	$Oblg_2$	ob_2
10	Nurse	Cancer	9am $\leq$ and $<$ 17pm	(if T $\geq$ 2.5)	override^{read}	$Oblg_2$	ob_1
11	Admin	Audit	Any	N.A.	read	N.A.	Ac_{log}
12	Admin	Audit	Any	N.A.	read	N.A.	Em_{log}

Table 8.1 Example of Defined Policy

course of action (Sending Notification Message) but for "$Oblg_2$", courses of actions (Sending Notification Message and Triggering Alarm) are performed. "T" represents the trust value of a user. In Table 8.1, policy 1, 2, 3 and 4 have the same definitions as the previous chapters. In policy 5, 6, 7 and 8, an additional condition (trust criterion) is added in policy 1 to 4 to detect abnormal data access from authorised users. Simultaneously, the obligation policy is activated when the user trust value is lower than 2.5 but the users can still access the medical record.

In policy 9, the nurse from "Heart" department is not allowed to access the medical data (ob_2) of patient from another department (Cancer) unless the nurse overrides the access policy for emergency data access. If his behaviour trust value is higher than or equal to 2.5, the nurse's overriding will be successful and the restricted access will be granted to him. Otherwise, his restricted access will be denied. In either case, the obligation policy will be activated to take a course of action. Policy 10 is for the nurse from "Cancer" department for the overriding process. The administrator from "Audit" department can easily check both access and emergency log to detect security policy violations and abnormal data access

regarding policy 11 and 12.

8.4 Threat Model

The attacker-centric based threat model [87] is respected and commonly used. Defence strategy is of course, improved if there is a reasonable understanding of how attackers think. By thinking like attackers and being aware of their likely tactics, the system can be more effective when applying countermeasures[1]. Several threats that can be faced in the applications can be categorised based on the goals of the attacks. Knowledge of these threats can help to organise a security strategy and might be able to help plan responses to these threats. In this section, the threat model is categorised based on STRIDE [86]. We analysed the STRIDE model in the medical scenario as follows:

- **Spoofing**: Spoofing is attempting to gain access to a system by using a false identity. This can be accomplished using stolen user credentials or false information. After the attacker successfully gains access as a legitimate user, elevation of privileges can begin. Example: A nurse pretends to be a doctor.

- **Tampering**: Tampering is the unauthorised modification of data but we did not address it explicitly in this dissertation. Same considerations apply to write as to read. Example: A nurse or doctor edits the medical record of a patient illegitimately.

- **Repudiation**: Repudiation is the ability of users to deny that they performed specific actions. Without adequate auditing, repudiation attacks are difficult to prove. The issue of repudiation is concerned with a user denying that he performed an action. The defence mechanism is needed in place to ensure that all user activity can be tracked and recorded. Lack of auditing and logging of changes made to data threatens the ability to identify when changes were made and who made those changes.
  Example: A nurse denies that he has edited the medical record.

- **Information disclosure**: Information disclosure is the unwanted exposure of private data. Sensitive data need to be stored securely to prevent a malicious user from gaining access to and reading the data. The disclosure of confidential data can occur when sensitive data can be viewed by unauthorised users. Only authenticated and authorised users should be able to access the data that is specific to them. Access to data

[1] A countermeasure is an action or technique that can reduce a threat and an attack by eliminating or preventing it.

Threat	Countermeasure
Spoofing	Strong Authentication (Attribute Based Encryption (ABE))
Tampering	Strong Authorisation (ABE and Access Control)
Repudiation	Audit Trials (Audit Record or Log)
Information Disclosure	ABE and Access Control
Denial of Service	Access Control
Elevation of Privilege	Access Control

Table 8.2 Possible Threats and Countermeasures

should be restricted to users.
Example: Other staff members from the hospital try to read the medical record.

- **Denial of Service**: Denial of service is the process of making system resources unavailable.
  Example: A common application layer DoS attack will send multiple simultaneous requests for data access. These requests will most likely put the access control module under DoS condition and the user will likely be unable to access the medical record.

- **Elevation of privileges**: Elevation of privilege occurs when a user with limited privileges uses the identity of a privileged user to gain access to a data resource.
  Example: A nurse tries to access restricted data by using the fault identity.

Based on the above discussion, these threats and attacks are trying to violate the security services such as confidentiality, integrity, authenticity, repudiation, etc. These threats and attacks should be protected by using security mechanisms or countermeasures. A countermeasure is a safeguard that addresses a threat and mitigates risk. Table 8.2 lists the security threats that can violate the security services and the possible countermeasures to defend against them in the proposed TBA^2C model.

8.5 Experimental Results and Discussion

Figure 8.3 shows the interface and decision outcomes of a nurse “Aung", who works as a day nurse in “Cancer” department, as observed from his path (/cancer/nurse/day/aung). Additionally, the location path for the nurse is used as the current location of the users to show that the trust value of the user can be varied based on the location and time range.

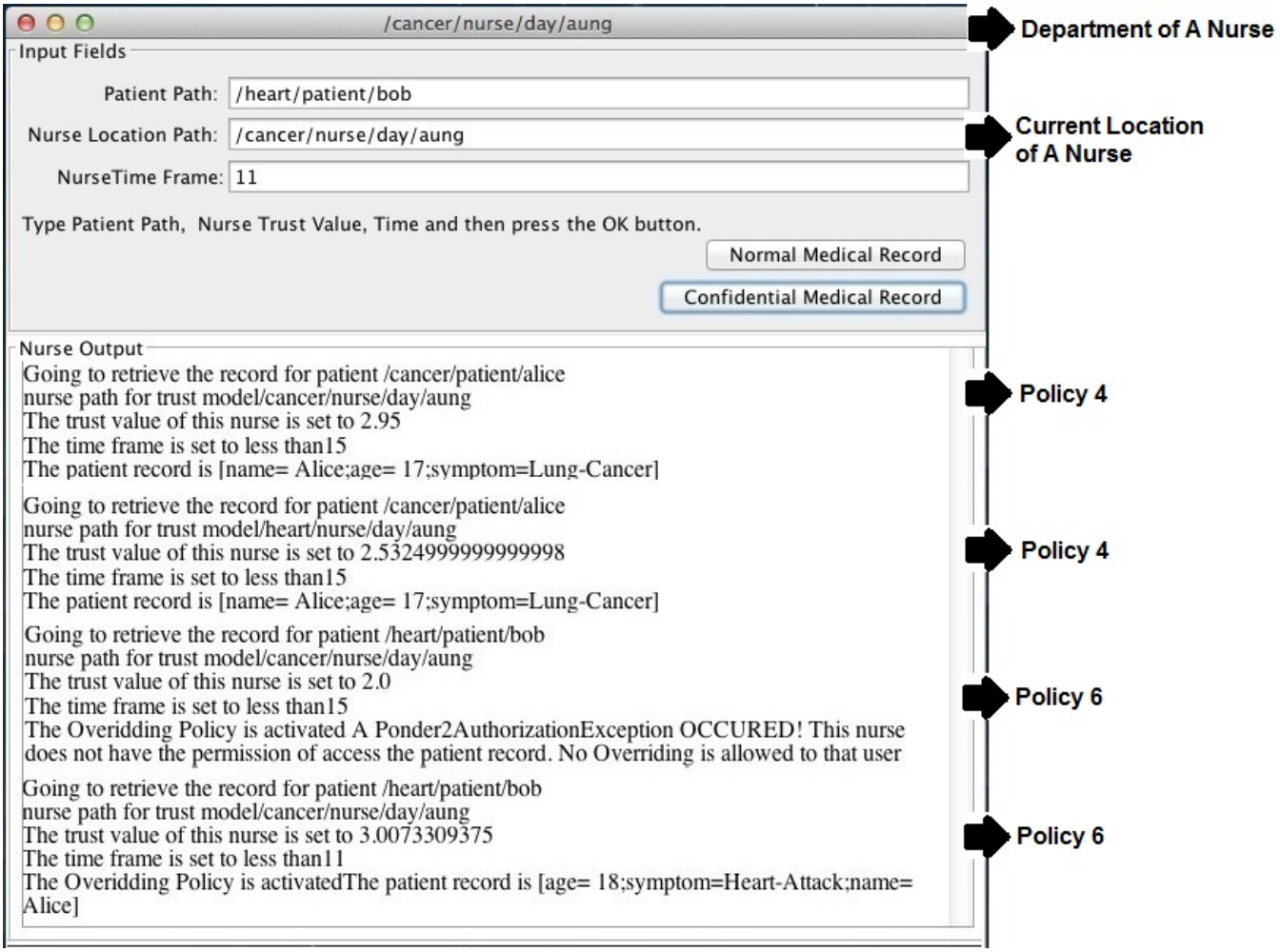


Fig. 8.3 User Interface and Decision Outcomes of a Nurse

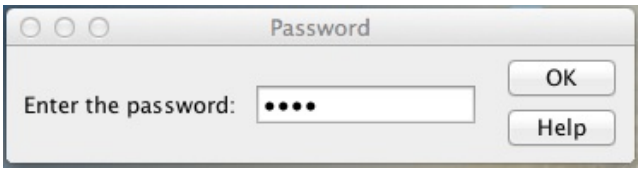


Fig. 8.4 Authentication Process for Overriding Process

In the first case, the nurse from "Cancer" department tried to access the medical data of a patient (ob_2) from his department within time range. His access was approved and his trust value was calculated and recorded (2.95) because he satisfied a normal authorisation policy. In the second case, he tried to access the same data (ob_2) but his physical location is different from where he works and the time range. The total trust value of the user is slightly decreased (2.53) from the previous case but he can still access the data because of the normal authorisation policy.

In the third case, the nurse tried to access the medical record of a patient (ob_1) from another department (Heart) but he needed to override the policy to access the data. For the overriding process, his trust value needs to be higher than 2.5, which is the defined value in the system. Regardless of these outcomes, the obligations such as the triggering of an alarm and sending of a notifying message will be activated and performed. If his trust value is not high enough, the system message will appear in the interfaces as "The nurse does not have the permission to access the medical record. No overriding access is allowed to that user". In this case, his access request is denied but the courses of action are still performed regarding auditing purpose.

In the final case, the user satisfies the defined thresholds from the overriding policy but here is an additional phase to provide further security services in the proposed model. This means that a user needs to re-authenticate to gain access to confidential medical data. The authentication interface and the confidential medical record interface can be seen in Figures 8.4 and 8.5. Overall, his access has been granted because of his behaviour trust value and contextual information as well as the authentication phase in the final case.

Figure 8.3 not only shows the interface of the nurse but also explains how the access decisions are made based on authorisation, obligation and overriding policies with the total behaviour trust value of the users.

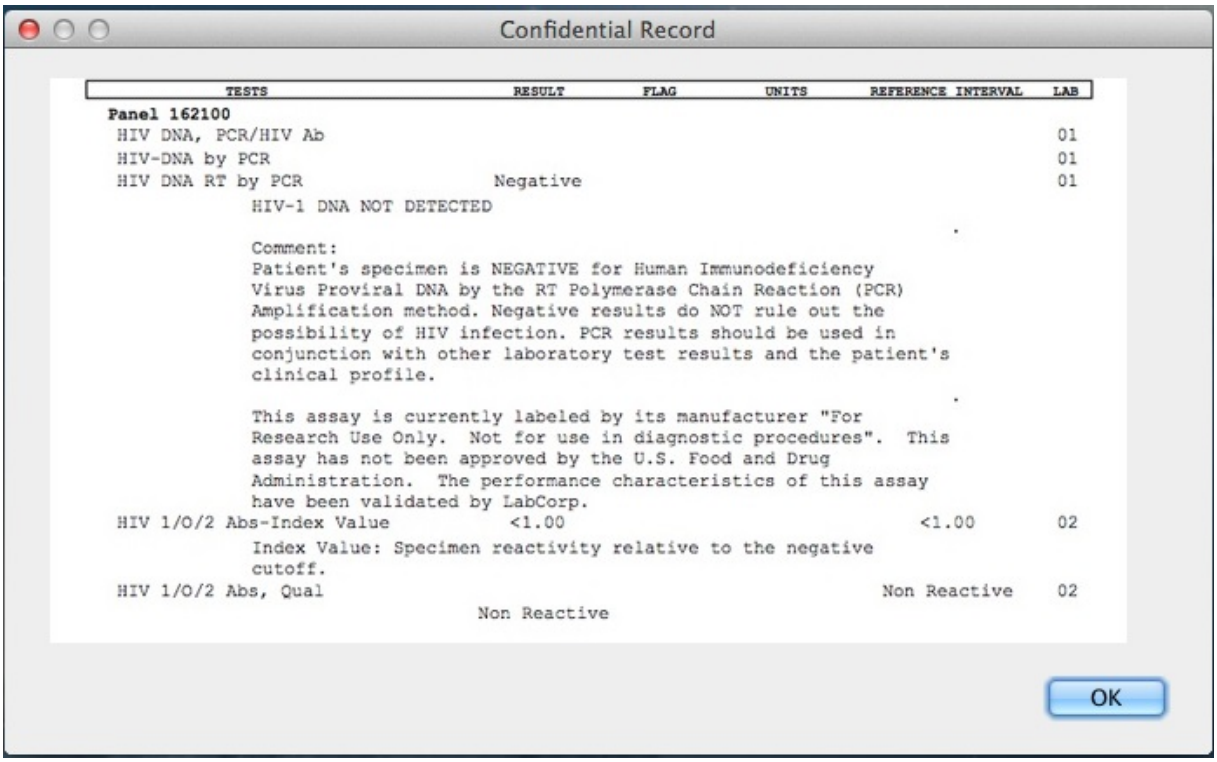


Fig. 8.5 A Confidential Medical Record

8.6 Conclusion

This chapter proposed the Trust-Based Adaptive Access Control (TBA^2C) model in which, a user behaviour trust model from the previous chapter is applied to use the trust value as one of the supporting factors for making access decisions in both authorisation policy and overriding policy. Additionally, the trust value is used in authorisation policy to detect abnormal data access from authorised users. This means that users still have access to the medical record but when the trust value is lower than defined threshold, the system assumes that it is an abnormal data access and activates an obligation policy. Regarding the decision outcomes, the features of TBA^2C model provides a flexible approach in WSNs. Therefore, the proposed TBA^2C model provides flexibility in the access control engine to enforce access decision dynamically and to address the conflict between data availability and data privacy in WSNs and WMSNs. To enable a full comparison with the proposed TBA^2C model, the Break-The-Glass Role Based Access Control (BTG-RBAC) [36] model is redesigned and developed under Ponder2, which is discussed in the next chapter.

Chapter 9

$BTG-AC$: Break-The-Glass Access Control Model

9.1 Introduction

In this chapter, a step-by-step development and an evaluation framework of Break-The-Glass Role-Based Access Control (BTG-RBAC) [36] for Wireless Sensor Networks (WSNs) is presented in order to make a meaningful comparison with the proposed Trust-Based Adaptive Access Control (TBA^2C) model because the BTG-RBAC model has a similar structure as the proposed TBA^2C model. Both models were developed and implemented in the Ponder2 package. Firstly, the core RBAC model is discussed; followed by the core Role-Based Access Control (RBAC) with obligations; and then the BTG-RBAC model. Finally, the development framework of the BTG-RBAC model for WSNs in Ponder2 is presented. Some modifications have been made on the BTG-RBAC model to fit the requirements of WSN applications. The modified model has been named Break-The Glass Access Control ($BTG-AC$).

9.2 A Core Role-Based Access Control Model

The American National Standards Institute (ANSI) standard core RBAC model [58] is a standard access control model. Most of the access control models in information systems are based on the core RBAC model. Before the details of BTG-RBAC are explained, some basic information about core RBAC is presented. The BTG-RBAC model is an extended version of core RBAC with some obligations. The overall picture of the core RBAC model

can be seen in Figure 9.1.

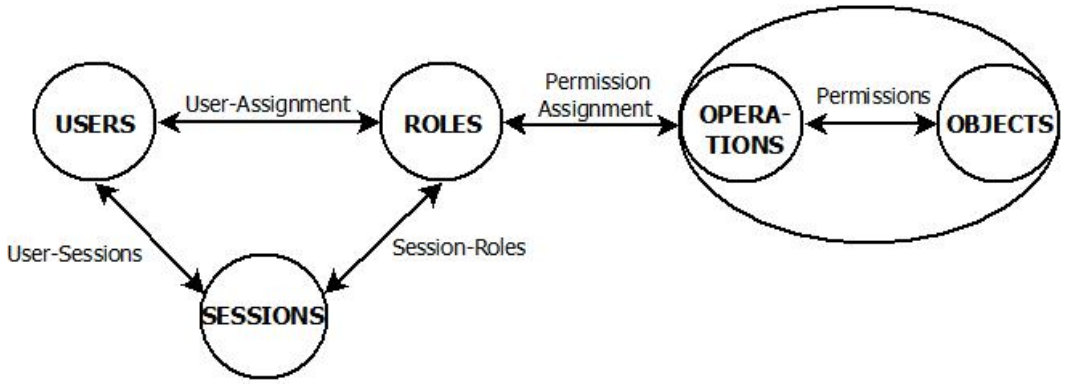


Fig. 9.1 A Core RBAC Model

The core RBAC model has five basic elements: USERS, ROLES, SESSIONS, OPERATIONS, and OBJECTS, and there are five relations between them. The five relations between these elements are explained as follows:

- User-Assignment (UA): UA $\in$ (belong to) USERS and ROLES, a many to many relations between users and roles
- User-Sessions (US): US (u : USERS) $\rightarrow n^{SESSIONS}$, a mapping of user (u) onto (n) sessions
- Session-Roles (SR): SR (s : SESSIONS) $\rightarrow s^{ROLES}$, a mapping of session (s) onto a set of roles
- Permission-Assignment (PA): PA $\subseteq$ (subset of) Permissions and ROLES, a many to many relation between permissions and roles
- Permissions (PRMS): PRMS $\rightarrow p^{(OPERATIONS)and(OBJECTS)}$, the mapping between permission and operations which gives a set of operations (ops) associated with the permission p, (p : PRMS) $\rightarrow$ (ops $\subseteq$ OPERATIONS) and the mapping between permission and objects which gives a set of objects associated with permission (p : PRMS) $\rightarrow$ (ob $\subseteq$ OBJECTS)

The authorisation decision is made within the core RBAC model based on the inputs of the current session, the requested operation and the targeted object. A result indicates

whether the user request is authorised or not and it returns Boolean Value as a return value. The equation of a decision-making process in core RBAC is explained as follows:

$$Access : SESSIONSxOPERATIONSxOBJECTS \rightarrow Boolean \tag{9.1}$$

The Access(s,op,ob) function is equivalent to:

$$\exists r \in ROLES : r \in SR(s) \bigwedge((op, ob), r) \in PA \tag{9.2}$$

This means that if a role (r) is mapped from the current session (s), that role (r) is allocated the permission to perform the operation (op) on a targeted object (ob). If a value exists in predefined roles, the function will return TRUE for permitted access and FALSE for denied access as a boolean.

The step-by-step process of user access to the targeted object with the core RBAC model is explained as follows:

1. A user sends an access request to the targeted object in the system.
2. The system authenticates the user.
3. The authentication service returns the authenticated identity of the user.
4. The system calls the RBAC policy engine and passes through the session details, the requested operation and targeted object (9.1).
5. The RBAC engine returns GRANT; (or DENY, in which case a denied message is sent from the system to the user and the request terminates here).
6. The system makes the requested operation to resource in the targeted object.
7. The targeted object returns the results.
8. The system returns the results to the user.

9.3 A Core Role-Based Access Control Model with Obligations

In this model, a new basic element OBLIGATIONS (OBLGS) [151] is introduced to the core RBAC. All of the basic five elements of the core RBAC function the same as in section

9.2. There are some changes in the core RBAC model because of the new element OBLGS. The overall diagram of the core RBAC with obligation model is shown in Figure 9.2.

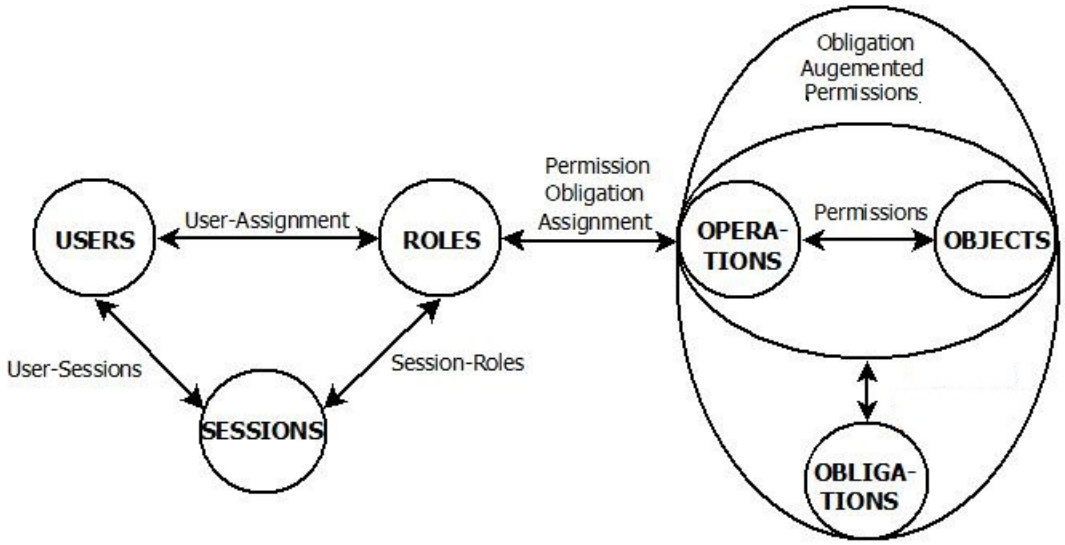


Fig. 9.2 A Core RBAC with Obligations [151]

The relation and mapping between OPERATIONS and OBJECTS has been replaced from Permission to Obligation Augmented Permissions (OPRMS), which is defined as follows:

OPRMS = PRMS x OBLGS

At the same time, the Permission-Assignment (PA) is changed to Permission-Obligations Assignment (POA) because of the new element OBLGS. The POA definition is expressed as follows:

POA $\subseteq$ OPRMS x ROLES

oprm $\in$ OPRMS is equivalent to oprm = (r, prm, oblgs). This means that if the permission (prm) is allocated to role (r) through obligation-augmented permission (oprm) which is exercised by role (r), the obligations (oblgs) will be triggered. The obligations will be used along with the authorisation decision. Therefore, the decision-making process (Access

function) will be enhanced to:

$$Access : SESSIONSxOPERATIONSxOBJECTS \rightarrow BooleanxOBLGS \tag{9.3}$$

The possible results for the decision-making process (Access function) are explained as follows:

- (TRUE) $\rightarrow$ Permitted access to an object.
- (TRUE, OBLGS) $\rightarrow$ Permitted access to an object and perform the obligation along with authorisation decision.
- (FALSE) $\rightarrow$ Denied access to an object.
- (Flase, OBLGS) $\rightarrow$ Denied access to an object and perform the obligation along with authorisation decision.

The step-by-step process of user access to the targeted object with the core RBAC with obligations are the same as with the core RBAC model, which was already discussed in the previous section. The added process to the core RBAC model is performing and retrieving the obligations, if they exist in the predefined roles of the system.

9.4 Break-the-Glass Role-Based Access Control

The BTG-RBAC model is an extended version of the core RBAC with obligations by adding Break-The-Glass (BTG) functionality [37] within the RBAC engine. Ferreira [36] introduced the BTG-RBAC engine to integrate BTG in the core RBAC model. The overview diagram of the BTG-RBAC model can be seen in Figure 9.3.

Based on Figure 9.3, there is an additional element called BTG. The relations between elements have changed in the BTG-RBAC model. The Permission Obligation Assignment (POA) from core RBAC with obligation is modified to POA-BTG in BTG-RBAC. Also there is another relation between permissions (PRMS) and BTG namely PRMS-BTG = OPRMS x BTG. A new modified relation (POA-BTG) is expressed as follows:

POA-BTG = PRMS-BTG x ROLES

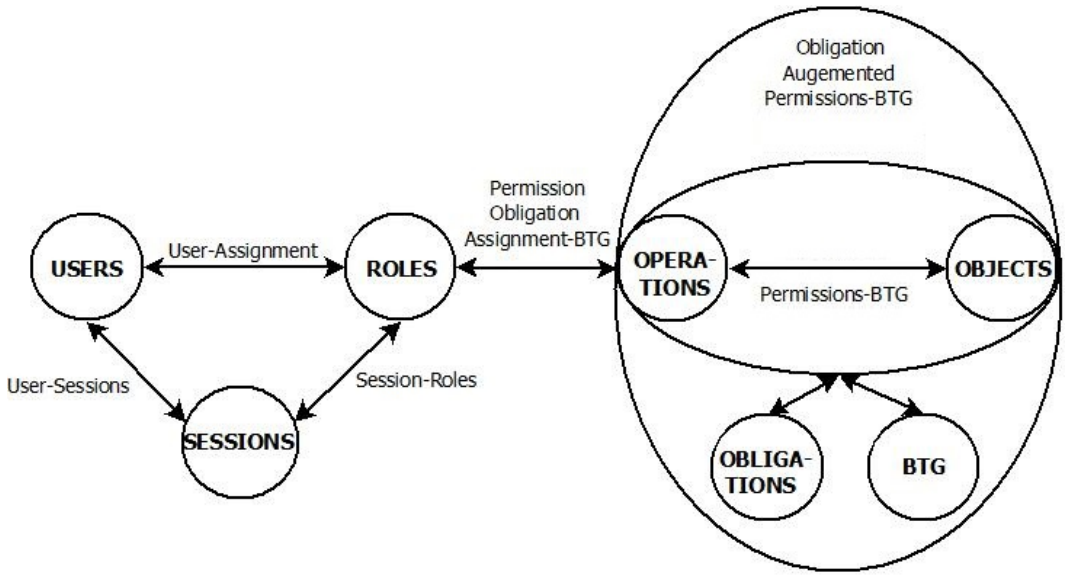


Fig. 9.3 A BTG-RBAC Model

Also the relation OPRMS is used in BTG-RBAC model where:

$$OPRMS \subseteq OPRMS-BTG \& OPRMS-BTG \subseteq PRMSxBTGsxOBLGS \tag{9.4}$$

The essential property of the BTG-RBAC model is that the BTG state variable of the permission can be set to “TRUE” or “FALSE” depending on the predefined role, but initially it starts with a “FALSE” state. The state can be “TRUE” when there is a policy that allows the user to perform a BTG operation on a targeted object. To perform the BTG operation, the new roles describing who is allowed to perform the BTG operation on the targeted object are added. The obligations are added to the BTG operation ($O^{BTG(op)}$) permission that allow the administrator to define some actions to perform when the "glass is broken".

BTG state variables require a service that can reset “TRUE” to “FALSE”. It can be done automatically and manually. Automatic resetting means that the access control engine itself resets the BTG state variable to “FALSE” after a specified event has occurred but this event must be specified by the administrator when creating the BTG policy. Based on Table 9.1, the event could be the expiration of a time period such as 30 minutes or after an access request has been made while the BTG state was “TRUE”. Automatically resetting the BTG state to “FALSE” controls availability of a resource once the “the glass has been broken” before additional access can be granted. Manually resetting means that human intervention must occur before the BTG state is set from “FALSE” to “TRUE” after the access has been

granted.

Role	**Operation**	**Object**	**Condition**
r^1	Read	ob^1	30mins
r^2	Reset	BTG State	

Table 9.1 Example of BTG State Variables

Based on the above discussion, the BTG-RBAC model is considered to provide data availability in emergency situations and it is also aimed at E-Health applications in general wireless and wired networks. The BTG-RBAC model is implemented in PREMIS [106] with MySQL [139] database but it is not suitable to use in WSNs because PREMIS must be supplemented by metadata that can record detailed technical attributes of specific object types or media and hardware, and it is difficult to automate creation of metadata structures at present. Therefore, a modified version of BTG-RBAC is developed and implemented in order to fit in WSNs.

9.5 $BTG-AC$: A Break-The Glass Access Control Model in Ponder2

Based on the requirements of WSNs, the framework of the BTG-RBAC model was modified and redesigned to function in WSNs, we call this Break-The-Glass Access Control ($BTG-AC$), but it still has similar functions to those of the BTG-RBAC model. The main difference is that the $BTG-AC$ model has been developed and implemented within the Ponder2 policy package.

9.5.1 Limitations in Ponder2

There are some limitations when developing the $BTG-AC$ model in Ponder2.

- There is no BTG state variable in the modified version of BTG-RBAC. Instead, fixed BTG states such as “TRUE” or “FALSE” are used in the modified version of BTG-RBAC.

- The BTG state is set up "TRUE" for some access control policy to perform the BTG action. Additionally the administrator can change or modify the BTG state for a new policy or existing policy.
- It is assumed that the authentication process is already provided in PEP because there is no user log in process in the modified version of BTG-RBAC.

Apart from these limitations, the BTG-RBAC model was developed and implemented in Ponder2. The decision-making process will be different for each user. Some users may be able to access data without the BTG option. Some may have the BTG option to access the data resource but the obligations, which have the same functionality as section 9.3, such as notifying the manager, triggering an alarm and writing to an audit must be performed when the users perform the BTG action. Additionally, the prevention and detection mechanism discussed in chapter 6 is added in the $BTG-AC$ model to detect security policy violations.

An overview of $BTG-AC$ in the Ponder2 framework can be seen in Figure 9.4. There are two main modules in the $BTG-AC$ model: Policy Enforcement Point (PEP) and Policy Decision Point (PDP). User requests will go through PEP and all the user information will be forwarded to PDP for the decision-making processes the same as in the previous models. The main difference is that the BTG policy is developed in the access control module.

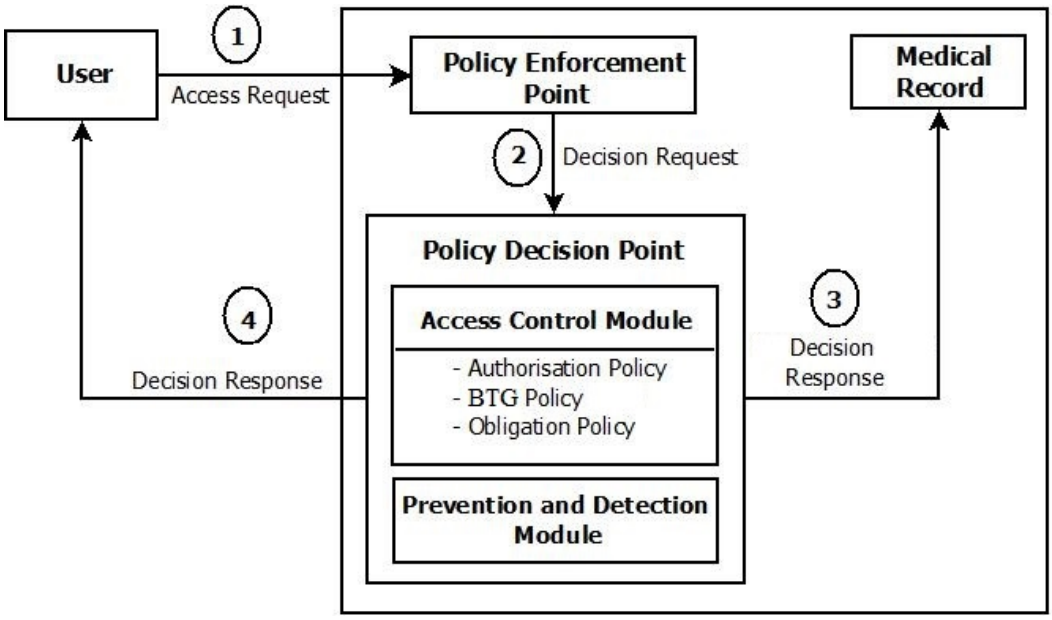


Fig. 9.4 A $BTG-AC$ Model

9.5.2 Access Control Module

The access control module is used to enforce the policies for the decision-making process. In the access control module, there are three different policies: authorisation, BTG and obligation policy. In the $BTG-AC$ model, BTG and the obligation policies are introduced to make access decisions in normal as well as emergency situations. In normal access control models, the decision outcomes will be either permitted access or denied access. The existing decision outcomes are extended in $BTG-AC$ as follows:

- (Permit, $\emptyset$) $\rightarrow$ A user has permission to access the targeted object.
- (Permit, OBLGS) $\rightarrow$ A user is allowed to access the targeted object but an obligation is performed when the access is given.
- (Deny, $\emptyset$) $\rightarrow$ A user request to access the targeted object is denied.
- (Deny, OBLGS) $\rightarrow$ Alongside a denied access, some obligations are performed.
- (Permit, BTG * OBLGS) $\rightarrow$ A user's request for access has been granted by performing BTG action and obligations such as "Write to Audit", " Trigger the Alarm" or "A Notification Message" are performed along with the access decision.

Based on the above decision outcomes, it is clear that the introduction of BTG and obligation policy is beneficial for healthcare applications in WSNs. The following section will explain the definition of the BTG policy and the obligation policy. The definition of authorisation policy is the same as in chapter 6.

Break-the-Glass (BTG) Policy

A BTG policy is used to perform a BTG operation on a targeted object. To perform the BTG operation, the new policy is added that describes who is allowed to perform a BTG action for the targeted object, for instance, a confidential medical record of the patient in an emergency but some obligations will be triggered and performed at the same time. The administrator defines the BTG policy for each situation where the BTG action is required by users in an emergency situation. An example BTG policy can be seen as follows:

Def: BTG Policy
subject Nurse
target ob_3
action Read

condition BTG state = TRUE
call Obligation Policy

Based on the above policy, it allows a user to access confidential data (ob_1) even if he does not have the access right but BTG state variable has to be "TRUE". It is assumed that the BTG policy is already defined in advance for these kinds of situations to perform BTG action at the targeted object. If there is no BTG policy for that object, the user request will not be granted.

Obligation Policy

An obligation policy is used along with authorisation decisions in some situations. It still has the same property as section 9.3. The example of obligation policy is explained as follows:

Def: Obligation-Policy
on auditrecord
if BTG action is performed
do write.audit < subject, Time, Target, User Role >
and reset BTG state to FALSE
and notify manager

The above obligation policy is used along with the BTG operation allowing an administrator to take actions when the "glass is broken". The obligation policy is linked with the prevention and detection module to store the user information and his access request in an audit log for detecting security policy violations.

9.5.3 Access Control Policy

A medical scenario is developed under the Ponder2 package to evaluate the $BTG-AC$ model for Body Sensor Networks (BSNs) and Wireless Medical Sensor Networks (WMSNs). In the medical scenario, there are two different types of data for each patient: confidential medical records (ob_3) and normal medical records (ob_1). The access policies for users' access to these medical records will be different based on the access privileges and roles of the users. Also different security levels are required in these medical records. Tight policies might be used for confidential medical records to provide data privacy. Nevertheless, the access to even confidential data can be essential in some circumstances. For example, the doctor should be able to access the confidential medical record of a patient

when the nurse cannot but the decision can be changed to a positive decision if the nurse performs the BTG actions.

Policy	**Role**	**Operation**	**Object**	**BTG State**	**Obligations**
1	Doctor	read	ob_1	N.A.	N.A.
2	Doctor	read	ob_3	N.A.	oblg [Write to Audit]
3	Nurse	read	ob_1	N.A.	oblg [Write to Audit]
4	Nurse	$O^{BTG(read)}$	ob_3	TRUE	oblg [Notify Manager; Write to Audit; Reset BTG to FALSE]
5	Admin	$reset^{BTG}$	ob_3	N.A.	N.A.
6	Admin	read	log	N.A.	N.A.

Table 9.2 Example of BTG-RBAC policy

In Table 9.2, policy 1 states that a doctor is allowed to read object 1 (ob_1). As in policy 2, the doctor is allowed to access the confidential medical record (ob_3) but an obligation such as “Write to Audit" is activated. Policy 3 is allowed a nurse to read ob_1 but it will trigger one obligation that is “write to audit". In policy 4, the nurse is not permitted to access the confidential data (ob_3) unless he performs the BTG action in that object for emergency data access, but the BTG state variable needs to be “TRUE” meaning that BTG is enabled. Therefore, an extra BTG policy is needed for the nurse (see policy 5). Additionally, the system will perform obligations such as “write to audit" and “reset BTG variable to FALSE". This implies BTG = (TRUE or FALSE). Policy 5 is quite simple. It is allowed to reset the BTG variable to “FALSE” to “TRUE” or “TRUE” to “FALSE”. Once the BTG operation is used, the administrator needs to reset the BTG state variable of that user for the next attempt. The administrator or manager can easily check the audit log to detect any use from authorised and unauthorised users regarding policy 6.

9.5.4 Evaluation Framework Based on A Medical Scenario

In this section, user interface, BTG interface, the audit log interface for the prevention and detection module and how the access decision was made based on different access policies are presented with following screen shots.

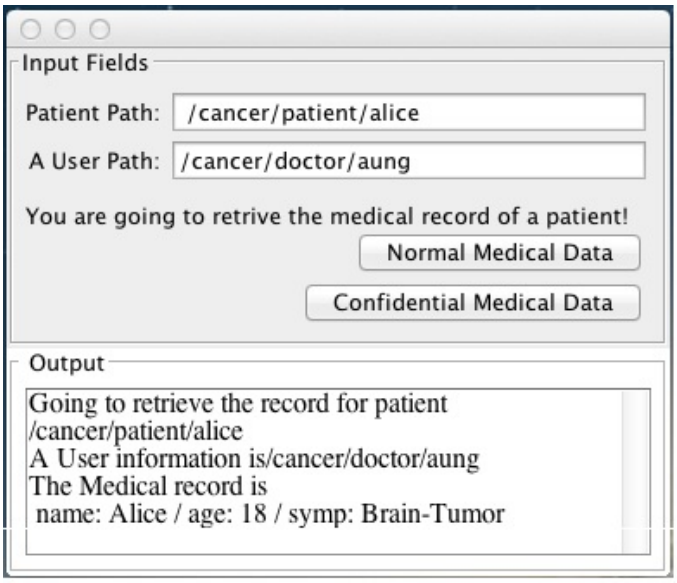


Fig. 9.5 Interface and Decision Outcomes for a Doctor

User Interface and Decision Outcomes

To evaluate the $BTG-AC$ model for medical data in WSNs, the user interfaces were developed in the Ponder2 package. Based on Figure 9.5, a doctor (Aung) tries to access the normal medical data of a patient (Alice). His access has been granted without any obligation. When he requests access to the confidential data, his requested information will be stored as an audit log to detect any security breaches of that user.

Different access policies are applied for a nurse. Figure 9.6 shows the interface of a nurse (Htoo). Based on Figure 9.6, the nurse can access the normal medical record of a patient (Alice) but one obligation action is triggered and activated when the access is given. The nurse does not have access rights to the confidential medical data unless the BTG policy is used to make an authorisation decision as in urgent or emergency circumstances. At the same time, obligations are triggered and activated. The management teams can check the audit log to prevent and detect security violations.

BTG Interface

Simple interfaces for the BTG action are developed. When a nurse wants to perform a BTG action to access patients' confidential data, the BTG interface will appear. The user's attempt to gain access will be notified to the user and his management team and necessary actions will be taken for security purpose. A confirmation message will appear twice before

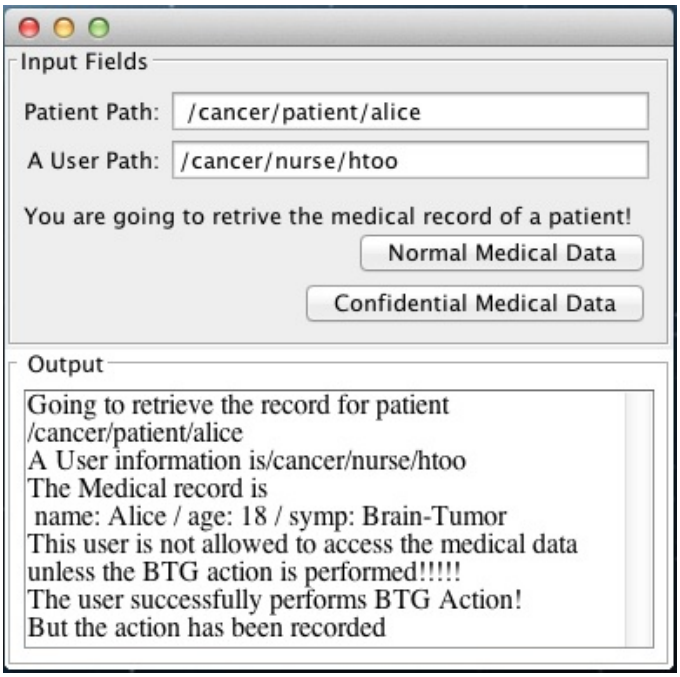


Fig. 9.6 Interface and Decision Outcomes for a Nurse

the access is given to the nurse. The interfaces for BTG action are shown in Figure 9.7.

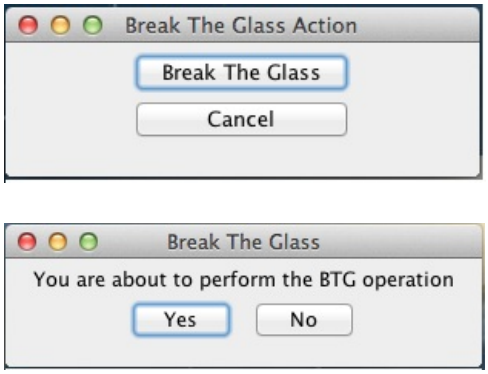


Fig. 9.7 Interfaces for BTG

Audit Log Interface

The interface of an audit log can be seen in Figure 9.8. This Figure shows what kind of information and data are stored in the audit log. The first audit log shows that the nurse accessed the normal medical record of Alice. In the second log, the same nurse requested access to the confidential medical record by performing the BTG action and his access was granted. A doctor who accessed a confidential medical record was granted access as can

be seen in the audit log of that patient. All the access requests to the medical records are recorded based on the user access requests. Based on the audit log, the management teams can check which users performed the BTG action and who among these were granted access to the confidential medical records.

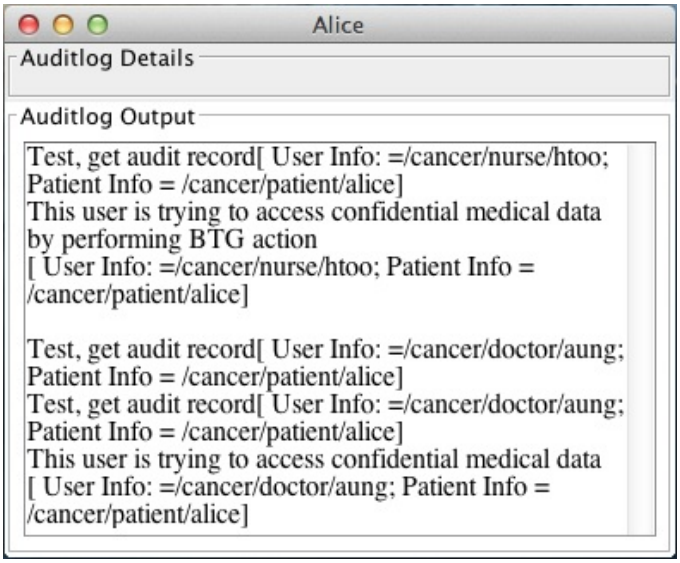


Fig. 9.8 An Interface for an Audit Log

9.6 Conclusion

The overall contributions of this chapter are the design and development of the $BTG-AC$ model for medical data in WSNs so as to allow a meaningful comparison with TBA^2C. The concepts of BTG and obligation policy can provide data availability in emergency situations. The access control module and prevention and detection module have been found to cooperate together to make an access decision and record a user's accountability for unauthorised information release from both authorised and unauthorised users. Based on the decision outcomes with a medical scenario, the BTG-RBAC model proposed by Ferreira *et al.* [37] can be applied for medical data in WSNs after some changes within the access control engine are made. A weakness of $BTG-AC$ is that a human decision is needed to predefine BTG policy for each object regarding emergency data access, unlike the TBA^2C model. A detailed comparison of TBA^2C and $BTG-AC$ is discussed in the next chapter.

Chapter 10

Comparison Between TBA^2C and $BTG-AC$ Models

10.1 Introduction

This chapter recapitulates both Trust-Based Adaptive Access Control (TBA^2C) and Break-The-Glass Access Control ($BTG-AC$) and makes a comparison based on the evaluation criteria. Additionally, the evaluation criteria are discussed for both TBA^2C and $BTG-AC$ models.

10.2 Evaluation Based on Features

In this section, the criteria used for the comparison and evaluation of both TBA^2C and $BTG-AC$ models are studied. To make a meaningful comparison, the evaluation criteria such as the network architecture model, the concepts and approaches, the decision outcomes, the access control policy and role, the data confidentiality and data privacy, and the data availability are discussed.

10.2.1 Network Architecture Model

Access control models can be different based on their network architecture model when the cryptographic keys, roles, policies and attributes are distributed to users from the trusted authority or controller. The TBA^2C model has been developed in Ponder2 [129], which is implemented as a Self-Managed Cell (SMC). The assumption is made that the SMC is used as a sensor and the access control engine is developed inside it. This means that each sensor

is deployed with the access control engine to make an effective decision within itself based on the users' request but the data aggregator is deployed centrally for the trust evaluation to support in the access control engine. Therefore, the TBA^2C model is not fully distributed but it can make and adjust access decisions dynamically. The $BTG-AC$ model is based on a centralised approach because each sensor node cannot store all the possibilities of defined situations and BTG operations to provide the data availability in the system. Therefore, the assumption is made that one SMC is used as data aggregator to store all the policies to make the decision effectively and it performs as a centralised access control manager in WSNs.

10.2.2 Concepts and Approaches

Both TBA^2C and $BTG-AC$ models use different concepts and approaches to fill the research gaps and the requirements of the application in WSNs. The similarity between these two WSN access control models is that both aim to provide data availability in emergency and unanticipated situations. An outline of the concepts and approaches for these two models can be seen in Table 10.1.

TBA^2C	$BTG-AC$
- Role Based Access Control - Discretionary Overriding of Access Control - User Behaviour Trust Model - Prevention and Detection Mechanism	- Role Based Access Control - Break-The-Glass concept

Table 10.1 The Concepts and Approaches for TBA^2C and $BTG-AC$

There is limited local decision-making capability in current WSN access control models because it is impossible to define in advance the possible denied and permitted access for all situations, especially in WMSNs and WSNs. TBA^2C is based on the concept of the discretionary overriding by Rissanen *et al.* [110] to provide flexibility in access control engine and to adjust access decisions dynamically based on the user behaviour trust value.

Li-qin *et al.* [74] mentioned that predicting user behaviour is important and significant

in forming a trustworthy network. Measuring user behaviour is difficult to evaluate and manage and is a new research issue in WSNs. In the TBA^2C model, a simple user behaviour trust model is proposed based on weighted running average algorithm that evaluate the total trust value of users based on current users' information and their previous trust value. For the current behaviour trust value, the geometric mean is used to evaluate based on user behaviour information. In addition, the trust values are used in both authorisation and overriding policy to check whether the users are trustworthy and untrustworthy to detect security policy violations by integrating with the prevention and detection mechanism and the obligation policy. Therefore, the TBA^2C model is proposed based on the above three concepts to address the conflict between data availability and data privacy, and to detect security policy violations.

The $BTG-AC$ model uses core RBAC with obligation and BTG concept to make decisions regarding access for emergency and unanticipated situations. The authorisation decision-making process is made within the core RBAC engine based on the inputs of the current section, the requested operation and the target object. The main idea of the BTG concept is to allow the users emergency and urgent access to the system when a normal authentication process does not perform or work perfectly. This means that, if the users face in emergency and unanticipated situation, they break-the-glass to bypass access control for urgent data access. Unlike TBA^2C, the emergency data access in $BTG-AC$ is based on predefined BTG state variables (TRUE or FALSE). This means that, the administrator needs to define BTG state variables for users in advance. This is only for one time use and the administrator needs to reset the BTG state variable for the next attempt. Therefore, some kind of user interactions are still involved in $BTG-AC$ and there is no mechanism to detect abnormal data access from authorised users.

The BTG concept can provide flexibility in access control engines to a certain extent. The features of the BTG concept can be provided in the TBA^2C model by simply changing and defining BTG state variables. In the $BTG-AC$, whether the users can perform BTG action in emergency and unanticipated situations are based on BTG state variables (TRUE or FALSE). In TBA^2C, the condition of trust value from the overriding policy can be used and changed to boolean values (TRUE for activating BTG action and FALSE for deactivating BTG action). Instead of using the trust value of users for the overriding process, the binary values can be used as the condition for whether the users can perform BTG action or overriding action in unanticipated situations. Therefore, the properties of $BTG-AC$ model

can be easily applied in the framework of TBA^2C.

10.2.3 Access Control Policy

Generally, there are different policies in each access control model. In this subsection, the way in which the access control policies are defined in both TBA^2C and $BTG-AC$ is presented. Both models address how to provide data availability service in emergency and unanticipated situations in WSNs. Therefore, the policies that relate to data access for emergency and unanticipated situations are discussed here.

Policy	Role	Department	Time	Condition	Operation	Oblg	Object
1	Nurse	Cancer	9am $\leq$ and $<$ 17pm	(if T $\geq$ 2.5)	override^{read}	$Oblg_2$	ob_3
2	Admin	Any	Any	N.A.	read	N.A.	Ac_{log}
3	Nurse	Cancer	9am $\leq$ and $<$ 17pm	T = TRUE	override^{read}	$Oblg_2$	ob_3

Table 10.2 Example of TBA^2C Policy

Based on Table 10.2, policy "1" in TBA^2C allows a nurse from "Cancer" department to access the confidential data (ob_3) in emergency and unanticipated situations but some obligations will be activated. Based on policy "1", the nurse can override access policy but the restricted access will be only granted to that user when his behaviour trust value is greater than or equal to 2.5. The administrator can easily check the audit log to detect security violations from authorised users based on policy 2. Policy 3 shows that the property of $BTG-AC$ model can be provided in TBA^2C by modifying the condition of trust criterion to boolean value that uses as BTG state variable (TRUE for activating BTG state and False for deactivating).

Unlike TBA^2C, the $BTG-AC$ model has an additional policy to perform BTG action for emergency and unanticipated situations. The defined policy of $BTG-AC$ can be seen in Table 10.3. In policy "1", the user is not permitted to access the confidential data (ob_3) unless he performs the BTG action in that object for emergency data access, but the BTG state

Policy	Role	Operation	Object	BTG State	Obligations
1	Nurse	$O^{BTG(read)}$	ob_3	TRUE	oblg [Notify Manager; Write to Audit; Reset BTG to FALSE]
2	Admin	$reset^{BTG}$	ob_3	N.A.	N.A.
3	Admin	read	log	N.A.	N.A.

Table 10.3 Example of $BTG-AC$ policy

variable needs to be “TRUE” meaning that BTG is enabled. Therefore, an extra BTG role is needed for the nurse. Additionally, some obligations will be activated when "the glass is broken". Policy 2 is quite simple. It is allowed to reset the BTG variable to “FALSE” to “TRUE” or “TRUE” to “FALSE”. Policy 3 allows the administrator to check the audit log.

Based on the above discussion, the policy definition for both TBA^2C and $BTG-AC$ has a similar structure. The weakness of the $BTG-AC$ model is that an additional policy is needed for each user to perform BTG operation for emergency access. As a result, the BTG policy needs to be considered in advance and predefined before the system is running in real-time.

10.2.4 Decision Outcomes

In TBA^2C, the existing decision outcomes in current access control models such as permitted access and denied access are extended into five different outcomes because of the overriding policy with the user behaviour trust value and the prevention, and detection mechanism. This also means that the access decision can be dynamically adjusted by using authorisation, overriding and obligation policy based on the user behaviour trust value and the contextual information. These decision outcomes are explained as follows:

- Permitted Access: A user access request has been permitted.
- Denied Access: A user access request has been denied. The user is not allowed to access the resources.
- Permitted Access with Obligation: A user access request has been permitted but an obligation is executed when data access is given to that user especially for important

and confidential information.

- Permitted Access with Overriding and Obligation: A user does not have privilege to access the resources but his request will be granted if he overrides policy within some constraints. The obligation policies are activated when access is granted to the user.
- Denied Access with Overriding and Obligation: A user access will be denied, if he tries to override the policy and does not satisfy some thresholds from that policy. At the same time, the obligations such as write to audit, etc. will be performed.

Based on the above discussion, it is clear that the introduction of the overriding policy with the user behaviour trust value can provide flexibility in access control engines and can make access decisions effectively by extending the existing decision outcomes with certain degrees of prevention and detection for both defined and unanticipated situations but the TBA^2C model has to set the defined trust value for the overriding process.

In the $BTG-AC$ model, the decision outcomes are extended because of the additional policies such as BTG policy and obligation policy. The decision outcomes are stated as follows.

- (Permit, $\emptyset$) $\rightarrow$ A user has permission to access the targeted object.
- (Permit, OBLGS) $\rightarrow$ A user is allowed to access the targeted object but an obligation is executed when the access is given.
- (Deny, $\emptyset$) $\rightarrow$ A user's request to access the targeted object is denied.
- (Deny, OBLGS) $\rightarrow$ Alongside a denied access, some obligations are performed.
- (Permit, BTG * OBLGS) $\rightarrow$ A user's request for access has been granted by performing BTG action and obligations such as "Write to Audit", " Trigger the Alarm" or "A Notification Message" are performed along with access decision.

Based on the above discussion, it is clear that the introduction of BTG and obligation policy in $BTG-AC$ is beneficial for WSNs. Unlike TBA^2C, the $BTG-AC$ model needs an additional policy to perform a BTG operation for each user, which requires all the possible data access to be defined in advance.

10.2.5 Data Confidentiality and Data Privacy

In TBA^2C, the assumption is made that Attribute-Based Encryption (ABE) [20] is used for data storage as well as authentication services. This means that data confidentiality and privacy are provided in normal situations. To provide data privacy and confidentiality in emergency and unanticipated situation, the TBA^2C model uses the prevention and detection mechanism and the user behaviour trust value together. In this model, the user behaviour trust value is evaluated in each user's access request. Only trusted users, who satisfy the thresholds from the system, can have access to requested data in emergency situations. On the other hand, if someone abuses the system or behaves unacceptably, the risk of damaging that data is higher than in normal data access. In addition, the prevention and detection mechanism keeps all the user information from the requested access in an audit log for the auditing purposes because security breaches can happen at any time. Two audit logs are used in the TBA^2C model: emergency log to detect security policy violations that are related to the overriding process and access log to detect the abnormal data access from authorised users. The system will assume as abnormal data access, when the user behaviour trust value is lower than defined value in the normal authorisation processes but the user can still access the medical record in these cases.

Unlike TBA^2C, $BTG-AC$ is proposed especially for emergency situations but it can be extended by applying a suitable cryptographic method for data confidentiality. However, when users perform BTG actions, there is no facility to protect the privacy of users' information. Therefore, a careful consideration of data confidentiality and data privacy is needed in the $BTG-AC$ model for both normal and emergency situations.

10.2.6 Data Availability

Both TBA^2C and $BTG-AC$ models are designed for making access decisions dynamically in emergency and unanticipated situations. In the TBA^2C model, the decisions regarding access can be evaluated and adjusted effectively, based on policies such as authorisation, obligation and overriding. Especially in emergency situations, the user behaviour trust value and the overriding policy are used to make and adjust access decisions effectively and efficiently. For emergency or urgent data access, the user has to override the denial of access based on predefined thresholds and the user behaviour trust value. This means that the decision-making process can be dynamically adjusted and effectively evaluated regarding data access because of the introduction of the overriding policy with the user behaviour

trust value. No human interaction is needed in order to override access policy for emergency situations in the TBA^2C model apart from the defining trust value in the system.

$BTG-AC$ has similar properties to TBA^2C but human interaction is still needed; as well, the BTG role needs to be predefined in advance for emergency situations. Users need extra roles (such as defining BTG state variables) for breaking-the-glass in unexpected and unanticipated situations. BTG policy is designed to provide extra access decisions for users when they are needed for emergency and urgent data access.

10.3 Conclusion

This chapter recapitulates both TBA^2C and $BTG-AC$ models to make a comparison between them based on the evaluation criteria. Current WSN access control models are not flexible enough to adjust access decisions dynamically for any situation. The advantage of both TBA^2C and $BTG-AC$ is that data availability is provided in normally defined situations as well as emergency situations; however, some restrictions and limitations are applied to the $BTG-AC$ model regarding BTG state variables that need to be predefined. This means that additional processes are required for the BTG model. As well, an additional policy is needed to activate the BTG operation for each user. The TBA^2C model is only suitable for high-end sensor devices. In addition, extra storage is required for the user behaviour trust evaluation. As well, a fixed infrastructure is required for TBA^2C to apply in WSNs because of both discretionary overriding process and user behaviour trust model, but it address the conflict between data availability and data privacy, and can detect abnormal data access. Based on the previous chapters, the next chapter concludes with research contributions and possible directions for future work.

Chapter 11

Conclusion

11.1 Introduction

This chapter reviews the contributions made in this dissertation to the Wireless Sensor Network (WSN) research community. The Trust-Based Adaptive Access Control (TBA^2C) model is very generic and due to the flexibility of the decision-making process regarding data access, there are many more application areas that it could be applied to. Accordingly, some further developments of TBA^2C to provide further security services are discussed. Finally, the conclusion is drawn.

11.2 Research Summary

At the beginning of this research, gaps were identified on the main problems and weakness among WSN access control models. These problems constituted the basis for the research explored during the course of this dissertation. The main objectives of this research work are to design flexible access control roles and policies that can address the conflict between data availability and data privacy during emergency and unanticipated situations, and to develop a new access control model that can make and adjust access decisions effectively and efficiently based on the aforementioned policies. To achieve this, the access control policies need to integrate both application requirements and user needs. These needs can be very complex to gather and integrate within an access control policy, but they are crucial nevertheless.

This research proceeded to study the possible approaches to achieve these objectives

and to develop and design a new decentralised access control model to address the research issues in the WSN research community. Firstly, the adaptive access control model was developed based on the concept of discretionary overriding to address the data availability issue in healthcare applications for WSNs because the lack of data availability can result in further decline in patients' conditions. In the healthcare industry, security is the degree of protection against danger, loss, damage and criminal activity. Therefore, we extended the adaptive access control model with prevention and detection mechanisms to detect security policy violations, and the concept of obligation to take a course of action when a restricted access is granted or denied. However, there is no consideration for privacy of patients' information because data availability is prioritised to the first place in the adaptive access control model.

To address the conflict between data availability and data privacy, this research proposed the Trust-based Adaptive Access Control (TBA^2C) model that integrates the concept of trust into the previous model. A simple user behaviour trust model is developed to calculate the behaviour trust value which is used as one of the defined thresholds to override access policy for data availability purpose. The trust model can also protect data privacy because only the user who satisfies the relevant trust threshold, can get a restricted access even in emergency and unanticipated situations. Notwithstanding, the TBA^2C model is easy to adapt with other trust models in WSNs instead of using a simple behaviour trust model from chapter 7.

Ponder2 was used to develop the TBA^2C model gradually, starting from a simple access control model to the full TBA^2C. In Ponder2, a Self-Managed Cell (SMC) simulates a sensor node with the TBA^2C engine inside it. From efforts to find any similar such systems, this project is confident that the proposed TBA^2C model is the first to realise a flexible access control engine and to address the conflict between data availability and data privacy by combining the concepts of discretionary overriding, the user behaviour trust model, and the prevention and detection mechanism together.

11.3 Contribution to Knowledge

The main contribution to the WSN research community that this work makes is the Trust-Based Adaptive Access Control model (TBA^2C) model itself. The TBA^2C model is conveyed in this dissertation via medical application and comprised the following significant contributions:

- The introduction of overriding policy based on a user behaviour trust value and contextual information is the main novel element of the proposed TBA^2C model. The discretionary overriding concept to address data availability issue is not a new idea for wireless networks but it has not been introduced and applied in WSNs before. The novel usage of the discretionary overriding concept with user behaviour trust in adjusting decisions regarding data access for emergency and unanticipated situations is a new concept.

- The combination of the discretionary overriding concept and the behaviour trust model is a possible solution that helps to address the conflict between data availability and data privacy by using the behaviour trust value as one of the defined thresholds in the access policies. Only the trusted user, who satisfies these thresholds including trust value, can get a restricted access in emergency and unanticipated situations.

- The framework of the proposed TBA^2C model provides a flexible approach in access control engines to make access decisions effectively and immediately in both defined and unanticipated situations. Additionally, the usage of user behaviour monitoring and the prevention and detection mechanism can detect security policy violations such as unauthorised information release, unnecessary overriding process and abnormal data access from both authorised and unauthorised users. The use of a behaviour trust value in an authorisation policy is a possible approach to detect abnormal data access from authorised users.

- The concepts of possibility-with-override and the user behaviour trust model could become the foundation for further implementation of access control engines in WSNs as well as other systems requiring access control.

The overall contribution of this research work is that it has successfully designed a novel decentralised access control model to make and adjust access decisions effectively and efficiently whenever the system faces unexpected and unanticipated situations.

11.4 Research Limitations

Some limitations during the course of this research are worth mentioning. The proposed TBA^2C model is developed in the Ponder2 package using SMC as a sensor, which consists of a set of hardware and software components that represent an administrative domain, as

a sensor node. In future, the proposed TBA^2C model is considered for implementation in actual sensor nodes.

11.5 Recommendations for Future Work

This section outlines some further possible concepts and approaches which can apply in the TBA^2C model to provide further security services.

11.5.1 Attribute Based Encryption (ABE)

In future, ABE based encryption is considered to be applied in TBA^2C for user's authentication process. Additionally, the ABE approach will use to encrypt the collected and sensed data at sensor nodes to provide data confidentiality. Sahai and Waters [50] proposed the ABE scheme to model and design a scalable and flexible access control system. ABE is a public key cryptography primitive generalising Identity-Based Encryption (IBE) [47] that is associated with a user's identity in a single user message. In ABE, a group of users is described by the combination of several descriptive attributes and access structures, which is also called an attribute policy. In ABE, the public key encryption is based on one-to-many encryption. There are two different types of ABE proposed by Sahai and Waters [50], namely Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In KP-ABE, sensed and stored data in the sensor node are encrypted with a set of attributes; the user's private key is associated with an access structure that specifies which types of ciphertexts the key can decrypt. Only the users that have the right access structure and the key can access and decrypt the encrypted data. In CP-ABE, the ciphertext is associated with the access structure. The user's private key is associated with the attributes that specify which type of ciphertext the key can decrypt. Some ABE-based fine-grained access control models use ECC for key management and distribution.

The users and sensor nodes need to receive keys, access structure and attributes from Distributed Centres (DCs). All DCs are disjointed from each other, so the user can only obtain certain types of attributes and access structure from each DC. Based on the ABE scheme, a user needs to show his or her identification (ID) to each DC to gain access structures and secret keys. In this case, the user's ID can be the Medium Access Control (MAC) address of his or her Personal Digital Assistant (PDA), personal computer or any other unique identity. Each user may have different access structures from a DC that depend on

how much data or what kind of information the user wants to access from a sensor node. The access privileges and access structure will be different, based on user roles and responsibilities. Sensor nodes are preloaded with attributes and public keys from DCs. A public key associated with attributes, is used for data encryption in a sensor node.

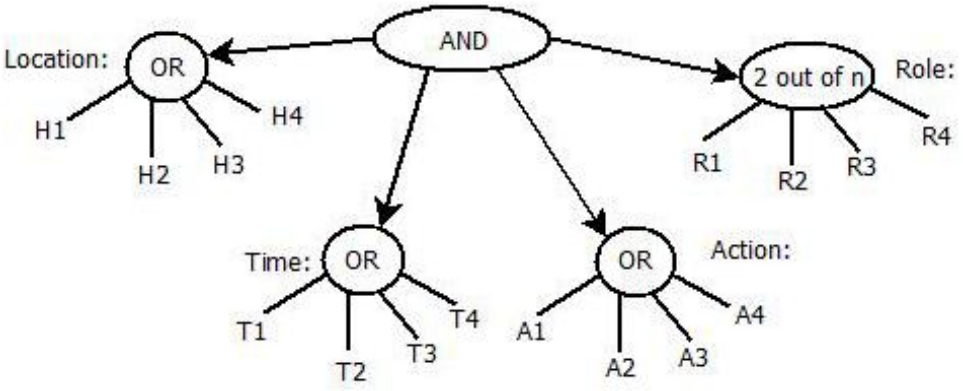


Fig. 11.1 An Access Structure

For example in a medical scenario, the sensor nodes are usually deployed to collect medical information from a certain location. Each sensor node may be responsible for collecting specific types of data such as cardiology information, blood pressure and heart rate. Sensor nodes may also have their owners, i.e., a person who takes care of them. Hence, it can be specified that sensor nodes use these attributes such as location = (hospital or home), data type = (blood pressure, cardiology information, heart rate), action = (read, write, update, etc.). This further enables data access privileges of users to be specified based on these attributes. In the above example, the access structure of a user may be designated as ”location is hospital OR home AND data type is cardiology OR blood pressure AND actions are read OR write OR update”, which allows the users to obtain data within the hospital area. In addition, other requirements such as a user having to possess at least two or three of these roles (general physician, physician, doctor, nurse, chemist, etc) can be provided for further security purposes. An overview diagram of the access structure based on the ABE approach can be seen in Figure 11.1 for data encryption and authentication purposes.

11.5.2 Re-authentication or Continuous Authentication

In most cases, once a user is initially authenticated, the system or mechanism has no effective method to verify that the current user is the same authenticated user during real time system usage. Therefore, user re-authentication is needed as another layer of security and

the system needs to intelligently identify any changes of the users. Masquerading is an important factor for identity theft in current authentication systems because there is a lack of a mechanism to prevent and detect it. There are many proposed re-authentication systems [23], [66], [65], [24], [60], [30] for wireless networks. Among them, the location based re-authentication process [66] is suitable for WSNs because the sensor nodes have capability to capture and record the current user's location. In location-based re-authentication, the users' location information is continuously checked to ensure the users' claimed location is the same as their actual location in order to verified to prevent a masquerading attack.

In TBA^2C, the location of users is continuously sensed after the users are authenticated. If a user changes location in that period, the current session that the user already authenticated for is expired, so the user needs to re-authenticate to check and obtain data from the network. The advantage is that the sensor node can sense and store multi-media information. Because of this, the re-authentication process can be easily accomplished in WSNs and WMSNs.

11.5.3 Predicted Users' Behaviour Trust

Even the TBA^2C model is capable of working with other trust models in WSNs, the predicted user's behaviour trust value is considered as another possible factor to extend a simple behaviour trust model in chapter 7 for the evaluation of the total behaviour trust value. Li-qin *et al.* [74] mentioned that predicting user behaviour is important and significant in forming a trustworthy network. Measuring user behaviour is difficult to evaluate and manage and is a new research issue in WSNs. A simple proposed trust model in chapter 7 is calculated the behaviour trust value based on the current trust value and previous trust value. In future, the current user information from the recent transaction and previous user information from the audit log that is stored in the prevention and detection mechanism can be used for the evaluation of predicted trust. Bayesian Network [94] and Naive-Bayes classifier [25] are considered to apply for an evaluation of the predicted trust in the proposed trust model. Bayesian Network and Naive-Bayes in general are relationship networks that use statistical methods to represent probability relationships between different entities. It is a compact representation of a joint probability distribution for reasoning under uncertainty. Bayesian Network and Naive Bayes provide a flexible method to present differentiated trust and combine different aspects of trust.

Yuan *et al.* [145], [146] introduced a dynamic trust model based on the Naive Bayes classifier for ubiquitous environments to prevent illegal nodes from joining a network. The prior probability and past interaction history formula and expression can be applied in the proposed trust model for evaluation of predicted user behaviour trust value. Prior probability reflects the acceptance level based on different user criteria. Past interaction history is the system's prior knowledge of acceptance based on the decision-making process.

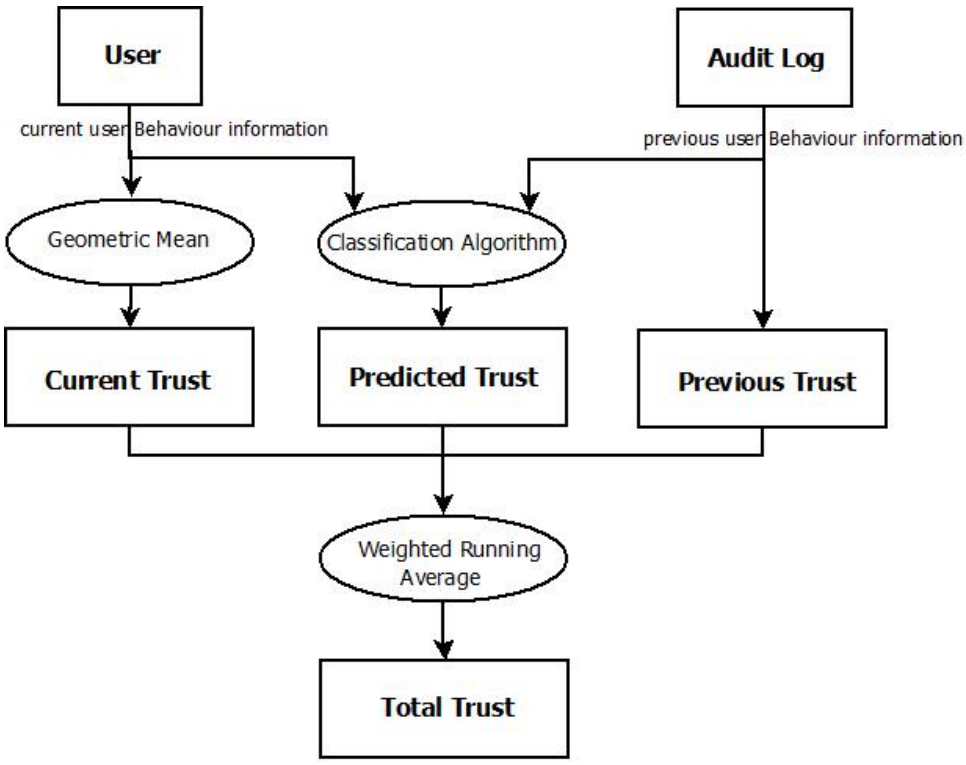


Fig. 11.2 A New Framework of the User Behaviour Trust Module

Current user information from the requested query and previous user information from the audit log can be used for both prior probability and past interaction history to evaluate the predicted behaviour trust value in the proposed model. An overview diagram of the proposed user behaviour trust model can be seen in Figure 11.2. Classification algorithms such as Bayesian Network and Naive-Bayes, can be applied in TBA^2C to evaluate the predicted trust.

11.5.4 Risk Assessment

In TBA^2C, risk assessment can be applied in the access control module as another key component for the decision-making process. The definition of risk can be different, based on how the risk assessment module is designed and what kind of information is used for the risk evaluation process. In TBA^2C, the risk analysis can be done and identified regarding current trust value, previous trust value and user information such as role, location and time.

To define a set of risk analysis functions for the risk assessment module, a careful consideration of situations and threats that may lead to risk is needed. In addition, appropriate functions and methods are needed to evaluate or calculate the risk value based on recognised situations and treats. In the risk assessment module, risk value will be compared with defined thresholds and then evaluated for the final result. It will be forwarded to the access control module to use as one of the supporting factors for the decision-making process.

11.6 Conclusion

This chapter has reviewed this thesis's contributions to the WSN research community and possible extensions to improve the TBA^2C model. The proposed TBA^2C model is easy to adapt with other concepts to provide further security services in WSNs. This chapter has also discussed possible extensions to modify the proposed model as pathways for future work. Suggestions are given for further research into features that move beyond the scope of this work such as the Attribute-Based Encryption (ABE) scheme for the user authentication process as well as data storage; a complex classification algorithm to evaluate and calculate the predicted trust value of users; and risk assessment for real-world applications in WSNs and WMSNs.

References

[1] Accorsi, R. and Stocker, T. (2008). Automated privacy audits based on pruning of log data. In *Enterprise Distributed Object Computing Conference Workshops, 2008 12th*, pages 175–182.

[2] Aivaloglou, E. and Gritzalis, S. (2010). Hybrid trust and reputation management for sensor networks. *Wirel. Netw.*, 16(5):1493–1510.

[3] Akyildiz, I., Melodia, T., and Chowdhury, K. (2008). Wireless multimedia sensor networks: Applications and testbeds. *Proceedings of the IEEE*, 96(10):1588–1605.

[4] Akyildiz, I. F., Melodia, T., and Chowdhury, K. R. (2007). A survey on wireless multimedia sensor networks. *Comput. Netw.*, 51(4):921–960.

[5] Akyildiz, I. F. and Stuntebeck, E. P. (2006). Wireless underground sensor networks: Research challenges. *Ad Hoc Networks*, 4(6):669 – 686.

[6] Akyildiz, I. F., Sun, Z., and Vuran, M. C. (2009). Signal propagation techniques for wireless underground communication networks. *Physical Communication Journal (Elsevier)*, 2:167–183.

[7] Al-Hamdani, W. A. (2007). Cryptography based access control in healthcare web systems. *Security Issues in Sensor and Ad Hoc Networks*.

[8] Al-mahmud, A. and Morogan, M. C. (2012). Article: Identity-based authentication and access control in wireless sensor networks. *International Journal of Computer Applications*, 41(13):18–24. Published by Foundation of Computer Science, New York, USA.

[9] Alemdar, H. and Ersoy, C. (2010). Wireless sensor networks for healthcare: A survey. *Computer Networks*, 54(15):2688–2710.

[10] Alqatawna, J., Rissanen, E., and Sadighi, B. (2007a). Overriding of access control in xacml. *8th IEEE International Workshop on policies for Distributed Systems and Networks*.

[11] Alqatawna, J., Rissanen, E., and Sadighi, B. (2007b). Overriding of access control in XACML. In *Policies for Distributed Systems and Networks, 2007. POLICY '07. Eighth IEEE International Workshop on*, pages 87–95.

[12] Ana, F., Cruz-correia, R., Luís. B, A., and A, C. (2007). Access control: how can it improve patients' healthcare. Technical report, Student Health Technology Information, University of Kent.

[13] Anderson, J. (1973). Information in a multi-user computer environment. In *Advances in Computers*.

[14] Atakli, I. M., Hu, H., Chen, Y., Ku, W.-S., and Su, Z. (2008). Malicious node detection in wireless sensor networks using weighted trust evaluation. In Rajaei, H., Wainer, G. A., and Chinni, M. J., editors, *SpringSim*, pages 836–843. SCS/ACM.

[15] Bao, F., Chen, I.-R., Chang, M., and Cho, J.-H. (2011). Trust-based intrusion detection in wireless sensor networks. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–6.

[16] Bao, F., Chen, I.-R., Chang, M., and Cho, J.-H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *Network and Service Management, IEEE Transactions on*, 9(2):169–183.

[17] Ben, L., Lee, D. K., and Palsberg, J. (2005). Avrora: Scalable sensor network simulation with precise timing. *4th International Conference on Information Processing in Sensor Networks*.

[18] Bender, A., Katz, J., and Morselli, R. (2006). Ring signatures: Stronger definitions, and constructions without random oracles. In *Proceedings of TCC 2006, volume 3876 of LNCS*, pages 60–79. Springer-Verlag.

[19] Bertino, E. and Ghinita, G. (2011). Towards mechanisms for detection and prevention of data exfiltration by insiders: Keynote talk paper. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, pages 10–19, New York, NY, USA. ACM.

[20] Bethencourt, J., Sahai, A., and Waters, B. (2007). Ciphertext-policy attribute-based encryption. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, SP '07, pages 321–334, Washington, DC, USA. IEEE Computer Society.

[21] Blocki, J., Christin, N., Datta, A., and Sinha, A. (2011). Audit mechanisms for privacy protection in healthcare environments. In *Proceedings of the 2Nd USENIX Conference on Health Security and Privacy*, HealthSec'11, pages 10–10, Berkeley, CA, USA. USENIX Association.

[22] Boneh, D., Gentry, C., and Waters, B. (2005). Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Proceedings of the 25th annual international conference on Advances in Cryptology*, CRYPTO'05, pages 258–275, Berlin, Heidelberg. Springer-Verlag.

[23] Brosso, I., La Neve, A., Bressan, G., and Ruggiero, W. (2010). A continuous authentication system based on user behavior analysis. In *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, pages 380–385.

[24] Campbell, J. P., Campbell, W. M., Jones, D. A., Lew, S. M., Reynolds, D. A., and Weinstein, C. J. (2003). Biometrically enhanced software-defined radios. In *Proceedings of Software Defined Radio Technical Conference*.

[25] Chai, K. M. A., Chieu, H. L., and Ng, H. T. (2002). Bayesian online classifiers for text classification and filtering. In *Proceedings of the 25th annual international ACM SIGIR conference on Research and development in information retrieval*, SIGIR '02, pages 97–104, New York, NY, USA. ACM.

[26] Chase, M. and Chow, S. S. M. (2009). Improving privacy and security in multi-authority attribute-based encryption. *16th ACM Conference on Computer and Communications Security*.

[27] Chatterjee, S., Das, A. K., and Sing, J. K. (2014). A novel and efficient user access control scheme for wireless body area sensor networks. *Journal of King Saud University - Computer and Information Sciences*, 26(2):181 – 201.

[28] Crispo, B. (1999). Delegation of responsibilities. In Christianson, B., Crispo, B., Harbison, W., and Roe, M., editors, *Security Protocols*, volume 1550 of *Lecture Notes in Computer Science*, pages 118–124. Springer Berlin Heidelberg.

[29] Damianou, N., Dulay, N., Lupu, E., and Sloman, M. (2001). The ponder policy specification language. *POLICY '01 Proceedings of the International Workshop on Policies for Distributed Systems and Networks*.

[30] Deutschmann, I., Nordstrom, P., and Nilsson, L. (2013). Continuous authentication using behavioral biometrics. *IT Professional*, 15(4):12–15.

[31] Dodge, Y. (2008). Weighted arithmetic mean. In *The Concise Encyclopedia of Statistics*, pages 565–566. Springer New York.

[32] Duan, J., Gao, D., Foh, C. H., and Zhang, H. (2013). TC-BAC: A trust and centrality degree based access control model in wireless sensor networks. *Ad Hoc Netw.*, 11(8):2675–2692.

[33] Fasolo, E., Rossi, M., Widmer, J., and Zorzi, M. (2007). In-network aggregation techniques for wireless sensor networks: a survey. *Wireless Communications, IEEE*, 14(2):70–87.

[34] Fernandez-Gago, M., Roman, R., and Lopez, J. (2007). A survey on the applicability of trust management systems for wireless sensor networks. In *Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2007. SECPerU 2007. Third International Workshop on*, pages 25–30.

[35] Ferraiolo, D. F. and Kuhn, D. R. (1992). Role-based access controls. *15th National Computer Security Conference*.

[36] Ferreira, A., Chadwick, D., Farinha, P., Correia, R., Zao, G., Chilro, R., and Antunes, L. (2009). How to securely break into rbac: The btg-rbac model. In *Proceedings of the 2009 Annual Computer Security Applications Conference*, ACSAC '09, pages 23–31, Washington, DC, USA. IEEE Computer Society.

[37] Ferreira, A. M. (2010). *Modelling Access Control for Healthcare Information Systems: How to control access through policies, human processes and legislation*. PhD thesis, University of Kent and Faculdade De Ciencias Universidade Do Porto.

[38] Ferreria, A., Correia, R., Monterio, H., Brito, M., and Antunes, L. (2011). Usable access control policy and model for healthcare. *Computer Based Medical System (CBMS)*.

[39] Firozabadi, B. S. (2005). *Decentralised Privilege Management for Access Control*. PhD thesis, Imperial College, University of London.

[40] Firozabadi, B. S. and Sergot, M. J. (2000). Power and permission in security systems. In *Proceedings of the 7th International Workshop on Security Protocols*, pages 48–59, London, UK, UK. Springer-Verlag.

[41] Firozabadi, B. S., Tan, Y. H., and Lee, R. M. (1999). Formal definations of fraud. *Logics and Information Systems- New Studies in Deontic Logic and Computer Science*.

[42] Ganeriwal, S. and Srivastava, M. B. (2004). Reputation-based framework for high integrity sensor networks. In *Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN '04, pages 66–77, New York, NY, USA. ACM.

[43] Garcia-Morchon, O. and Wehrle, K. (2010). Modular context-aware access control for medical sensor networks. In *Proceedings of the 15th ACM symposium on Access control models and technologies*, SACMAT '10, pages 129–138, New York, NY, USA. ACM.

[44] Gaubatz, G., Kaps, J.-P., and Sunar, B. (2004). Public key cryptography in sensor networks - revisited. In *ESAS*, pages 2–18.

[45] Gaurkar, S. and Ingole, P. K. (2013). Access control and intrusion detection for security in wireless sensor network. *Internal Journal of Scientific and Technology Research.*, 16(2).

[46] Gay, D., Levis, P., von Behren, R., Welsh, M., Brewer, E., and Culler, D. (2003). The nesc language: A holistic approach to networked embedded systems. *SIGPLAN Not.*, 38(5):1–11.

[47] Gentry, C. (2006). *Handbook of information Security*. John Wiley and Sons.

[48] Ghani, N. A., Selamat, H., and Sidek, Z. M. (2012). Analysis of existing privacy-aware access control for e-commerce application. *Global Journal of Computer Science and Technology*.

[49] Gligor, V. D. (2011). Handling new adversaries in wireless ad-hoc networks (transcript of discussion). In Christianson, B., Malcolm, J. A., Matyas, V., and Roe, M., editors, *Security Protocols XVI*, volume 6615 of *Lecture Notes in Computer Science*, pages 120–125. Springer Berlin Heidelberg.

[50] Goyal, V., Pandey, O., Sahai, A., and Waters, B. (2006a). Attribute-based encryption for fine-grained access control of encrypted data. In *ACM Conference on Computer and Communications Security*, pages 89–98.

[51] Goyal, V., Pandey, O., Sahai, A., and Waters, B. (2006b). Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, pages 89–98, New York, NY, USA. ACM.

[52] Greene, H. A. and Wright, D. (2012). Security lessons learned from hipaa enforcement. *3rd USENIX Workshop on Health Security and Privacy, HealthSec '12*.

[53] Gura, N., Patel, A., W, A., Eberle, H., and Shantz, S. C. (2004). Comparing elliptic curve cryptography and rsa on 8-bit cpus. In *Cryptographic Hardware and Embedded Systems - CHES 2004*, pages 119–132. Springer Berlin Heidelberg.

[54] He, D., Bu, J., Zhu, S., Chan, S., and Chen, C. (2011). Distributed access control with privacy support in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 10(10):3472–3481.

[55] Herrick, D. M., Gorman, L., and Goodman, J. C. (2010). Health Information Technology: Benefits and Problems. Technical Report 327.

[56] Hur, J. (2011). Fine-grained data access control for distributed sensor networks. *Wirel. Netw.*, 17(5):1235–1249.

[57] Imran, M., Said, A. M., and Hasbullah, H. (2010). A survey of simulators, emulators and testbeds for wireless sensor networks. *IEEE, International Symposium on Information Technology*.

[58] INCITS (2004). Information Technology - Role-Based Access Control. Technical report, American National Standard for Information Technology, International Committee for Information Technology Standard.

[59] Ishmanov, F. and Kim, S. W. (2011). A secure trust establishment in wireless sensor networks. In *Electrical Engineering and Informatics (ICEEI), 2011 International Conference on*, pages 1–6.

[60] Jagadeesan, H. and Hsiao, M. (2009). A novel approach to design of user re-authentication systems. In *Biometrics: Theory, Applications, and Systems, 2009. BTAS '09. IEEE 3rd International Conference on*, pages 1–6.

[61] Johnson, D., Menezes, A., and Vanstone, S. (2001). The elliptic curve digital signature algorithm : ECDSA. In *International Journal of Information Security*, pages 36–63. Springer-Verlag.

[62] Josang, A. and Ismail, R. (2002). The beta reputation system. In *In Proceedings of the 15th Bled Electronic Commerce Conference*.

[63] Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. In *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, pages 113 – 127.

[64] Karthik, N. and Dhulipala, V. (2011). Trust calculation in wireless sensor networks. In *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, volume 4, pages 376–380.

[65] Kim, J., Baek, J., and Shon, T. (2011). An efficient and scalable re-authentication protocol over wireless sensor network. *Consumer Electronics, IEEE Transactions on*, 57(2):516–522.

[66] Kurkovsky, S. and Syta, E. (2010). Approaches and issues in location-aware continuous authentication. In *Computational Science and Engineering (CSE), 2010 IEEE 13th International Conference on*, pages 279–283.

[67] Lampson, B. W. (1974). Protection. *SIGOPS Oper. Syst. Rev.*, 8(1):18–24.

[68] Levis, P. (2006). Tiny operating system: TinyOS. Technical report, TinyOS Community.

[69] Levis, P. and Lee, N. (2003). Tossim: A simulator for tinyos networks. *University of California ,Berkeley, California*.

[70] Lewis, N., Foukia, N., and Govan, D. (2008). Using trust for key distribution and route selection in wireless sensor networks. In *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE*, pages 787–790.

[71] Li, J., Zhao, G., Chen, X., Xie, D., Rong, C., Li, W., Tang, L., and Tang, Y. (2010a). Fine-grained data access control systems with user accountability in cloud computing. *IEEE 2nd International Conference on Cloud Computing Technology and Science*.

[72] Li, M., Lou, W., and Ren, K. (2010b). Data security and privacy in wireless body area networks. *Wireless Commun.*, 17(1):51–58.

[73] Li, Z. and Gong, G. (2008). A survey on security in wireless sensor networks. *Technical Report, University of Waterloo*.

[74] Li-qin, T., Chuang, L., and Yang, N. (2010). Evaluation of user behaviour trust in cloud computing. *2010 International Conference on Computer Application and System Modeling(ICCASM 2010)*.

[75] Liu, K., Abu-Ghazaleh, N., and Kang, K.-D. (2007). Location verification and trust management for resilient geographic routing. *Journal of Parallel and Distributed Computing*, 67(2):215 – 228.

[76] Liu, T., Chen, D.-J., and Zhou, M.-Z. (2011). Pair-wise key update in wireless sensor networks based on reputation model. In *Electronics, Communications and Control (ICECC), 2011 International Conference on*, pages 1558–1561.

[77] Liu, T. and Zhou, M.-Z. (2010). A key management scheme in wireless sensor networks based on behavior trust. In *Progress in Informatics and Computing (PIC), 2010 IEEE International Conference on*, volume 1, pages 556–559.

[78] Lupu, E., Dulay, N., Sloman, M., Sventek, J., Heeps, S., Strowes, S., Twidle, K., Keoh, S.-L., and Schaeffer-Filho, A. (2008). Amuse: autonomic management of ubiquitous e-health systems. *Concurr. Comput. : Pract. Exper.*, 20(3):277–295.

[79] Maerien, J., Michiels, S., Huygens, C., Hughes, D., and Joosen, W. (2013). Access control in multi-party wireless sensor networks. In Demeester, P., Moerman, I., and Terzis, A., editors, *Wireless Sensor Networks*, volume 7772 of *Lecture Notes in Computer Science*, pages 34–49. Springer Berlin Heidelberg.

[80] Malan, D. J., Welsh, M., and Smith, M. D. (2004). A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In *Proceedings of the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*.

[81] Mana, M., Feham, M., and Bensaber, B. A. (2011). Trust key management scheme for wireless body area networks. *I. J. Network Security*, 12(2):75–83.

[82] Marsh, D. W., Baldwin, R. O., Mullins, B. E., Mills, R. F., and Grimalia, M. R. (2009). A security policy language for wireless sensor network. *Journal of Systems and Software*.

[83] MATLAB (2012). *MATLAB and Statistics Toolbox Release 2012b(R2012b)*. The MathWorks Inc., Natick, Massachusetts.

[84] Maw, H., Xiao, H., Christianson, B., and Malcolm, J. (2014a). An evaluation of break-the-glass access control model for medical data in wireless sensor networks. In *e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on*, pages 130–135.

[85] Maw, H. A., Xiao, H., Christianson, B., and Malcolm, J. A. (2014b). A survey of access control models in wireless sensor networks. *Journal of Sensor and Actuator Network*, 3(2):150–180.

[86] Meier, J., Alex, M., Michael, D., Srinath, V., Ray, E., and Anandha, M. (2003). Threats and countermeasures. *Microsoft Developer Network*.

[87] Mirembe, D. and Muyeba, M. (2008). Threat modeling revisited: Improving expressiveness of attack. In *Computer Modeling and Simulation, 2008. EMS '08. Second UKSIM European Symposium on*, pages 93–98.

[88] Moakher, M. (2005). A differential geometric approach to the geometric mean of symmetric positive-definite matrices. *SIAM J. Matrix Anal. Appl*, 26.

[89] Moffett, J. D. and Sloman, M. S. (1990). Delegation of authority. In *in Integrated Network Management II, I. Krishnan and*, pages 595–606. Elsevier Science Publishers B.V. (North-Holland.

[90] Mohammad, A., Khdour, T., Kanaan, G., Kanaan, R., and bani Ahmad, S. (2011). Analysis of existing access control models from web services applications' perspective. *Journal of Computing*.

[91] Momani, M. (2008). *Bayesian Methods for Modelling and Management of Trust in Wireless Sensor Networks*. PhD thesis, University of Technology, Sydney.

[92] Momani, M., Aboura, K., and Challa, S. (2007). Rbatmwsn: Recursive bayesian approach to trust management in wireless sensor networks. In *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, pages 347–352.

[93] Momani, M. and Challa, S. (2008). Gtrssn: Gaussian trust and reputation system for sensor networks. In Sobh, T., editor, *Advances in Computer and Information Sciences and Engineering*, pages 343–347. Springer Netherlands.

[94] Momani, M., Challa, S., and Alhmouz, R. (2008a). Bnwsn: Bayesian network trust model for wireless sensor networks. In *Communications, Computers and Applications, 2008. MIC-CCA 2008. Mosharaka International Conference on*, pages 110–115.

[95] Momani, M., Challa, S., and Alhmouz, R. (2008b). Can we trust trusted nodes in wireless sensor networks? In *Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on*, pages 1227–1232.

[96] Moraru, L., Leone, P., Nikoletseas, S., and Rolim, J. D. P. (2007). Near optimal geographic routing with obstacle avoidance in wireless sensor networks by fast-converging trust-based algorithms. In *Proceedings of the 3rd ACM Workshop on QoS and Security for Wireless and Mobile Networks*, Q2SWinet '07, pages 31–38, New York, NY, USA. ACM.

[97] Morchon, O. G. and Wehrle, K. (2010). Efficient and context-aware access control for pervasive medical sensor networks. *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference*.

[98] Nagarathna, K., Kiran, Y., Mallapur, J., and Hiremath, S. (2012). Trust based secured routing in wireless multimedia sensor networks. In *Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International Conference on*, pages 53–58.

[99] Newsome, J., Shi, E., Song, D., and Perrig, A. (2004). The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd international symposium on Information processing in sensor networks*, IPSN '04, pages 259–268, New York, NY, USA. ACM.

[100] Ng, H. S., Sim, M. L., and Tan, C. M. (2006). Security issues of wireless sensor networks in healthcare applications. *BT Technology Journal*, 24(2):138–144.

[101] Ngo, D. N. (2006). *Deployment of 802.15.4 Sensor Networks for C4ISR Operations*. PhD thesis, Navy Postgraduate School, Monterey, California.

[102] Padmavathi, G. and Shanmugapriya, D. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security, IJCSIS*, 4.

[103] Pathan, A., Lee, H.-W., and Hong, C. S. (2006). Security in wireless sensor networks: issues and challenges. In *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, volume 2.

[104] Perrig, A., Stankovic, J., and Wanger, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, 47(6):53–57.

[105] Polley, J., Blazakis, D., McGee, J., Rusk, D., Baras, J. S., and Karir, M. (2004). Atemu: A fine-grained sensor network simulator. *First Annual IEEE Communications Society Conference on In Sensor and Ad Hoc Communications and Networks*.

[106] PREMIS (2012). Premis data dictionary for preservation metadata. Technical report, OCLC Research.

[107] Radu, C., Govaerts, R., and Vandewalle, J. (1996). A restrictive blind signature scheme with applications to electronic cash. In *Communications and Multimedia Security*, pages 196–207.

[108] Raymond, D. R. and Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, 7(1):74–81.

[109] Rissanen, E., Firozabadi, B., and Sergot, M. (2005). Discretionary overriding of access control in the privilege calculus. In Dimitrakos, T. and Martinelli, F., editors, *Formal Aspects in Security and Trust*, volume 173 of *IFIP International Federation for Information Processing*, pages 219–232. Springer US.

[110] Rissanen, E., Firozabadi, B., and Sergot, M. (2006). Towards a mechanism for discretionary overriding of access control. In Christianson, B., Crispo, B., Malcolm, J., and Roe, M., editors, *Security Protocols*, volume 3957 of *Lecture Notes in Computer Science*, pages 312–319. Springer Berlin Heidelberg.

[111] Rivest, R. L., Shamir, A., and Adleman, L. (1983). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 26(1):96–99.

[112] Rostad, L. and Edsberg, O. (2006). A study of access control requirements for healthcare systems based on audit trails from access logs. In *Computer Security Applications Conference, 2006. ACSAC '06. 22nd Annual*, pages 175–186.

[113] Ruj, S., Nayak, A., and Stojmenovic, I. (2011). Distributed fine-grained access control in wireless sensor networks. In *IPDPS*, pages 352–362.

[114] Sahafizadeh, E. and Parsa, S. (2010). Survey on access control models. *2nd International Conference on Future Computer and Communication*.

[115] Samarati, P. and Vimercati, S. (2001). Access control: Policies, models, and mechanisms. In Focardi, R. and Gorrieri, R., editors, *Foundation of Security Analysis and Design*, volume 2171 of *Lecture Notes in Computer Science*, pages 137–196. Springer Berlin Heidelberg.

[116] Sandhu, R., Ferraiolo, D., and Kuhn, R. (2000). The NIST model for role-based access control: Towards a unified standard. In *Proceedings of the Fifth ACM Workshop on Role-based Access Control*, RBAC '00, pages 47–63, New York, NY, USA. ACM.

[117] Sandhu, R. and Munawer, Q. (1998). How to do discretionary access control using roles. *RBAC '98 Proceedings of the third ACM workshop on Role-based access control*.

[118] Sandhu, R. and Samarati, P. (1996). Authentication, access control, and audit. *ACM Comput. Surv.*, 28(1):241–243.

[119] Seitz, L., Rissanen, E., and Firozabadi, B. S. (2006). A classification of delegation schemes for attribute authority. In *Formal Aspects in Security and Trust, Fourth International Workshop, FAST 2006, Hamilton, Ontario, Canada, August 26-27, 2006, Revised Selected Papers*, pages 158–169.

[120] Sen, J. (2010). A survey on wireless sensor network security. *International Journal of Communication Networks and Information Security*, 1.

[121] Shaikh, R., Jameel, H., d'Auriol, B., Lee, H., Lee, S., and Song, Y.-J. (2009). Group-based trust management scheme for clustered wireless sensor networks. *Parallel and Distributed Systems, IEEE Transactions on*, 20(11):1698–1712.

[122] Shamir, A. (1985). Identity-based cryptosystems and signature schemes. In Blakley, G. R. and Chaum, D., editors, *Advances in Cryptology*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer Berlin Heidelberg.

[123] Singh, S. (2011). Trust based authorization framework for grid services. *Journal of Emerging Trends in Computing and Information Sciences*, 2(3).

[124] Skeen, D. (1982). A quorum-based commit protocol. Technical report, Ithaca, NY, USA.

[125] Srinivasan, A., Teitelbaum, J., and Wu, J. (2006). DRBTS: Distributed reputation-based beacon trust system. In *Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on*, pages 277–283.

[126] Sun, Z., Wang, P., Vuran, M. C., Al-Rodhaan, M. A., Al-Dhelaan, A. M., and Akyildiz, I. F. (2011). Bordersense: Border patrol through advanced wireless sensor networks. *Ad Hoc Networks*, 9(3):468 – 477.

[127] Sundresh, S., Kim, W., and Agha, G. (2004). SENS: A sensor, environment and network simulator. *37th Annual Simulation Symposium (ANSS37)*.

[128] Tanachaiwiwat, S., Dave, P., Bhindwale, R., and Helmy, A. (2004). Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks. In *Performance, Computing, and Communications, 2004 IEEE International Conference on*, pages 463–469.

[129] Twidle, K., Lupu, E., Dulay, N., and Sloman, M. (2008). Ponder2 - a policy environment for autonomous pervasive systems. In *Proceedings of the 2008 IEEE Workshop on Policies for Distributed Systems and Networks*, POLICY '08, pages 245–246, Washington, DC, USA. IEEE Computer Society.

[130] Vella, M. N. (2010). Survey of wireless sensor network security. *Texas A and M University-Corpus Christi, Computer Science Program*.

[131] VINT, P. (2012). The network simulator -ns-2. Technical report, University of Southern california.

[132] Wander, A. S., Gura, N., Eberle, H., Gupta, V., and Shantz, S. C. (2005). Energy analysis of public-key cryptography for wireless sensor networks. In *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*, PERCOM '05, pages 324–328, Washington, DC, USA. IEEE Computer Society.

[133] Wang, H., Sheng, B., and Li, Q. (2006a). Elliptic curve cryptography based access control in sensor networks. *Int. J. Secur. Netw.*, 1(3/4):127–137.

[134] Wang, S., Liu, K., and Hu, F. (2005). Simulation of wireless sensor networks localization with omnet++. *2nd International Conference on Mobile Technology, Applications and Systems*.

[135] Wang, W. and Bhargava, B. (2004). Visualization of wormholes in sensor networks. In *Proceedings of the 3rd ACM workshop on Wireless Security*, WiSe '04, pages 51–60, New York, NY, USA. ACM.

[136] Wang, Y., Attebury, G., and Ramamurthy, B. (2006b). A survey of security issues in wireless sensor networks. *IEEE Communications Surveys and Tutorials*, 8:20–23.

[137] Wang, Y., Smith, S. W., and Gettinger, A. (2012). Access control hygiene and the empathy gap in medical IT. Technical Report TR2012-713, Dartmouth College, Computer Science, Hanover, NH.

[138] Wang, Y., Wong, D., and Huang, L. (2011). A one-pass key establishment protocol for anonymous wireless roaming with PFS. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1 –5.

[139] Widenius, M. and Axmark, D. (2002). *Mysql Reference Manual*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 1st edition.

[140] William, M. (2007). A peek behind the OCR wall of shame. Technical report, Legal Issue, Developments and Other Pertinent Information Relating to the Creation, Use and Exchange of Electronic Health Records.

[141] Wood, A. D. and Stankovic, J. A. (2002). Denial of service in sensor networks. *IEEE Computer Society*, 35:54–62.

[142] Yao, Z., Kim, D., and Doh, Y. (2008). PLUS: parameterised localised trust management-based security framework for sensor networks. *Int. J. Sen. Netw.*, 3(4):224–236.

[143] Ye, F., Luo, H., Cheng, J., Lu, S., and Zhang, L. (2002). A two-tier data dissemination model for large-scale wireless sensor networks. In *Proceedings of the 8th annual international conference on Mobile computing and networking*, MobiCom'02, pages 148–159, New York, NY, USA. ACM.

[144] Yu, S., Ren, K., and Lou, W. (2011). FDAC: Toward fine-grained distributed data access control in wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.*, 22(4):673–686.

[145] Yuan, W., Guan, D., Hung, L. X., Lee, Y., and Lee, S. (2006a). A trust model with dynamic decision making for ubiquitous environments. In *Networks, 2006. ICON '06. 14th IEEE International Conference on*, volume 1, pages 1–6.

[146] Yuan, W., Guan, D., Lee, S., and Lee, Y. (2006b). A dynamic trust model based on naive bayes classifier for ubiquitous environments. In *Proceedings of the Second international conference on High Performance Computing and Communications*, HPCC'06, pages 562–571, Berlin, Heidelberg. Springer-Verlag.

[147] Yun, J.-H., Kim, I.-H., Lim, J.-H., and Seo, S.-W. (2007). WODEM: wormhole attack defense mechanism in wireless sensor networks. In *Proceedings of the 1st international conference on Ubiquitous convergence technology*, ICUCT'06, pages 200–209, Berlin, Heidelberg. Springer-Verlag.

[148] Zhang, J., Shankaran, R., Orgun, M., Varadharajan, V., and Sattar, A. (2010a). A dynamic trust establishment and management framework for wireless sensor networks. In *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, pages 484–491.

[149] Zhang, J., Shankaran, R., Orgun, M., Varadharajan, V., and Sattar, A. (2010b). A trust management architecture for hierarchical wireless sensor networks. In *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, pages 264–267.

[150] Zhang, R., Zhang, Y., and Ren, K. (2009). DPA2C: Distributed privacy-preserving access control in sensor networks. In *INFOCOM 2009, IEEE*, pages 1251–1259.

[151] Zhao, G., Chadwick, D., and Otenko, S. (2007). Obligation for role based access control. In *International Symposium on Security in Networks and Distributed Systems*, SSNDSO7 '07.

[152] Zhao, G. and Chadwick, D. W. (2008). On the modeling of Bell-LaPadula security policies using RBAC. In *Proceedings of the 2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, WETICE '08, pages 257–262, Washington, DC, USA. IEEE Computer Society.

[153] Zhou, Y., Zhang, Y., and Fang, Y. (2007). Access control in wireless sensor networks. *International School on Foundations of Security Analysis and Design*.

[154] Zhu, Y., Keoh, S. L., Sloman, M., Lupu, E., Zhang, Y., Dulay, N., and Pryce, N. (2008). Finger: An efficient policy system for body sensor networks. In *Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on*, pages 428–433.

[155] Zhu, Y., Keoh, S. L., Sloman, M., and Lupu, E. C. (2009). A lightweight policy system for body sensor network. *IEEE Transactions on Network and Service Management*.

Appendix A

Pipeline of Publications

A.1 An Adaptive Access Control Model with Privileges Overriding and Behaviour Monitoring in Wireless Sensor Networks

[Published in Q2SWinet'12: Proceedings of the 8th ACM Symposium on QoS and Security for Wireless and Mobile Networks]

An Adaptive Access Control Model with Privileges Overriding and Behaviour Monitoring in Wireless Sensor Networks

Htoo Aung Maw
University of Hertfordshire
Hatfield, United Kingdom
h.maw@herts.ac.uk

Hannan Xiao
University of Hertfordshire
Hatfield, United Kingdom
h.xiao@herts.ac.uk

Bruce Christianson
University of Hertfordshire
Hatfield, United Kingdom
b.christianson@herts.ac.uk

ABSTRACT
Wireless Sensor Networks (WSNs) have attracted a lot of interest in the research community because of their wide range of applications. Due to the distributed nature of WSNs and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. Access control is a critical security service in WSNs to prevent unauthorised access from the users. Current access control models in WSNs cannot make access control decisions efficiently and effectively when the system faces unexpected and unanticipated events because access control decisions are based on predefined access policies and roles. Sometimes, users may need to access stored data for emergency and immediate data access but the system cannot grant access to this kind of users' request. Based on the needs of real world requirements, we propose an adaptive access control model that builds on the concepts of overriding access privileges and user behaviour monitoring to provide a flexible approach in the access control model. The proposed access control model will adapt to unanticipated events by using privilege overriding and adjust its decision based on users' behaviour. The proposed approach can make an access control model much flexible and also detect abnormal users' request from the authorised users. To the best of our knowledge, the proposed access control model is the first to realize the flexibility of access control model by using the concept of possibility-with-override and users' behaviour monitoring in WSNs.

Categories and Subject Descriptors
C.2 [Computer-Communication Networks]*: General Security and Protection*:
C.2 [Computer-Communication Network]*:* Network Architecture and Design_*Wireless Communication*

General Terms
Design, Security

Keywords
Access Control, Wireless Sensor Networks, Overriding Access Control, User Behaviour Monitoring

Q2SWinet'12, October 24–25, 2012, Paphos, Cyprus.
ACM 978-1-4503-1619-4/12/10.

1. INTRODUCTION
Wireless Sensor Networks (WSNs) consist of hundreds or even thousands of distributed, autonomous, low power, low cost and small sized devices each with sensing, processing and communicating capabilities to monitor the real world environment and collect information through infra-structureless ad-hoc wireless network. Sensor networks are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring.

Nowadays, a sensor node has a capability of sensing data from environments and storing data locally in a distributed fashion or transmitting to central storage in a centralised approach. Stored data from sensor nodes are vulnerable and should keep secretly. In addition, access to the sensed and stored data needs to protect against from the unauthorized users. In many applications, data sensed by sensor nodes are related to security and privacy issue and should be accessible only to the authorised users. Users' access to that valuable data will be different based on access privileges of those users. Therefore, data confidentiality and control access to that data are two main requirements to provide in WSNs.

This paper focuses on access control in WSNs- i.e., how to prevent unauthorised data access from the users. Li and Gong [1] pointed out that WSNs suffer from many constraints like limited energy resources, memory, and low computation capability that impose unique security challenges and make innovative approaches desirable. Security techniques and access control models in other wireless technologies cannot be applied directly in WSNs because of its unique characteristic. As a result, existing security mechanisms and access control models are inadequate, ineffcient and new security approaches and access control models are desirable for WSNs. Towards addressing this challenges, this paper will propose an adaptive access control model with privileges overriding and behaviour monitoring, specially designed for WSNs.

2. BACKGROUND
Most of the current access control models in WSNs used traditional Role-Base Access Control model (RBAC) [2] to control user data access where roles and policies need to be defined in advance before the system makes an access decision. The decision is binary: denied access or permitted access. RBAC model has been widely accepted as a policy based access control model and it is suitable for most commercial applications. Some access control models use cryptographic methods for data storage and data access control but the systems still need to predefine attributes, roles and policies. In reality, it is impossible to predefine all the access needs for real

world applications because there may be unexpected events occurring in any situation and at any time.

There might be many situations, which cannot be defined in traditional RBAC model and cryptography based systems. For example, the roles and policies for emergency and unexpected situations cannot be defined in advance. When the system faces this kind of situations, what will the system do? In most of the emergency and urgent cases, the users cannot wait until someone comes and accesses data to the data sources. For real world applications, the system needs to be flexible enough to make access decisions based on unusual situations as well as on normal defined situations. In WSNs, using RBAC model cannot fulfill the requirements of the real world application. Therefore, a new access control model needs to introduce and develop for achieving the flexibility of access control in WSNs.

3. ADAPTIVE ACCESS CONTROL MODEL

In this section, a new access control model is proposed and named as an adaptive access control model with privileges overriding and behaviour monitoring. Adaptive access control model is an emerging concept that builds on the concepts of fine-grained access control, user behaviour monitoring and overriding access permissions to provide a flexible approach in access control. The proposed adaptive access control model can dynamically grant, deny and override permission based on overriding concept and user behaviour monitoring.

The main idea of the proposed approach is giving capabilities to the sensor nodes for making access decision and overriding access privileges in order to provide flexibility in the access control whenever unanticipated events occur at the sensor nodes. Possible, permit and deny access policies will be declared in the system, apart from that policies the system will use possibility-with-override [4] policies. In current access control models, all access decisions for users' request are depended on the predefined roles and policies. Comparing with current models, our proposed access control model can make overriding access decisions on any events based on user behaviour's trust value.

In the proposed model, the powerful sensor nodes may check user behaviour information whenever the user tries to access data at the sensor node. Users' permit access may be overridden to deny access by the access control model at sensor nodes because of their behaviour, even if the users possess the right access privileges. A central server will evaluate and calculate users' behaviour trust value and send it to all the base stationa in the sensor network by using broadcast communication. The proposed model aims to prevent the unauthorized, unusual and abnormal access from the users by using users' behaviour trust value. The proposed model is trying to achieve flexibility of the access control for making access decisions quickly and efficiently at the sensor node.

3.1 Overriding Access Privileges

In the proposed model, the owner of sensors' node will give an institutional power to the sensor node for decision-making process in the emergency and unexpected situations. There is a limited local decisions making capability in the current access control models because it is impossible to define the possibility of denial and permit access policies for all the situations. "Overriding of access control is one way for handling such hard to define and unanticipated situations where availability is critical" (J. Alqatawna et al) [3].

The propose model is based on the concept of discretionary overriding of access control by Rissanen et al [4]. When the system administrators pre-define security policies in an access control mechanism, there are different categories based on situation space. Rissanen suggested that there are three possible outcomes to an access request from users: denied, permitted and possible-with-override access. Based on these three possible outcomes, there are three ways to classify the situation. In this report, only "Define the permitted access and the denied access. By default everything else is possible"[16], will be used for our model. The system defines permitted and denied access policies for normal situations and leaves the possibility-with-override for the emergency and unusual situations as default. Users' behaviour trust values will be considered for overriding access decisions. Users' behaviour trust value will explain in next section.

3.2 Prevention and Detection Mechanism

Prevention and detection mechanisms will be used in overriding process as auditing to prevent the abuse usage of overriding. Whenever overriding cases occur at the access control mechanism, the system will keep a record of all the overriding processes for auditing. If there is no prevention mechanism in the access control model, all users might try to request overriding access privileges for the data access, whenever they want to access data at the sensor nodes. In my point of view, prevention and detection mechanism will be needed to protect unauthorised data access from the users.

All overriding operations are recorded as log file and the owner of a sensor node can be checked a log file whenever he receives alarm and warning message from the sensor nodes. Detection approach will be used in the auditing process. Sandhu and Samarati [6] mentioned that the role of auditing is an analysis of data to discover or diagnose the security violations. Audit data need protection from modification by an intruder. For triggering alarm and warning message, obligation roles will be used in the access control policies. An obligation is a requirement to take some course of action, whether legal or moral. Therefore, overriding and obligation policies should be defined in Ponder or WASL policy langusge in WSNs.

3.3 User Behaviour Monitoring

The proposed approach is trying to improve the flexibility in access control model by extending with user behaviour model. In current access control models, a user with right access privileges can access data and there is no way to prevent abnormal and unusual data access from the authorised user. User behaviour monitoring concept is proposed to check user behaviours and actions in WSNs. Whenever the users try to access data at the sensor nodes, the base stations will passively monitor user behaviours' information for the behaviour trust model.

The main idea of using base station as passive monitoring mechanism between users and sensor nodes is filtering and monitoring user behaviours and information like time, location, actions, etc. Monitored information by base station will be sent to a central server that calculates and evaluates user's behaviour trust value. For behaviour trust value, monitored user behaviour information will be compared with previous records, predict and predefine user behaviour information by using behaviour matrix algorithm in the central server.

Li-qin et al [5] mentioned that predicting user behaviour is important and significant in forming a trustworthy network. Measuring user behaviour is quite hard to evaluate and manage and it is a new research issue in WSNs. After evaluating and calculating trust value, central server will forward trust value to the base station. A base station will periodically broadcast to all the sensor nodes and update users' behaviour trust value for the overriding access decision-making process. User's behaviour trust value is important in making access decisions at the sensor nodes, when there is an unusual and abnormal data access from the authorised users. Users behaviour' monitoring engine will be designed and generated user's behaviour trust value for each user.

4. CONCLUSION AND FUTURE WORK

The overall contribution of this paper is to design an adaptive access control model for WSNs that combines both possible-with-override and behaviour monitoring concepts together. The adaptive access control model is enabling to make access decision quickly and efficiently, where the system faces unexpected events and abnormal or unusual situations. The adaptive access control model will be resided on each sensor node in WSNs. The flexibility of access control model is important to provide in WSNs, in term of efficiency, reliability, accountability and immediate data access. Designing a framework for user behaviour monitoring model is another objective to achieve in WSNs.

This paper proposed a new access control model to realise the privilege control of sensor networks, to solve the problems that users can only access the network at the specific time and the specific place and to provide overriding access decision-making process at the sensor nodes for emergency data access by achieving flexibility in an access control model. Currently we are working on the simulation and emulation tools to develop the proposed access control model in WSNs. For modelling and developing of the proposed access control in WSNs, IRIS version of sensor motes and IRIS Processor Radio Modules for based station will be used. Lotus motes are considered to use as powerful sensor nodes (base station) for passive monitoring. TOSSIM emulator will be used in development of the proposed model. Ponder and XACML language will be considered to define overriding and obligation policies and roles. The user behaviours' trust engine will be implemented in central server by using NS2 (Network Simulation 2) to check and evaluate the user behaviours' trust value. Overall, a new access control model is proposed for WSNs to achieve the flexibility in access control and prevent unauthorized, abnormal and unusual data access from both legitimate and illegitimate users in WSNs. To the best of our knowledge, the proposed access control model is the first to realize the flexibility of access control model by using the concept of possibility-with-override with users' behaviour trust value in WSNs.

5. REFERENCES

[1] Z. li and G. Gong. A Survey on security in wireless sensor networks. *Technical Report, University of Waterloo*, 2008.

[2] G. Zhao and D. W. Chadwick. On the modeling of bell-lapadula security policies using rbac. In *Proceedings of the 2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, WETICE '08,pages 257-262, Washington, DC, USA, 2008. IEEE Computer Society.

[3] J. Alqatawna, E. Rissanen, and B. Sadighi. Overriding of access control in xacml. *In Proceedings of the Eighth IEEE International Workshop on Policies for Distributed Systems and Networks*, POLICY '07, pages 87-95, Washington, DC, USA, 2007. IEEE Computer Society.

[4] E. Rissanen, B. S. Firozabadi, and M. Sergot. Towards a mechanism for discretionary overriding of access control. In *Proceedings of the 12th international conference on Security Protocols*, SP'04, pages 312-319, Berlin, Heidelberg, 2006. Springer-Verlag.

[5] T. Li-qin, L. Chuang, and N. Yang. Evaluation of user behaviour trust in cloud computing. *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, 2010.

[6] R. Sandhu and P. Samarati. Authentication, access control, and audit. *ACM Comput. Surv.*, 28(1): 241-243, Mar. 1996.

A.2 An Adaptive Access Control Model for Medical Data in Wireless Sensor Networks

[Published in Healthcom'13: 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services]

An Adaptive Access Control Model for Medical Data in Wireless Sensor Networks

Htoo Aung Maw, Hannan Xiao and Bruce Christianson
School of Computer Science
University of Hertfordshire
Hatfield, United Kingdom
Email: (h.maw,h.xiao,b.christianson)@herts.ac.uk

***Abstract*—Wireless Sensor Networks (WSNs) have recently attracted a lot of interest in the research community. The security mechanism with large overhead of computation and communication, are infeasible to apply in WSNs due to many constraints such as limited energy, resource and memory, and low computation capability. Current access control models cannot make an effective access decision in many events because access decisions are based on predefined access policies and roles. Sometimes, users may need to access important data urgently but apart from those predefined access policies, other user request will not be granted. An adaptive access control model is proposed aiming to provide a flexible and an effective access decision on user access request at any time. The proposed model is developed in Ponder2 framework with additional extensions to adapt the unexpected events by using privilege overriding and also adjust its decision based on users' behaviour trust value. A medical scenario is used as an example application to develop and evaluate the proposed model in Body Sensor Networks (BSNs) and WSNs. In this paper, detailed design, implementation phase, evaluation result and policies testing for the proposed adaptive access control model are presented. Based on an evaluation result, all the modules in the proposed access control model are cooperated to make an effective access decision.**

I. Introduction

Wireless Sensor Networks (WSNs) technology has been the interest of researchers and scientists in many research areas because of their potential to change the way of living with applications in retail, medicine, emergency management and many other areas. WSNs consist of hundreds and even thousand of low-cost small sized sensor nodes each with sensing, processing and communicating capabilities to monitor the real world environment and collect information through infrastructureless ad-hoc wireless networks. Nowadays, a sensor node can capture multimedia data and store data locally as the distributed manner or transfer it to a central storage as the centralized manner. WSNs become popular and play an essential role in the medical or healthcare domain. Wireless sensor nodes become smaller and more powerful to use in a wide range of medical applications such as health monitoring, chronic disease management and measuring user vital signs. Garci-Morchon and Wehrle [1] mentioned that user's medical data lead to security and privacy concern. Therefore, collected and stored data are important and it should be kept secretly. Additionally access to that private data needs to protect unauthorized access from both legitimate and illegitimate users. Using security mechanism can provide the security properties such as confidentiality, authentication, integrity, etc. and can prevent abnormal access from the internal and external users.

This paper focuses on an access control model in WSNs and Body Sensor Network (BSN). There are many constraints such as limited memory and power, which impose unique security challenges and make innovative approaches desirable in WSNs. A new security mechanism and access control model are needed because existing security mechanisms are not efficient, adequate and suitable to use and apply in WSNs. Towards addressing these challenges, this paper discusses an adaptive access control model and its implementation result in Ponder2 framework. The remaining structure of this paper is explained as follows. Section 2 discusses the related work. Section 3 provides an overview of the proposed access control model. In section 4, the development and implementation of an adaptive access control model are discussed. Section 5 represents an evaluation result based on a medical scenario. Section 6 concludes the paper.

II. Related Work

Access control is a critical security service to prevent unauthorized access of network resources from the users. In WSNs, users can enter the sensor field directly to access data at the sensor nodes. Different users may have different access privileges to access data at the sensor nodes based on their roles and policies. Most of the access control models in WSNs and Wireless Medical Sensor Network (WMSN) are based on traditional Role-Based Access Control (RBAC), which has been widely accepted as a policy access control model. Cryptography-based access control is designed for the untrusted environment, where the lack of global knowledge and control is defining characteristics. Cryptography is relied upon to control data access and to ensure data confidentiality and integrity. Cryptography methods in WSNs should meet the constraints of sensor nodes.

Distributed PRIvacy-preserving aCCESS control (PRICCESS) protocol [2] is proposed to provide privacy preserving distributed access control in WSNs. The PRICCESS model used Access Control List (ACL) to store the access permission of the group in the network controller. For ACL, roles need to be predefined in advance based on RBAC. Garci-Morchon et al [1] pointed out that RBAC model is not good enough to use in WSNs because in the traditional RBAC model, the roles and policies have to be predefined in advance. Based on that point of view, they proposed the Context-Aware RBAC [1] model for WMSNs. An access control decision will be based on the modular contextual information such as normal, emergency and critical, to ensure the users' safety. In normal situations,

978-1-4673-5801-9/13/$26.00 ©2013 IEEE

a user needs to verify his role to access the medical data of a healthy patient. The user can perform any action and can access data, when the system declares as critical and emergency case. One of the disadvantages of this model is, there is no prevention or detection mechanism and no verification process to check user's data access, when the critical situation occurs.

Ferreria et al [3] proposed the Break-the-Glass Role Based Access Control (BTG-RBAC). The main idea of this model is to gather necessary information from end users with their collaboration for usable access control policy that can perform BTG action in emergency cases. BTG extension is used for emergency and important cases whenever a user wants to access data urgently and immediately. When the user tries to perform BTG actions, the system will ask him if he really want to perform that action on specific object. If the user answers affirmatively, the system will activate the BTG operation and trigger the associated obligations like alarms, log file, etc. BTG-RBAC model is much more flexible than normal RBAC but one of the disadvantages is that human processes are needed in order to enforce the BTG rules.

Yu et al [4] proposed Fine-grained Data Access Control (FDAC) model which is based on Attribute-Based Encryption (ABE) [5]. The main idea of their approach is to provide a fine-grained access control over sensor data and is resilient against the attacks such as user colluding and node compromising. Their model is based on a centralized approach because only the network controller is managed for key management. If the network controller is compromised, there will be no security provisioning in the network. Therefore, a single point of failure can be occurred. In this approach, CP-ABE based selective broadcast is used for the user revocation and key revocation but there is no detailed information on how to use it.

To avoid a single point of failure, Ruj et al [6] proposed an access control scheme based on Multi-authority Attribute Based Encryption. Their objective is to provide fully distributed data access control by using several Distribution Centers (DCs). All the access structures from each DC, which need to satisfy the attributes from sensor nodes, are ANDed together to get a complete access for the single user. There is no detailed explanation of how to combine all the access structures together. Without the combining approach, the user has to store all the access structures in order to access different types of data from the sensor network.

From the above discussion, it is clear that achieving fine-grained data access control with flexibility is still an open challenge in WSNs. There is no protection for unauthorized usage from both legitimate and illegitimate users. A flexible access decision is needed because it is hard to predict and predefine data access policies for any unexpected and unanticipated events in the real world applications. Current access control models are not flexible enough to make an effective access decision at any time. Therefore, we proposed an adaptive access control model [7] to fill the gap in WSNs area. The proposed model has a similar structure like BTG access control model but the main difference is that no human effort is needed to override rules and policy for unexpected events because of the introduction of users' behaviour trust model, and prevention and detection mechanism.

III. Adaptive Access Control Model

Previously, we have proposed an adaptive access control model [7] to provide a flexible access decision in WSNs. The proposed model is incorporated the concept of possibility-with-override [8] into WSN for hard-to-define and unanticipated situations. Possibility-with-override means users might be able to override a denial of access, when unexpected events occur. The proposed model also uses user behaviour monitoring and trust model to check users' actions, location, time, etc. Whenever users try to access data at the sensor nodes, all user behaviour and user information will be kept by prevention and detection mechanism as an audit record to detect and prevent abnormal and unauthorized access. The detailed information of different modules inside the proposed adaptive access control model are explained in this section.

There are two main modules in the proposed access control model: Policy Enforcement Point (PEP) and Policy Decision Point (PDP). Whenever a user requests the access to an object, an access request will go through PEP for the authentication process and then it will forward a decision request to PDP for decision making process. PDP makes the access decision on user request based on defined policy. The decision response will be forwarded internally to the target. Also, PDP will forward the decision response to the users, whether they have the privileges to access data at the sensor nodes or not.

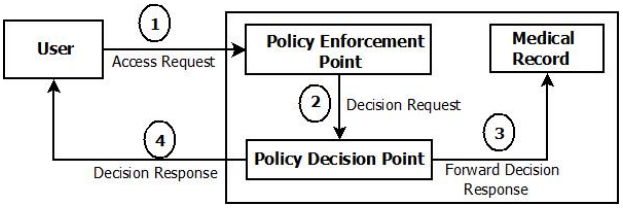


Fig. 1. An Overview of Implementation Framework

The proposed access control model is extended version of Ponder2 [9] by adding extra module and using additional information to provide flexibility. The proposed model is designed to make an effective access decision in both normal and emergency situations. Figure 1 shows the high level overview design of the proposed access control model. The detailed information of both PEP and PDP are explained in next sub section.

A. Policy Enforcement Point (PEP)

In the proposed framework, PEP is used as an authentication service provider between users and sensor nodes. The authentication service is an important security provisioning to provide in the system. Whenever PEP receives an access request from the user, it will check the user information like ID and cryptographic key for the authentication purpose. PEP checks the authenticity of the users, before it forwards the decision request to PDP. Currently, we assume that authentication service and key distribution are already provided in PEP. In future, we will work on the implementation of PEP by using Attribute-Base Encryption (ABE) [5] for data storage. Also Two-Tier Data Dissemination (TTDD) [10] protocol is considered to use for data transmission between users and nodes.

B. Policy Decision Point (PDP)

PDP is a main module in the proposed framework. There are three different modules inside the PDP as shown in Figure 2. These three modules are; the access control module, prevention and detection module, and user behaviour trust module. After PEP forwards the decision request to PDP, the information such as user, action, environment and context information will be forwarded to the access control module and the user behaviour trust module. The user behaviour trust module will calculate the trust value and forward that value to the access control module. The access control module will use the trust value from the user behaviour trust module and the other information, which is forwarded by PEP, to make access decisions on the user request. After the access control module makes a decision, it sends back a response message to the users and forwards internally to the target object. The three different modules of PDP are explained as follows.

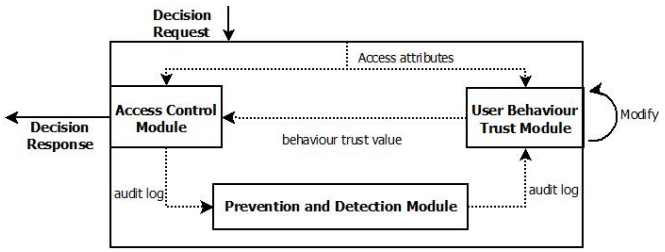


Fig. 2. Policy Decision Point

1) Access Control Module: The access control module is used to make an access decision based on access policies which are predefined in that module. In a normal access control model, there are two access decisions: permitted and denied access. If the user has the privileges to get data at the sensor nodes, his access will be permitted. If the user does not have rights to access data, his access will be rejected. In the proposed model, overriding access is introduced to provide flexibility and make access decisions effectively and efficiently, when the user needs to access data immediately. The access control module will only grant the overriding access to the user, when his trust value is high or trustworthiness enough to access data. Altogether, three access decisions are used in the proposed access control module: permitted access, denied access and overriding access.

In the access control module, there are several predefined authorization, obligation and overriding policies. In the proposed model, the permitted and denied access will be defined. By default, everything else is possible to override. The authorization policy will handle for normal permitted and denied access. The overriding and obligation policy will be used to make an effective access decision based on user behaviour trust value in unexpected events. The detailed definition of these three policies are explained as below.

- Authorization Policy
  An authorization policy is used to enforce the access control module to check whether a subject is authorized to execute an action on a target. In the authorization policy, subject, target, condition and action are used to define access role. Subject means a user, who is trying to access data from the target that stores information. Whenever the access control module receives a decision request, it will check the conditions i.e, location and time which are declared in the specific policy. If the decision request meets the criteria from a certain policy, the subject is allowed to do some actions at the target.

- Obligation policy
  An obligating policy expects zero or more conditions to be evaluated and one or more actions to be performed if the conditions are satisfied. One of the objectives of using an obligation policy is to provide finer-level access control than mere permitted and denied decisions. After a policy has been evaluated, specific obligations are sent along with the authorization decision. The obligation policies are used when the access control module is faced with abnormal user behaviour or overriding access.

- Overriding Policy
  The proposed adaptive access control model introduces an overriding policy based on a user behaviour trust module. Overriding of access control is one way to handle such hard-to-define and unanticipated situations where availability is critical. An overriding policy is used to support flexibility of access control in the proposed model. The policy is designed especially for unpredictable and unexpected situations. Current access control models cannot make an effective access decision based on predefined policies and roles, when an unexpected event occurs. It is hard to predict all of the access control policies because unpredictable events can happen at any time. Comparing the proposed model with other access control models, it provides a flexible approach to make the effective access decisions.

2) Prevention and Detection Module: The privacy and confidentiality of data are still provided even in the emergency case because of the prevention and detection and user behaviour trust module. The prevention and detection module is introduced to prevent abnormal and unauthorized access from both legitimate and illegitimate users. The main idea is to keep the information from user access request as an audit record. The audit record maintains a record of user activities in the system. An audit record can assist to detect security violations and flaws in the system.

In the proposed model, an event-oriented log method is used. The purpose of an event-oriented log is to record an event and specify when it occurred, the user information associated with that event and the results of the decision-making process. The prevention and detection module is used to prevent any specious access from the users to protect confidentiality and privacy of data. An audit record will be used by the user behaviour trust module to predict and calculate the user behaviour trust value for the user's next attempt. We will use ABE based encryption which is already explained under PEP section, to provide confidentiality and integrity of the audit data. The TTDD protocol is considered to provide a secure communication channel for data transmission within BSN and WSN.

3) User Behaviour Trust Module: In current access control models, a user with right access privileges can access data. There is no way to prevent abnormal data access from the authorized user. The proposed model can be protected from these kind of situations by using both the prevention and detection module, and the user behaviour trust module together. In the proposed model, the users' behaviour trust value is calculated and evaluated based on the audit record from the prevention and detection module. The behaviour trust value will be forwarded to the access control module and stored in a database for another evaluation process. The overall structure of users' behaviour trust module is shown in Figure 3. To determine the user behaviour trust value,

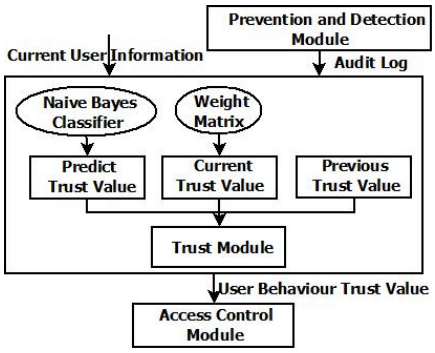


Fig. 3. A Framework of User Behaviour Trust Module

the previous, predicted and current value of user behaviour trust will be used. Current trust value will be calculated and evaluated based on the user information that is forwarded by the PEP. The previous trust value is stored in the trust module. For predicting user behaviour trust value, Naive-Bayes classification algorithm [11] will be used. The predicting user behaviour is important and significant in forming a trustworthy network. For the classification algorithm, the audit record from the prevention and detection module will be used. There might be more than two classifiers to predict the user behaviour trust value. Overall, the behaviour trust value of the user is calculated based on previous, predicted and current user trust value.

IV. Development of An Adaptive Access Control Model

The proposed adaptive access control model has been developed in Ponder2 [9] that is a popular policy language to use in BSN. Ponder2 comprises a self-contained, stand-alone, general-purpose object management system with message passing between objects. It incorporates an awareness of events and policies and implements a policy execution framework. It has a high-level configuration and control language called PonderTalk and user-extensible managed objects are programmed in Java.

Ponder2 is implemented as Self Managed Cell (SMC) [12] that is a set of hardware and software components forming an administrative domain. It is capable of self management. We assumed SMC as a sensor and try to implement access control model within the Ponder2. Everything in Ponder2 is a managed object. The managed object has to be loaded dynamically into the SMC from a library, thereby producing the factory managed object (Java class). The proposed model is an extended version of Ponder2 by applying possibility-with-override concept, user behaviour trust model and prevention, and detection mechanism together.

We developed the proposed adaptive access control model based on Ponder2 framework. The interface for all the users are implemented in Java based on the managed objects in Ponder2. The Java class file will be loaded dynamically into SMC. The access control module is already implemented for the proposed model and defined the policies based on an application scenario. We designed and implemented the prevention and detection module in Ponder2. The interface for the audit log is implemented in Java. The audit log keeps all the information from user requests, whenever users try to access patient medical records from any location at any time. The audit log is stores as "Write.csv" file that will be used by the user behaviour module to evaluate the trust value of each user. For the users' behaviour trust module, a simple calculation is used and developed. In future, we need to do more work on the user behaviour trust module.

V. Evaluation of Adaptive Access Control Model

In this section, a medical scenario is used to develop the proposed model for BSNs and WMSNs. The policy specification for all scenarios is similar but an access policy for example medical scenario is discussed in this section. SMC [12] is represented as a BSN. In this example, each patient has his own BSN, which consists of several sensors. Sensors sense and collect information such as glucose level, temperature, heart rate, etc. We assumed that sensed data are stored as the medical record in BSN. Users such as doctors and nurses are trying to access medical record of the patient via mobile, personal digital assistant or personal computer. For example, sensors can interact with each other via IEEE 802.15.4 wireless links and interactions with other mobile phone and personal digital assistant from users via Wifi or Bluetooth. Each SMC has its own policy management. Policies are managed by each SMC specifying which actions can be performed. For doctor and nurse, context information will be used, when they try to interact with other SMC or request to join the patient's BSN for data access. The following example scenario will show and express how the proposed access control model is designed and developed for WSNs.

In an example scenario, users are doctors, nurses, patients, patient's family and administrative staff. We assumed that all the users in this scenario are in a "Hatfield" hospital. All the users will try to access the medical record of the patient. Based on their access privileges, the access to the patient medical record will be different. Therefore, access policies are based on the users responsibility, their role and context information such as location and time. A simple scenario of medical application will be used to express and state the policy clearly.

There are two departments in an example scenario: Heart and Cancer department. Nurses and patients will be assigned in one of the department. A doctor can be assigned in the same department as nurse and patient or he can be assigned in any other department. The doctor should be a physician of Heart or Cancer department or General Practitioner (GP) in

"Hatfield" hospital. The doctor and nurse can access patient medical records with a normal authorization policy when they are in the same department as the patient. But the nurse and doctor cannot access the medical record of another patient, who is not in the same department as they are. Otherwise, there might be a lack of data privacy for patient's medical record. For such a case, the overriding policy is used to override the denied access in urgent and emergency cases.

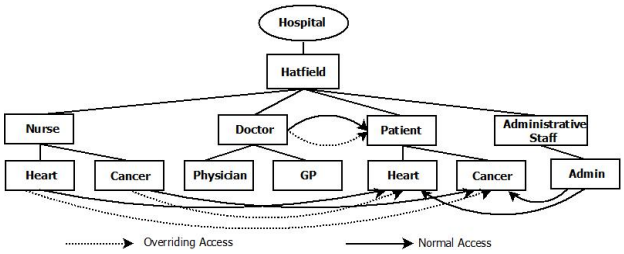


Fig. 4. Normal and Overriding Access

The patient's family might try to access data. They will have the access to the medical record but some important information will be hidden because of patient confidentiality and data security. It is the same for administrative staff. They can only access patient information like name, department and other general information, which means that they are not allowed to request the illness and prescription of the patient. Therefore, based on the role, responsibility of users and trust value, the access control model will make an effective access decision on user requests. Figure 4 explains the overview of normal and overriding access with an example scenario.

A. Evaluation Framework Based on Example Scenario

We evaluate and test the proposed adaptive access control model based on an example scenario. In this section user interface, policies definition of authorization, obligation and overriding, and audit log interface are explained based on the example scenario.

1) User Interface: The Interfaces for all the users in an example scenario have more or less the same feature but the information from the patient medical record will be changed based on their roles and access privileges. Consequently, the access decision will be different for each user. The interface of the nurse is shown in Figure 5.

In Figure 5, a user needs to give input of the patient path that includes the name and location of the patient. For example, Bob is a patient from the Heart department. The path of "Bob" is expressed as /patient/heart/bob. Aung is a nurse from Cancer department by looking at his path; /role/nurse/cancer/aung in above figure. All the trust values for the nurse and doctor are initialized as 5 that is average trust value. The range of the trust value is from 0 to 10. The user needs to fill the time framework, which is between one to twenty-four represented as twenty-four hours in a day. Time framework can be used to check time constraint, e.g a nurse can have access to the patient medical record only at a certain period of time. It is also part of information that will be used to predict the trust value of users.

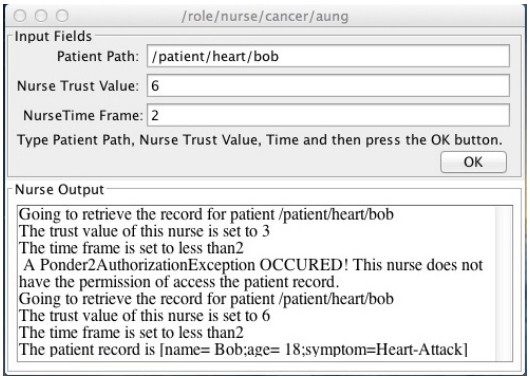


Fig. 5. Interface of A Nurse

Figure 5 also shows the access results of the decision-making process and medical record of the patient. The first result shows that, the nurse from Cancer department cannot access the medical record of the patient from Heart department. Therefore, his access request has been denied because he does not meet any criteria from the authorization policy. The second result shows that if a nurse's trust value is higher than average trust value, he can get the patient medical record from Heart department by overriding his denied access. The access control module assumes that he is trustworthy to access the medical record based on previous interaction between other patients and behaviour trust values. All the permitted, denied and overriding access of the users are kept as an audit record that is used to predict trust value of the users.

2) Authorization Policy: Authorization policy is used for normal permitted and denied access in the proposed model. For example, a nurse sends the access request to a target. The access control module will respond to access request based on the access policy, which is defined in that module for decision making process. The authorization policy can be changed based on the requirements of the application. There might be several authorization policies based on the users' level and access privileges. An example authorization policy is expressed as below:

Def: Permit-Policy
subject nurse **or** doctor
action getrecord
target patient from which department
condition location **or** time
focus target **or** subject

The above permit-policy defines that who has a right to access the medical record from a target object. Subject can only access the target object, when it meets the criteria from the permit policy such as condition. The authorization policy can be handled based on predefined policies, apart from that all the access requests will be denied. For example, the nurse from the Heart department can access medical record of patients from the same department.

3) Obligation Policy: Obligation policy is used in some events to prevent a certain condition. For example, if a nurse meets the criteria to override access policy, the obligation policy will be used and sent along with the overriding policy. Obligation policy is used for triggering an alarm and kept the audit record for further investigation. For example, if the

nurse's trust value is less than 5, his access will be denied. At the same time, the obligation policy will become active and keep the audit record based on user information and access request. Additionally, the security alarm will be triggered at the patient side. The format of obligation policy is shown as below.

Def: Audit-Log
on auditrecord
if policy type is override
or trust value is $<$ 5
do write.audit $<$ subject, Time, Target, Behaviour Trust Value, Context Value $>$

4) Overriding Policy: The proposed model extends the Ponder2 by adding an overriding policy. The overriding policy will check one or more one conditions for decision making process at the access control module. A user should be a nurse or a doctor and he can access data from anywhere at any-time. The nurse or doctor needs to meet at least two criteria to override the denied policy. The important factor is the user behaviour trust value which has to be over five to override the policy. If the trust value is set to zero, the person is untrustworthy but if it is set to ten, the person is trustworthy. To override the access policy, the subject have to meet more than one condition that are described as follow:

Def: Overriding-Policy
subject nurse **or** doctor
target patient <medical record>
if trust value is $>$ 5
and location = Hatfield
or time is between 8am to 10am
or nurse **or** doctor is staff
do Set-alarm **and** Audit-Log
action getrecord

For example, if a nurse wants to override his access policy in an emergency or urgent case, his user behaviour trust value has to be more than 5 and at least two of the above conditions need to be trued.

5) Prevention and Detection Mechanism: The prevention and detection mechanism keeps all the information from the user requests as an audit log, whenever users try to access patient medical records from any location at any time. The audit log can be seen on Figure 6. In the audit log format, the subject is a user, who tries to access medical record from the target. In the audit log, time, user behaviour trust value and context information such as location are also recorded. For example from Figure 6, "Doctor Oliver", who works as a "Physician" in "Hatfield" hospital, tried to access the medical record of "Bob" from "Heart" department at "12am" with his trust value "5" and his access request has been permitted.

Auditlog := [Subject + Time + Target + Trust Value + Context Value]

6) User Behaviour Trust Module: The user behaviour trust module used all the information from the audit log to evaluate and calculate the current and predicted user behaviour trust value. When the application is started, the trust value of all the users is initialized as five which is an average trust value. The trust value will be set between zero and ten based on the trust level of the users. The proposed user behaviour module is

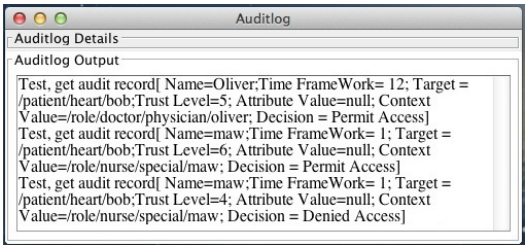


Fig. 6. Audit Log

not finished yet. The overriding policy is tested by giving the user trust value manually. Currently, the simple calculation is used for user behaviour trust value. Whenever the user access request has been permitted, his trust value will be increased by one. If it is a denied access, his trust value will be decreased by one. The user behaviour trust value is forwarded to the access control module. The computation effort of trust model will be evaluated after it is finished completely. The trust model needs to be analyzed and implemented carefully to meet the requirements of WSNs.

B. Summary

Based on the evaluation result with an example medical scenario, the access control module is cooperated with the user behaviour trust module, which worked together with prevention and detection mechanism to evaluate and calculate a trust value of users, to make an effective access decision. All policies are predefined in the access control module, which can adjust its decision based on trust value at any time. Based on the previous discussion, the overriding policy is useful to handle unanticipated situations. Therefore, all the modules in the proposed access model are worked together to make the effective access decision.

VI. Conclusion and Future Work

The overall contribution of this paper is to design and develop an adaptive access control model for medical data in BSNs and WSNs. In this paper, the interface of the example application, the development of possibility-with-override, and the prevention and detection mechanism are developed in Ponder2. The proposed model is developed in Ponder2 framework with additional extensions to adapt the unexpected events by using privilege overriding and also adjust its decision based on users' behaviour trust value. All the modules in the proposed access control are cooperated to make an effective access decision. In this paper, detailed design, implementation result and policy testing for the proposed adaptive access control model are discussed.

Currently, we are working on the user behaviour trust module. A classification algorithm will be used to predict the user behaviour trust value. The previous, current and predicted user trust value are needed to calculate the overall trust value of the user. It is also important to clean up the data from the audit log to use it for the classification algorithm. Further research is needed for how Naive-Bayes and weight metric algorithm can be applied in the user behaviour trust module. In future, we plan to implement the proposed adaptive access control model within the sensor nodes. IRIS version of sensor motes, IRIS

Processor Radio Modules and Lotus motes are considered for the implementation of the proposed model.

ACKNOWLEDGEMENT

The authors would like to thank Kevin P. Twidle who helped and gave a source code of the whole Ponder2 project.

REFERENCES

[1] O. Garcia-Morchon and K. Wehrle, "Modular context-aware access control for medical sensor networks," in *Proceedings of the 15th ACM symposium on Access control models and technologies*, ser. SACMAT '10. New York, NY, USA: ACM, 2010, pp. 129–138.

[2] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor network," *IEEE Transactions on wireless communications*, 2011.

[3] A. Ferreria, R. Correia, H. Monterio, M. Brito, and L. Antunes, "Usable access control policy and model for healthcare," *Computer Based Medical System(CBMS)*, 2011.

[4] S. Yu, K. Ren, and W. Lou, "Fdac toward fine-grained distributed data access control in wireless sensor networks," *IEEE Transaction on Parallel and Distributed Network*, 2011.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, ser. SP '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334.

[6] S. Ruj, A. Nayak, and I. Stojmenovic, "Distributed fine-grained access control in wireless sensor networks," in *IPDPS*, 2011, pp. 352–362.

[7] H. A. Maw, H. Xiao, and B. Christianson, "An adaptive access control model with privileges overriding and behaviour monitoring in wireless sensor networks," in *Proceedings of the 8h ACM symposium on QoS and security for wireless and mobile networks*, ser. Q2SWinet '12. New York, NY, USA: ACM, 2012, pp. 81–84.

[8] E. Rissanen, B. Sadighi, and M. Sergot, "Towards a mechanism for discretionary overriding of access control," *International Association for Cryptographic Research*, 2004.

[9] K. Twidle, E. Lupu, N. Dulay, and M. Sloman, "Ponder2 - a policy environment for autonomous pervasive systems," in *Proceedings of the 2008 IEEE Workshop on Policies for Distributed Systems and Networks*, ser. POLICY '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 245–246.

[10] H. Luo, F. Ye, J. Cheng, S. Lu, and L. Zhang, "Ttdd: A two-tier data dissemination model for large-scale wireless sensor networks," in *In Proceedings of International Conference on Mobile Computing and Networking (MobiCom*, 2003.

[11] C. K. I. Williams and D. Barber, "Bayesian classification with gaussian processes," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 20, no. 12, pp. 1342–1351, 1998.

[12] E. Lupu, N. Dulay, M. Sloman, J. Sventek, S. Heeps, S. Strowes, K. Twidle, S.-L. Keoh, and A. Schaeffer-Filho, "Amuse: autonomic management of ubiquitous e-health systems," *Concurr. Comput. : Pract. Exper.*, vol. 20, no. 3, pp. 277–295, Mar. 2008.

A.3 A Survey of Access Control Models in Wireless Sensor Networks

[Published in JSAN'14: Journal of Sensor and Actuator Networks]

J. Sens. Actuator Netw. **2014**, *3*, 150-180; doi:10.3390/jsan3020150

OPEN ACCESS

Journal of Sensor and Actuator Networks

ISSN 2224-2708

www.mdpi.com/journal/jsan

Article

A Survey of Access Control Models in Wireless Sensor Networks

Htoo Aung Maw *, Hannan Xiao, Bruce Christianson and James A. Malcolm

Department of Computer Science, University of Hertfordshire, Hatfield, AL10 9AB, UK;
E-Mails: h.xiao@herts.ac.uk (H.X.); b.christianson@herts.ac.uk (B.C.);
j.a.malcolm@herts.ac.uk (J.A.M.)

* Author to whom correspondence should be addressed; Email: h.maw@herts.ac.uk

Received: 23 January 2014; in revised form: 20 May 2014 / Accepted: 11 June 2014 / Published: 20 June 2014

Abstract: Wireless sensor networks (WSNs) have attracted considerable interest in the research community, because of their wide range of applications. However, due to the distributed nature of WSNs and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. Resource constraints in sensor nodes mean that security mechanisms with a large overhead of computation and communication are impractical to use in WSNs; security in sensor networks is, therefore, a challenge. Access control is a critical security service that offers the appropriate access privileges to legitimate users and prevents illegitimate users from unauthorized access. However, access control has not received much attention in the context of WSNs. This paper provides an overview of security threats and attacks, outlines the security requirements and presents a state-of-the-art survey on access control models, including a comparison and evaluation based on their characteristics in WSNs. Potential challenging issues for access control schemes in WSNs are also discussed.

Keywords: wireless sensor networks; access control schemes; security mechanisms; security vulnerabilities

---

1. Introduction

A wireless sensor network (WSNs) consists of hundreds or even thousands of distributed, autonomous, low-power, low-cost, small-sized devices, each with sensing, processing and

communication capabilities. Typically, these devices, known as sensor nodes, monitor the real-world environment and send the collected information to a gateway node through an infrastructure-less *ad hoc* wireless network. Sensor networks are envisioned to play an important role in a wide variety of areas, ranging from critical military surveillance applications to forest fire monitoring. WSN technology has been of interest to scientists in many research areas, because of its potential to change our way of living, with applications in entertainment, travel, retail, industry, medicine, health-care, traffic monitoring, military, emergency management, *etc*.

Among these applications, the military and medical applications are the most security-oriented fields of WSNs and have received the most attention from security researchers. WSNs are rapidly becoming an important technology in the medical or healthcare domain. Sensor nodes are becoming smaller and more powerful, making them suitable to use in a wide range of medical applications, such as health monitoring, chronic disease management and measuring user vital signs. Wireless medical sensor network (WMSN) is the name of this form of WSN used in the medical and healthcare domain. In WMSN, sensors are attached to the human body to monitor healthcare information, like electrocardiogram (ECG), blood pressure, *etc*. Medical staff can access, collect and record medical data directly from a patient's sensor for remote healthcare monitoring services. However Garcia-Morchon [1] mentioned that there are security and privacy concerns about possible access to user's medical data. Therefore, security services are required to provide the confidentiality of medical records and privacy of patient information. In addition, the control of access to patient's data becomes another issue in WMSN, because there might be a number of medical staff and family members, who try to interact with the confidential medical data.

WSNs can also be used for a number of purposes in the military sector, such as enemy tracking, military activities monitoring and battlefield surveillance. The rapid deployment, self-organization and fault tolerant characteristics of sensor networks make them a very promising data gathering technique for military Command, Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance (C4ISR) [2]. In military applications, the sensor nodes are used to collect the information of enemies and tracking military vehicles. The data sensed and stored at the sensor nodes are highly confidential, so security services, such as confidentiality, integrity, *etc.*, need to be provide by using security and access control mechanisms.

Nowadays, a sensor node can capture pictures and multi-media data. A sensor node has the capability of sensing data from the environment. It stores the sensed data locally in a distributed fashion or transmits the sensed data to central storage in a centralized approach. In both the centralized and distributed approach, data security and data access control are important issues in WSNs. As a large amount of data is stored in the sensor nodes locally, aspects of data security (such as confidentiality and integrity) have become serious concerns, because the sensor nodes are not well equipped with tamper-proof or tamper-evident equipment. From a data-centric point of view, the most challenging issues in WSNs are how to store the highly sensitive sensor data and how to control the access of internal and external users.

Based on the above discussion, access control is a critical security requirement to protect sensitive sensor information from unauthorized access, but it has not received attention in the context of WSNs by researchers. Data in real-time WSNs applications are made available to users on demand. Faye *et al.* [3] mentioned that the sensed data may no longer be accessed only at the base stations, and users can access data at the sensor node directly from anywhere in an *ad hoc* manner. Depending on user's access control

privileges, data access to the sensor nodes will be different. In this report, we will survey and discuss the state-of-the-art for access control schemes in WSNs.

The remainder of this paper is organized as follows. Background information of security vulnerabilities and security requirements and the traditional access control models for information systems are discussed in Section 2. Section 3 reviews WSN access control models that are proposed as models in the literature. Section 4 compares the current access control models based on characteristics, such as network architecture, key management, *etc*. Section 5 evaluates these access control models qualitatively and quantitatively. Section 6 discusses the potential research issues of access control models in WSNs, and finally, Section 7 concludes the paper.

2. Background

In WSNs, there are several attacks that can break the security services, such as confidentiality, availability, integrity, authenticity, *etc*. These security services can be protected in WSNs by using security mechanisms. In this section, we discuss the security vulnerabilities and security requirements for WSNs. We then introduce the traditional access control models. Access control is one of the security mechanisms that needs to be provided in WSNs.

2.1. Security Vulnerabilities and Security Requirements

The nature of WSNs makes them vulnerable to various kinds of attack. Security attacks can be categorized as passive or active: malicious users could either intercept private information or send false messages to the sensor nodes in WSNs. The listening and monitoring of the communication channels by unauthorized and malicious users are regarded as passive attacks. Sensor nodes can sense and collect data from their environments in WSNs; as a result, the network becomes vulnerable to potential abuse of these data resources. Vella [4] mentioned that the data obtained by sensing nodes need to be kept private and confidential. Since the data are stored in the sensor nodes without tamper-proof or tamper-evident equipment, the privacy and confidentiality of data become important to protect from passive attacks, such as eavesdropping, passive monitoring and traffic analysis [5].

An active attack can monitor, listen and modify data streams in the communication channels, where an adversary can maliciously disturb the communication channels between the sensor nodes. In harmful active attacks, the adversary can alter and spoof the packets and interfere with the wireless signals to jam the network. Ng *et al.* [6] argued that even if the information is protected from eavesdropping by means of encryption, the attacker may blindly modify that encrypted information and turn the information into meaningless information. The common active attacks in WSNs include camouflage [7], Sybil [8], wormhole [9], replay, hello flood [10], sinkhole [5], denial of service (DoS) [11] and node replication [5].

Apart from the active and passive attacks, Perrig [12] suggested that there might be other types of attack, which are not yet identified in all layers of the TCP/IP protocol stack in WSNs. Securing WSNs against all of the attacks and threats is a challenging task. WSN is considered a highly distributed and *ad hoc* approach, and because of that, the security requirements and goals of WSNs should be well studied and provided. The aim of security is to protect the right thing in the right way. Gligor [13] pointed out

that "A system without an adversary definition cannot be insecure. It can only be astonishing". WSNs are vulnerable to many attacks, because of the broadcast nature of the transmission links and the unprotected physical environment. Therefore, we need to analyze carefully which things need to be protected against which threats and how these attacks and threats can be detected and prevented. The security goals for WSNs are similar with other network technologies. Security properties, such as confidentiality, integrity, availability, access control, authorization, authentication, freshness and secure localization, need to be provided in WSNs.

In WSNs, there are two additional requirements which need to be investigated for the security of sensor networks because there may be situations like new sensor nodes are joined and deployed and old sensor nodes are failed to operate in the networks. Based on these requirements, Wang *et al.* [14] suggested that forward and backward secrecy need to be considered in WSNs. Forward secrecy means that an old sensor node should not be able to read any message after it leaves the sensor networks. Backward secrecy means that a new sensor node should not be able to read any previous message sent before it joined the sensor network.

Table 1. Security properties, security attacks and possible solutions in WSNs [6,9,15–17].

Security Properties	**Security Threats**	**Possible Solutions**
Confidentiality	Message Disclosure	Encryption, Access Control
Integrity	Message Modification	Digital Signature, Secure Hash Function
Availability	DoS (denial of service), Wormhole, Sinkhole, Hello Flood	Intrusion Detection, Pairwise Authentication
Access Control, Authorization	Unauthorized and Unauthenticated Access	Access Control, Key Distribution, Encryption
Authentication	Message Modification, Sybil, Replay and Spoofing Attack	Random Key Distribution, Digital Signature
Freshness	Replay and Spoofing attack	Time-stamp, One Way Secure Hash Function
Secure Localization	Node Capture and Note Replication Attack	Temper-proof and Temper-evident
Forward and Backward Secrecy	Message Disclosure	Key Distribution

Table 1 lists the security attacks and threats, which can violate the security properties, and the possible solutions to defend against them. Security mechanisms are essential to provide the required security properties in WSNs. An access control mechanism is one of them. Different users may have different privileges to access data based on their roles. An access control mechanism is one of the security mechanisms to prevent unauthorized usage in WSNs. Faye *et al.* [3] described how access control must be able to authorize and grant access privileges of users for data access in the sensor network and prevent

unauthorized access from the malicious users. This paper only focuses on the access control models in WSNs, and the next sub-section will present the traditional access control models for information system.

2.2. Traditional Access Control Models

There are two original access control models in information systems, which are mandatory access control (MAC) [18] and discretionary access control (DAC) [19]. MAC manages access control levels by means of an administrator in the organization. It uses a hierarchical approach to control access to the objects, which represent system resources here. The administrator defines an access control policy that cannot be modified by the subjects. MAC is mostly used in the systems where priority is placed on confidentiality, such as in military applications. In a DAC model, the owner of an object controls access to that object. This means that he has power to create the permissions for data access. By default, subjects without this permission cannot access the objects. Subjects mean users here.

The concept of an access control matrix, which defines the relationships between subjects, objects and the actions that the subjects want to perform on the objects, was introduced by Butler Lampson [20]. The subjects' identities are placed in rows and the objects' identities in columns. Each action that a subject wants to perform on an object is placed in the intersection of the corresponding row and column. The size of the access control matrix is directly proportional to the number of subjects and to the number of objects. Samarati and Vimercati [21] suggested that there are three possible approaches to implement the access control matrix in electronic systems, named authorization table, access control list (ACL) and capabilities. Among these, ACL and capabilities are commonly used in access control schemes. The three ways of representing the access control matrix are explained as follows:

- **Authorization Table**

  A three-dimensional table, corresponding to subjects, actions and objects, respectively. Each entry in the table corresponds to an authorization.

- **Access Control List (ACL)**

  Each ACL contains the list of subjects and their access permissions to a given object. When a subject tries to access an object, the ACL for that object is used to verify the request from the subject. If the subject access pair is in the ACL list, access will be granted. Otherwise, access will be denied. In the ACL approach, the lists of subject and action pair are stored for each object. An ACL is represented by a column in the matrix table as seen in Figure 1. In this figure, r, w and x stands for read, write and executable.

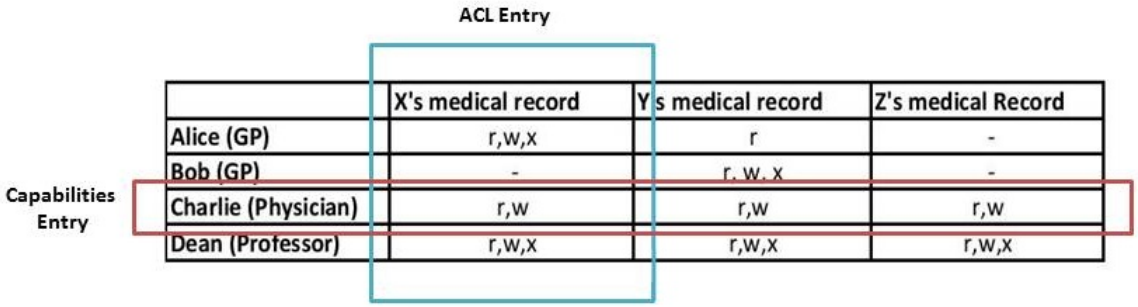
- **Capabilities**

  Capabilities are different from ACLs. Pairs of action and object are stored for each subject in the access control matrix. In a capability approach, the subject can get access to the object, when he presents the correct capability to the system. A subject's capabilities are represented by a row in the access control matrix.

The difference between ACLs and capabilities can be seen in Figure 1. One of the drawbacks of using an access control matrix is that when there are a large number of subjects and objects in the system, the

administration of those subjects and objects becomes very difficult to handle. The role-based access control (RBAC) model [22] has been developed to model access control permissions in an organization in a more manageable way than the access control matrix does. The detailed description of RBAC and other different types of access control models in WSNs based on their architectural model, strength and weakness will be explained in the next section.

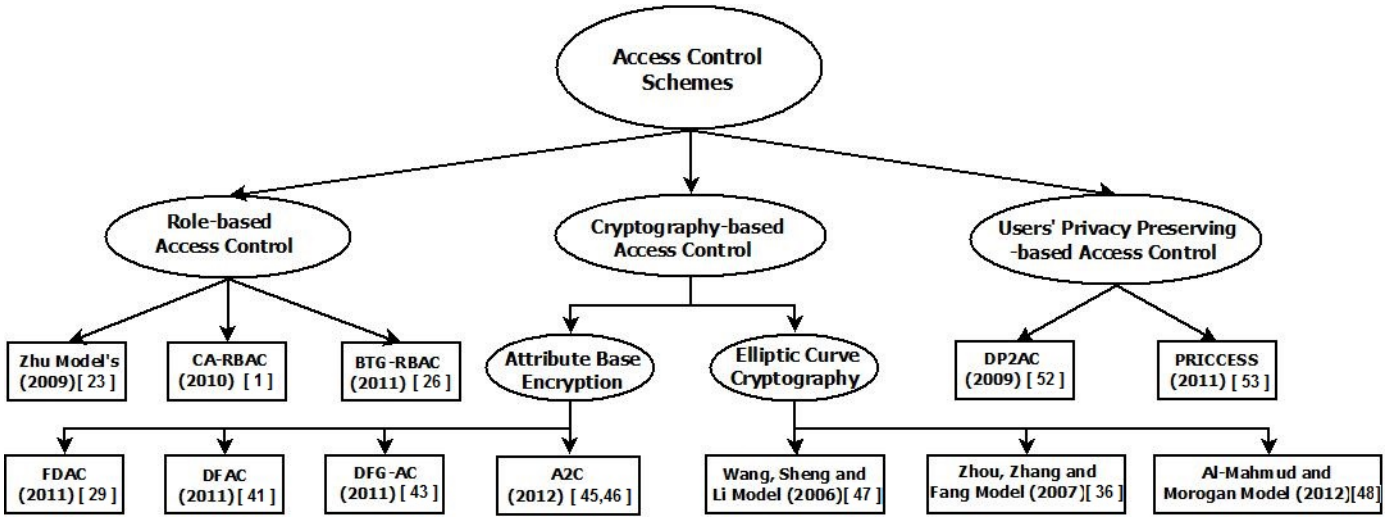
Figure 1. Difference between access control list (ACL) and capabilities.



3. Access Control Models in WSNs

A considerable number of access control models has been proposed for use in WSNs, though some of them are not yet implemented. In this section, we present the proposed access control models before we compare and contrast them in the next section. We group the proposed models into three main categories based on the nature of their architecture, namely: role-based access control (RBAC), cryptography-based access control (CBAC) and users' privacy preserving access control (UPPAC). A taxonomy of access control models for WSNs, including the publication year of each proposal, is shown in Figure 2.

Figure 2. A taxonomy of access control schemes in WSNs

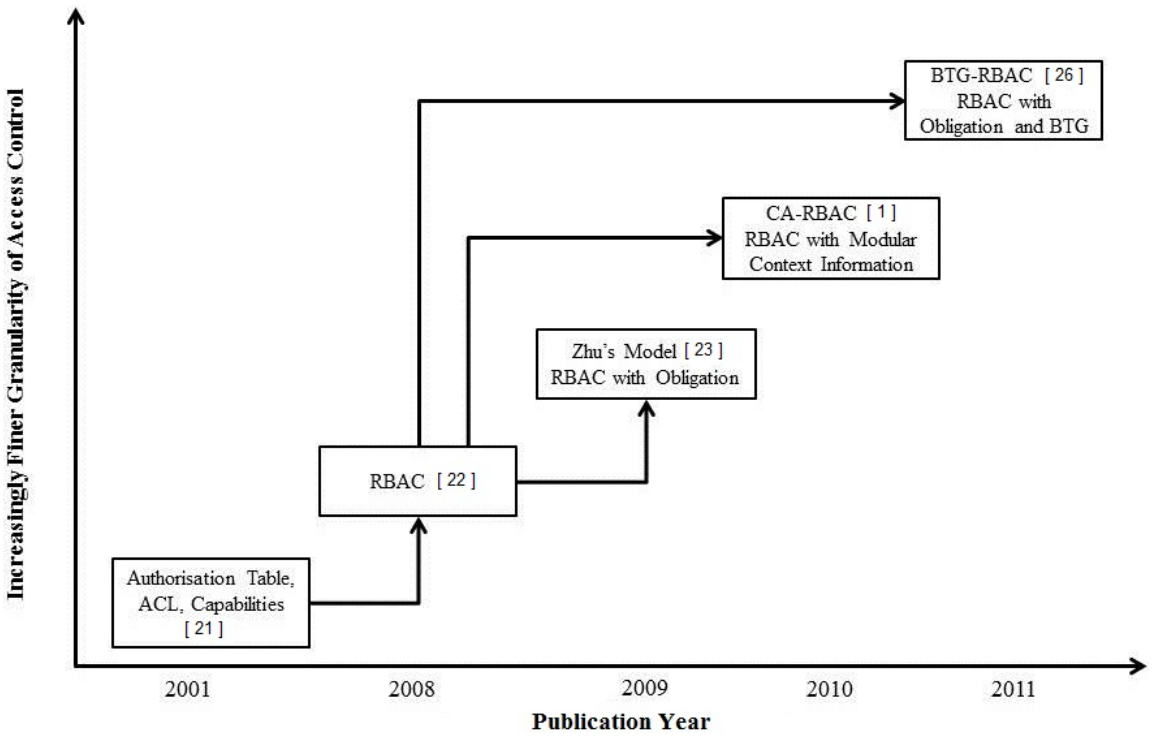


3.1. Role-Based Access Control (RBAC)

Most of the access control models in WSNs and WMSNs are based on traditional RBAC [22], which has been widely accepted as a policy-based access control model. Applications based on RBAC have been implemented and deployed in commercial companies and education industries. The principle of RBAC model is the role, defined as an intermediary concept relating a group of subjects to a set of access permissions. Any member from the subject group role has all of the permissions that are associated with that role. When a new subject is assigned to a group, he receives all of the associated access permissions, but these permissions are revoked when the subject leaves the group or is removed from the system. It is the same procedure to add and remove permissions from the roles. When a permission is added to a role, all of the members of the associated subject group will receive that permission. The permission will be revoked when it is deleted from the role. This feature helps to simplify system administration when there are many thousands of subjects and objects in an organization.

In RBAC, the access decision is a choice between two outcomes: permitted access or denied access. The following access control models are proposed based on the RBAC model with different extensions to provide further security properties in WSNs. Figure 3 shows how RBAC-based access control models have evolved in the WSN research community.

Figure 3. An evolution of role-based access control (RBAC)-based access control models in WSNs.



- **Zhu's Model** [2009]

  Zhu *et al.* [23] proposed a light-weight policy-based access control model, which used authorization and obligation policies to perform actions and make access decisions at the sensor

nodes in a WMSN. The main idea of the proposed approach is to support sensor-level access control policy. A light-weight policy system, which is known as Fingers [24], enables policy enforcement and interpretation on the distributed sensors to provide fine-grained access control. Each sensor manages its own policies to implement both the policy decision point (PDP) and policy enforcement point (PEP). A PDP interprets policies and makes a policy decision, while a PEP enforces the policy by permitting and denying a subject from performing the requested actions. A controller (perhaps a PDA) uses a Diffie–Hellman (DH) key agreement to share keys with the sensor nodes. The sensor nodes can communicate between each other in a WMSN by using secret keys from the controller. An authentication process is used to prevent malicious nodes and users from joining the network. Only the sensor nodes that have keys from the same controller can communicate with each other. If a user has access to the network controller, he can request it to perform some actions at the sensor nodes. As an application, this approach can be used in WMSN to prevent unauthorized access to actuators, such as insulin or other drug pumps, that may harm the patients.

- **Context-Aware Role-Based Access Control (CA-RBAC)** [2010]

  Garci-Morchon and Wehrle [1] proposed the context-aware role-based access control (CA-RBAC) model based on a modular context structure for WMSNs. The aim of the model is to provide context awareness and adapt its security properties to ensure the users' safety in WMSNs. Wehrle *et al.* [25] pointed out that the RBAC model is not good enough to use in a WSN, because in traditional RBAC models, the roles and policies have to be predefined in advance. In the proposed model, the decision-making process is divided into three modular context situations: critical, emergency and normal condition. Based on these situations, the access privileges to sensed data will be different. The access control decision will be made based on context information, such as time, location, *etc*., and the access control policies of three different modules. In a WMSN, the sensor nodes are attached to the human body to sense and check medical information for a healthcare service. In the normal case, an authorized doctor needs to verify his access control role in order to access the medical data of a patient, but a nurse may not have the same level of privilege. When the system declares a critical or emergency case based on the modular context information, the doctor or nurse can perform any action and can access data, even though they may not be able to access that data in a normal condition. One of the disadvantages of this model is that there is no prevention or detection mechanism, as well as no verification process to check a user's data access, when the critical situation occurs.

- **Break-the-Glass Role-Based Access Control (BTG-RBAC)** [2011]

  Ferreria *et al.* [26] proposed the break-the-glass role-based access control (BTG-RBAC) model based on the RBAC model. The main idea of this model is to gather necessary information from the end users with their collaboration for a usable access control policy that can perform the BTG action in emergency situations. The break-the-glass (BTG) rule allows the users' to have emergency and urgent access to the system when a normal authentication does not perform or work properly. They introduced BTG rules in order to override access policy whilst providing non-repudiation mechanisms for its usage. In a real environment, unanticipated situations may

occur because it is impossible to predict all of the access permissions in advance for all situations. The BTG extension is used for emergency and important cases whenever a user wants to access data urgently and immediately. When the user tries to perform BTG actions, the system will ask him if he really wants to perform that action on a specific object. If the user answers affirmatively, the system will activate the BTG operation and trigger the associated obligations, like alarms, log file, *etc.* The BTG-RBAC model made the system much more flexible than normal RBAC, but one of the disadvantages is that human processes are needed in order to enforce the BTG rules.

3.2. Cryptography-Based Access Control (CBAC)

Cryptography-based access control (CBAC) is another form of access control model for the information systems. Ghani *et al.* [27] mentioned that the CBAC mechanism is designed for untrusted environments, where a lack of global knowledge and control are defining characteristics. It absolutely relies on cryptography to control data access and to ensure data confidentiality and integrity. The main idea is to use a unique key for each data resource. Users who are allowed to access that data resource are assigned the key for data access [28]. Cryptography methods in WSNs should meet the constraints of sensor nodes, such as limited power, resources and memory shortage. Therefore, choosing a suitable cryptography method is important in WSNs. There are two types of cryptographic method; asymmetric encryption, known as public key cryptography (PKC), and symmetric encryption, known as symmetric key cryptography (SKC). The PKC-based scheme provides better data access security than SKC in the open multi-user environment [29]. The nature of PKC is using two keys: one for encryption and one for decryption. In PKC, the data encryption is usually targeted to only one recipient or one group. This means that any message encrypted by using a public key can be decrypted only with the corresponding private key.

Many researchers considered that PKC schemes, such as Rivest–Shamir–Adleman (RSA) [30] and the DH key agreement scheme [31], were unsuitable for applications in WSNs, because of the big size of the code, message and data, the long processing time and the high power consumption. Sen [5] suggested that public key algorithms are computationally intensive and usually execute lots of multiplication instructions to perform a single-security operation. Therefore, one-to-one encryption is not efficient to be used in WSNs, because the overhead of encryption and the amount of cipher text are directly proportional to the total number of authorized users. Broadcast encryption [32] is an alternative solution to provide a one-to-many encryption method, but it requires the users to present their keys and other information individually. However, recent studies [33–35] argued that it is feasible to employ PKC in WSNs by using the right selection of algorithms and associated optimization, parameters and low power methods.

Many researchers in WSNs are interested in SKC schemes because of the lower computation overhead of SKC. SKC uses the same key for both encryption and decryption between two communicating hosts, who share the secret key. SKC seems to be suitable for low-end devices, like sensor nodes, because of their low overhead [36]. One major issue of using SKC methods is how to securely distribute the key between communication nodes. It is a major problem of using SKC, because key pre-distribution is not

always feasible and reliable in WSNs. Even many symmetric ciphers are still too expensive to implement on sensor nodes.

Key management in WSNs has received lots of attention from researchers. Key management is an essential mechanism to ensure security in network services and applications, when cryptographic schemes are applied in the sensor networks. The main idea is to establish keys between nodes, trusted authorities and users in a secure and reliable manner. There are three different tasks in key management, namely key establishment, key revocation and key update. Key management is a big challenge in WSNs, because the sensor nodes can be deployed in any location and they know nothing about their neighbour nodes before deployment.

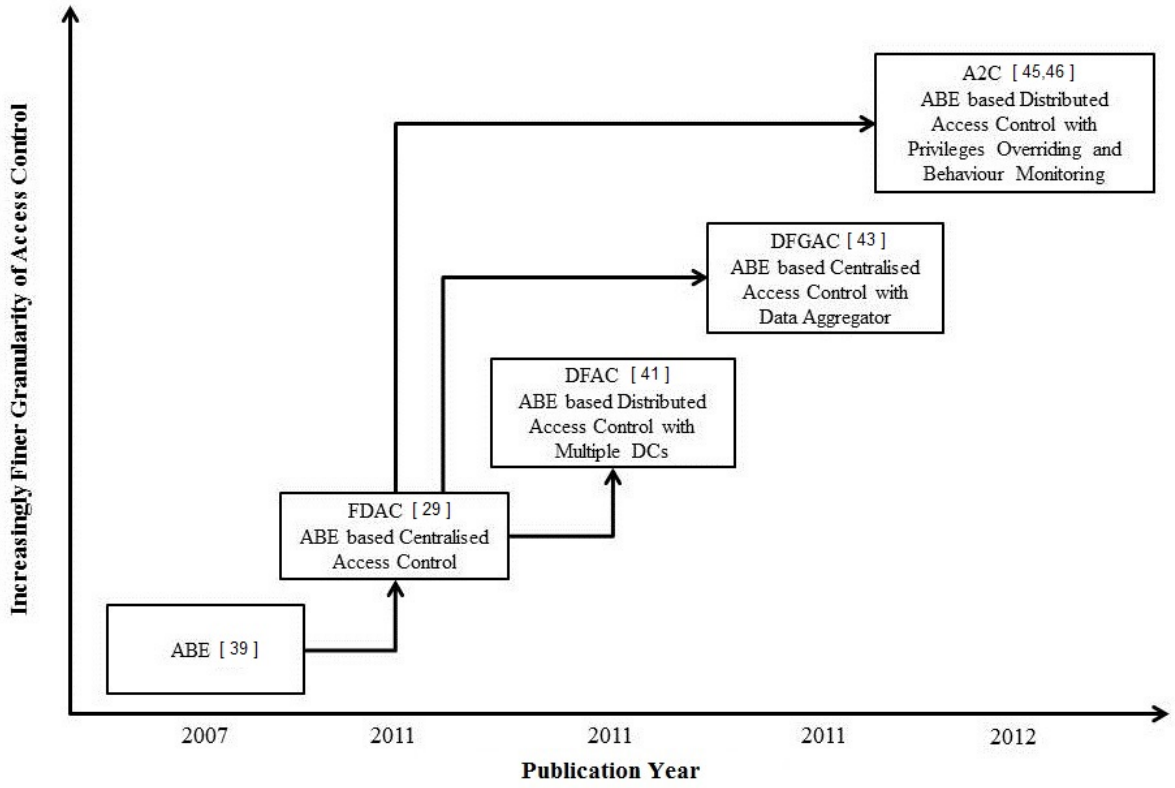
Choosing a suitable cryptography method is important in WSNs. In this section, we will explain two different types of CBAC models, namely elliptic curve cryptography (ECC)-based access control and attribute-based encryption (ABE)-based fine-grained access control.

3.2.1. Attribute-Based Encryption (ABE)-Based Fine-Grained Access Control

Sahai and Waters [37] proposed the ABE scheme to model and design a scalable and flexible access control system. ABE is a public key cryptography primitive generalising identity-based encryption (IBE) [38], which is associated with user's identity in a single user message. In ABE, a group of users is described by the combination of several descriptive attributes and access structures, which is also called an attribute policy. In ABE, the public key encryption is based on one-to-many encryption. There are two different types of ABE, which are proposed by Sahai and Waters [37], namely key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, data that is sensed and stored in the sensor node is encrypted with a set of attributes; the user's private key is associated with an access structure that specifies which types of ciphertexts the key can decrypt. Only the users that have the right access structure and the key can access and decrypt the sensed data. In CP-ABE, the ciphertext is associated with the access structure. The user's private key is associated with the attributes that specify which type of the ciphertext the key can decrypt. Some ABE-based fine-grained access control models use ECC for key management and distribution.

The ABE [39] method is commonly used in the access control models for data encryption and storage in WSNs. Li *et al.* [40] suggested that ABE is a highly promising public key encryption approach to realize scalability and fine-grained access control, where the flexible access permissions and rights are assigned to each individual user. Fine-grained access control facilitates granting different kinds of access permissions to a number of users. The sensors may sense or collect various types of information, like medical and battlefield information, which may belong to different security levels. Fine-grained access control is a security requirement to protect sensitive information from unauthorized access. One alternative way of providing fine-grained access control in WSNs is using an ABE scheme. The step-by-step development of ABE-based access control models in the WSN research community is shown in Figure 4. Based on this Figure, the four access control models, which use ABE-based encryption to provide fine-grained access control, are discussed next.

Figure 4. An evolution of attribute-based encryption (ABE)-based access control models in WSNs.



- **Fine-Grained Distributed Data Access Control (FDAC)** (2011)

  Yu *et al.* [29] proposed the fine-grained distributed data access control (FDAC) model based on ABE. The main idea of their approach is to provide a distributed data access control, which is able to support fine-grained access control over sensor data and is resilient against attacks, such as user collusion (unauthorized users may collude to compromise the encrypted data) and node compromise (the sensor node could be compromised by a malicious user, due to lack of compromise-resistant hardware.). A network controller, which stores access structures, acts like a central distribution centre and distributes keys to users in FDAC. Only users with the right access structure and the right key can access data at the sensor nodes. The access structures will be different for each user depending on the access privileges of users.

  For example, in a battlefield application, the sensor nodes may be responsible for collecting different types of data, such as vibration, smoke, *etc.*, in different locations (village, forest). Therefore, the attributes, such as {location = village, data type = (vibration, smoke), owner = (explosion experts, officers)}, are used to specify the data access privileges of users. Based on the above example, the access structure of a user is designated as "(location is village) AND (type is vibration)", which allows the user to obtain the vibration data within the village area. More sophisticated access structures can be defined based on the application requirements. If the network controller is compromised by a malicious user, there will be no security provisioning in the system anymore. User revocation (user revocation may be one of the following: the service subscription is expired, the user changes group intentionally or the user or group key

is compromised) can be done by updating the master secret key that is embedded in the user secret key via broadcasting. In this approach, CP-ABE-based selective broadcast is used for user revocation, but there are no details on how to use it.

- **Distributed Fine-Grained Access Control (DFAC)** (2011)

  Ruj *et al.* [41] proposed a fully distributed fine-grained access control (DFAC) scheme using multi-authority ABE [42] to prevent a single point of failure. Instead of using one authority, like FDAC, several distribution centres (DCs) are used to store and distribute different access structures, sets of attributes and cryptographic keys to users and sensor nodes. All DCs are disjoint from each other. Each DC has its own access subtree (a subtree contains attributes at the leaf nodes of that subtree.) for each sensor node. Users, who want to access data at the sensor node, need to activate their ID with each DC to obtain access structures, access subtrees and keys. All of the subtrees from each DC are ANDed together to build a complete access structure for a single user, but the user has to store all of the access structures in order to access different types of data from the sensor network. This model facilitates modification and secret key distribution when the access rights of a user are changed, but the communication overhead of the user's revocation process is higher than with FDAC.

- **Distributed Fine-Grained Data Access Control for Distributed Sensor Networks (DFG-AC)** (2011)

  Hur [43] proposed an access control model called distributed fine-grained data access control (DFG-AC). It uses both a network controller and a data aggregator for central key management and central storage. The collected data from sensor nodes are transferred to the data aggregator by using a distributed sensor data collection protocol, such as the Two-Tier Data Dissemination protocol (TTDD) [44]. The main idea of using the data aggregator as central storage is to perform more data encryption. Additionally, the users can get all of the information by accessing the data aggregator. The data aggregator is more powerful than the sensor nodes, and it can use complex encryption methods. The advantage of the proposed model is that it considers the stateless receiver problem. (Practically, users may miss a key update message. Therefore, they cannot keep their key states up-to-date. This problem is known as the stateless receiver problem.) To solve this problem, key revocation is done with a stateless group key distribution mechanism using a binary tree. One of the disadvantages is that the transmitting data from sensor nodes to the data aggregator consumes lots of battery power and energy. In addition, there might be a single point of failure because of the centralised data storage. This model provides user revocation by using the KP-ABE scheme with the attributes for distributed WSNs.

- **Adaptive Access Control** (A2C) (2012)

  Htoo *et al.* [45,46] proposed an adaptive access control (A2C) model with privilege overriding and behaviour monitoring to provide fine-grained access control for medical data in WSNs. A2C incorporates the concept of possibility-with-override and a user behaviour trust model into WSNs for hard-to-define and unanticipated situations. This model has a similar structure to BTG-RBAC, but the main difference is that no human effort is needed to override rules and policies, because

of the introduction of the overriding access privileges, the users' behaviour trust model and the prevention and detection mechanism. In this model, the users may be able to override a denial of access, when unexpected events occur. In addition, the users' behaviour trust model is used to check user's action, location, time, *etc*. The advantage of this model is that all of the user behaviour information is kept by the prevention and detection mechanism as an audit record to detect and prevent abnormal and unauthorised access, whenever the users try to access data from WSNs. ABE-based encryption and TTDD are used for data storage and data transmission. The main contribution of the proposed model is to adapt to unexpected situations by using privilege overriding and also to adjust its decision based on users' behaviour trust values.

3.2.2. Elliptic Curve Cryptography-Based Access Control (EC-CBAC)

Elliptic curve cryptography-based access control (EC-CBAC) models [36,47,48] use ECC to authorize and grant users access to data. They prevent the malicious nodes from joining the sensor network. ECC has become popular as the solution for WSN due to low computational overhead and small key size. Unlike for the RBAC and ABE-based access control models, there is no table for the evolution of ECC-based models in this section. The similarity of the proposed models is simply that they used ECC-based encryption.

- **Wang, Sheng and Li Model** (2006)

  Wang *et al.* [47] proposed an access control model based on ECC. The main objective of the proposed model is to use an ECC scheme for granting user access rights to the collected data. Different users may have different levels of data access due to restriction of access implicated by the data confidentiality and privacy. ECC is used in key distribution and sharing information between the users and a key distribution centre (KDC). In this approach, KDC is responsible for generating all security primitives, such as random numbers, access lists and hash functions, and maintains a user list with associated user identifications. The users have to request access permission from KDC. Access lists, which comprise user identity, group identity and user privilege mask, define the user's access privileges. User access privilege mask is a number of binary bits, and each bit represents a specific information or service. Therefore, users who possess the same mask and access privileges are put in the same group.

- **Zhou, Zhang and Fang Model** (2007)

  Zhou *et al.* [36] proposed an access control protocol based on ECC for node authentication and key establishment. The main idea of their approach is to accomplish node authentication and key establishment for new nodes, whenever they join the sensor network. The proposed access control model uses node identity and node bootstrapping time for the node authentication procedure. They introduced the node bootstrapping time into authentication procedures to differentiate malicious nodes from legitimate new nodes. In this model, the authors are mostly looking at the node deployment to prevent malicious nodes from joining the network. A certification authority (CA) is used to generate a certificate, which includes ID information and bootstrapping time, to authenticate the identity of a new node. Furthermore, the node certificate is signed with CA's

private key. Therefore, the adversaries cannot alter ID and bootstrapping time. When the new node is deployed in WSNs, it shows its certificate to the neighbour nodes in order to verify its identity with CA's public key. This access control protocol enforces control sensor node deployment and prevents malicious nodes from joining sensor networks.

- **Al-Mahmud and Morogan Model** (2012)

  Al-Mahmud and Morogan [48] proposed an identity-based authentication and access control model in WSNs. The main idea of the proposed model is to use an identity-based signature (IBS) [49] for providing both user authentication and data access control in WSNs. This protocol is based on the IBS scheme, where an ECC-based digital signature algorithm (DSA) [50] is used to sign and verify a message. A base station (BS) is responsible for generating the private keys of both users and sensor nodes in the network. For the key distribution, a one pass key establishment protocol [51] is used to share session keys between sensor nodes and users. Users are required to register with BS. Based on the access request from the users, BS generates private key and access structure for each user. The sensor nodes are preloaded with hash value of user identities and the private key, which will be used for the authentication process. After the authentication process, the sensor node will check whether the user is authorized to access the data.

3.3. Users' Privacy-Preserving Access Control (UPPAC)

Most of the access control models in WSNs are to provide data privacy and data confidentiality. The privacy of users and sensor nodes in WSNs is different from data privacy and has received less attention in the literature. In user privacy, users aim to hide their ID and other information. Therefore, no one in the network knows the real ID of a user, except the network authority and the user himself. Recently, there are two schemes proposed for the privacy-preservation of users' information in WSNs, namely distributed privacy-preserving access control (DP2AC) [52] and distributed privacy-preserving access control (PRICCESS) [53]. The PRICCESS model is related to the RBAC model. The main reason why the PRICCESS model is presented under UPPAC is that it provides user privacy preserving distributed access control in WSNs.

- **Distributed Privacy-Preserving Access Control (DP2AC)** (2009)

  Zhang *et al.* [52] proposed distributed privacy-preserving access control (DP2AC). The owner of the sensor network generates the token by using a blind signature [54]. Users need to buy tokens from the network owner before entering the sensor network. The tokens can be verified by any sensor node in the network, but no one can tell the identity of the token holder, including the network owner. There is no relationship between user identities and tokens, so privacy preservation for users is achieved. Once the token is validated by a sensor node, it provides the user with a certain amount of requested data, which is equivalent to the denomination of the token. The main objective of the proposed DP2AC model is that the network owner can prevent unauthorised access to sensed data, while users can protect their data access privacy.

  However, a recent study [55] pointed out that DP2AC is not fine-grained access control, because each anonymous user has the same access privileges. Furthermore, the network user cannot sign

a query command, because of the blind signature. As a result, the adversary can easily intercept the tokens and impersonate authorized users to access data at the sensor nodes. A disadvantage of using tokens in a WSN is that the sensor nodes need more storage for the token detection mechanism. All of the used tokens have to be recorded and stored in the sensor nodes to prevent the tokens being reused by malicious and unauthorized users.

- **Distributed Privacy-Preserving Access Control (PRICCESS)** (2011)

  He *et al.* [53] proposed the PRICCESS protocol for WSNs. The main contribution to the research community of this protocol is that it provides user privacy-preserving distributed access control in a single-owner multi-user sensor network. A ring signature [56] is used to protect the anonymity of users by using a group ID and group signature. Each group of users has different access privileges, IDs and keys for signature. Users have to activate their information with a network controller to receive the group ID and keys for data access. Users with the same access privileges are likely to be put in the same group by the network controller. The PRICCESS model used an ACL matrix to store the access list of the group for data access control in the network controller. Any user from the group can use a group key when he signs the message for data access request. Therefore, the network controller verifies that the message has been signed by one of the group members without knowing who the actual signer is. One of the disadvantage of using ring signature is that the overhead of signature becomes large when there is a large number of user groups in the network.

We have categorized and briefly discussed the access control models for WSNs in this section; next we compare these access control models.

4. Comparison of Access Control Models in WSNs

This section compares current access control models as have been discussed above based on network model, key management, data encryption, policy specification, the decision-making process, user revocation and user privacy preservation. An outline of the comparison is presented in Table 2.

4.1. Network Model

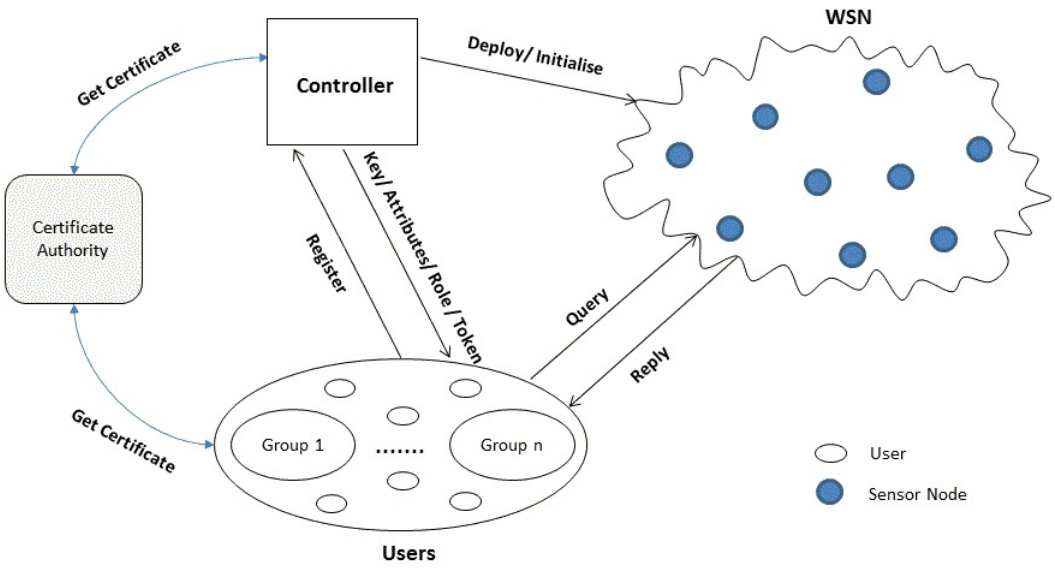
Access control models can be different based on their network architecture model when the cryptographic keys, roles, policies and attributes are distributed to users from the trusted authority or controller. Based on the above discussion about current access control models in WSNs, we separated them into two different network architecture models, namely the centralised network model and the distributed network model.

In a centralised network model, WSN is deployed and initialized with key, role, attributes, *etc*., by the controller. Whenever the users want to access data from the network, they have to register with the controller to obtain the keys, access structure, token, role, *etc*. Some schemes involve cooperation with a certificate authority (CA) before the users register with the controller. The users can send a query message with keys, access structure, token, *etc*., which have to be matched the keys, attributes, role, *etc*., from the sensor nodes. If the users have the right access privilege, the sensor nodes will allow the users to access data based on their access privileges.

Table 2. Comparison of access control models in WSNs.

Access Control Model	Network Architecture and Component	Key Management	Encryption and Decryption	Policy Specification and Decision-Making Process	User Revocation	User Privacy Preservation
Zhu's Model [23]	Authentication Manager (AM)	DH	-	Role, Purpose, Operation	-	-
CA-RBAC [1]	System Administrator (SA)	-	-	Role, Context Information	-	-
BTG-RBAC [26]	System Administrator (SA)	-	-	Role, Purpose, Operation, Obligation	-	-
FDAC [29]	Network Controller (NC)	DB-DH	ABE	Attributes-Based Key	CP-ABE	-
DFAC [41]	Distribution Centre (DC)	B-DH	ABE	Attributes-Based Key	ABE	-
DFG-AC [43]	System Controller (SC) and Data Aggregator	B-DH	ABE	Attributes-Based Key	Attribute Level User Revocation	-
A2C [45]	System Administrator (SA)	-	ABE	Attributes-Based Key, Context Information, Behaviour Trust Value	-	-
Wang, Sheng and Li Model [47]	Key Distribution Centre (KDC)	EC-DH	ECC	Key	-	-
Zhou, Zhang and Fang Model [36]	Certificate Authority (CA)	DH	ECC	Key	-	-
Al-Mahmud and Morogan Model [48]	Base Station (BS)	One-Pass Key Establishment Protocol	ECC-Based IBE	Key (Built on ID)	-	-
DP2AC [52]	Network Owner	RSA-DH	RSA	Role, Token	-	Blind Signature
PRICCESS [53]	Certificate Authority (CA)	DH	ECC	Role, Group Key	-	Ring Signature

Figure 5. Centralized network model.

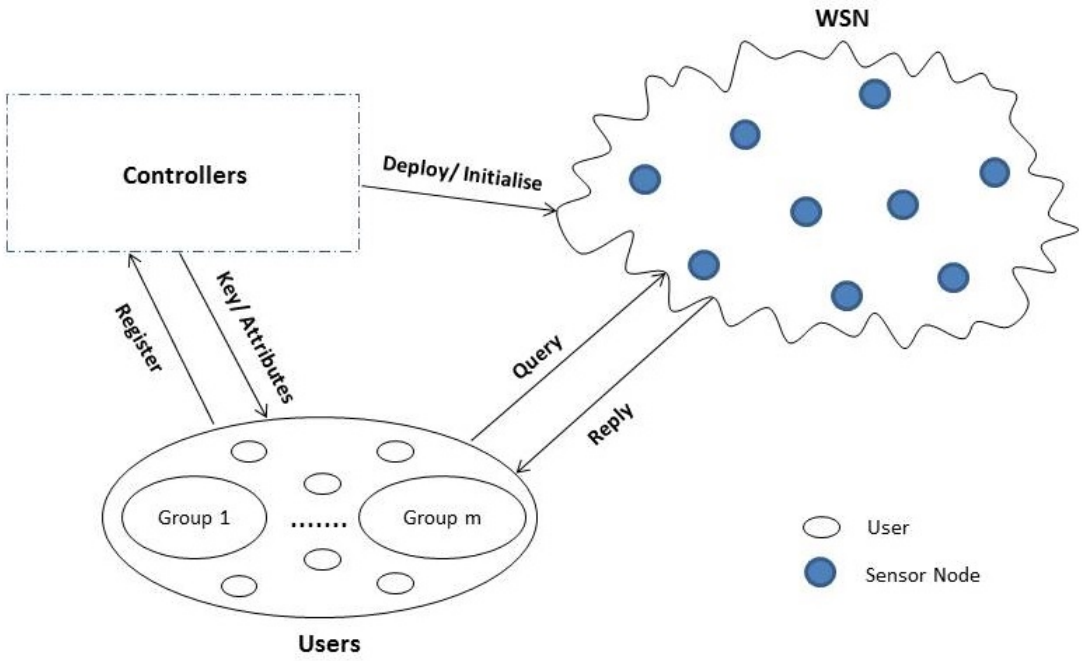


An overview diagram of the centralised network model is shown in Figure 5. The current access control models, such as Zhu's model [23], CA-RBAC [1], BTG-RBAC [26], the FDAC model [29], DFG-AC [43], Wang, Sheng and Li's model [47], Zhou, Zhang and Fang's model [36], Al-Mahmud and Morogan's model [48], DP2AC [52] and PRICCESS [53], used the centralised network model. The controller shown in Figure 5 might be identified as the authentication manager (AM) [23], system administrator (SA) [1,26], network controller (NC) [29], system controller (SC) [43], key distribution center (KDC) [47], base station (BS) [48], certificate authority (CA) [36,53] or network owner [52]. Users have to register with the controller to obtain the access privileges for data access. The disadvantage of the centralised network management model is that a single point of failure can occur at anytime, because the controller manages all of the key generation, distribution, *etc*. If the controller is compromised, there is no security provision in the network.

In the distributed network model, multiple controllers manage the WSN instead of it being handled by just one controller, as in the centralized network model. A user has to register with several distribution centres (DCs) to obtain the data access according to his/her access privileges. In the distributed approach, the controllers are not cooperating with each other. The public key of the network is derived from the attributes. A sensor node is preloaded with some attributes from each DC and the public key parameter set based on the possession of attributes. Each user needs to present his/her identity to each DC to get a set of attributes and a set of access structures. An access structure consists of subtrees, which contain attributes at the leaf nodes. Even at the leaf nodes of subtrees, there are AND, OR and t-out-of-n threshold operations. Each DC gives only one access subtree to the user. All of the subtrees from each DC are ANDed together to build a complete access structure for a single user. The user who matches a set of attributes with a sensor is able to access data from that sensor. If one controller is compromised by an attacker, he can only get certain types of data, which are managed by that controller. The disadvantage of the distributed approach is that the sensor nodes need to interact with more than one controller and store

multiple keys when the network is initialised and deployed by the controllers. The overview diagram of the distributed network model can be seen in Figure 6.

Figure 6. Distributed network model.



Based on the above discussion, most of the access control models in WSNs use the centralised approach apart from DFAC [41] and A2C [45], which use the distributed approach. However, the network models are quite similar for all the access control models. In each model, different controllers are used for network management and for key distribution. All of the controllers have similar functionality, such as CA or trusted authority. Overall, AM, CA, SA, NC, DC, KDC and the network owner, which have much the same functionality, are used in the current models to handle network management and key distribution.

4.2. Key Management

The Diffie–Hellman (DH) key exchange protocol and ECC are widely used for key distribution and key management in access control models in WSNs. Simple DH key exchange is used in Zhu's scheme [23] to provide sensor level access control and to protect from malicious nodes joining the network. DH key exchange protocol is simple and fully distributed, and ECC has smaller-sized cryptographic keys than other public key schemes. Therefore, the combination of DH and ECC is suitable to use in resource and memory limited small devices, like sensor nodes. The ECC-based DH key management scheme is used in Zhou, Zhang and Fang's model [36], PRICCESS [53] and Wang, Sheng and Li's model [47]. ECC-based decisional bilinear Diffie–Hellman (DB-DH) is used in FDAC [29]. However, bilinear Diffie-Hellman (B-DH) is used in both DFG-AC [43] and DFAC [41]. RSA-based public and private keys are used for key management in DP2AC [52], but the key management scheme is based on the DH approach. In addition, the uTESLA[57] protocol is used by the network owner to

update keys of the sensor nodes. In Al-Mahmud and Morogan's model [48], a one-pass key establishment protocol is used for the key distribution and shared session keys between sensor nodes, users and the base station. There is no explanation about the key management scheme in BTG-RBAC [26] and CA-RBAC [1].

4.3. Data Encryption

A popular encryption method for data storage in WSNs is using ABE at the sensor nodes. ABE-based encryption is popular relative to other public key encryption methods because of its highly promising approach to realize scalability and fine-grained access control. The ABE method is used in the FDAC [29], DFAC [41], DFG-AC [43] and A2C [45] models for data encryption, as well as for data access control. Data in the sensor nodes are encrypted using attributes and keys from the trusted authorities. Data access is given only to users who have both keys and access structures to match the attributes and keys from the sensor nodes. Other public key encryption methods are based on ECC and RSA. ECC is a popular choice for data encryption, because of its characteristics, such as small sized key and low overhead. ECC-based encryption is used in Zhou, Zhang and Fang's model [36], PRICCESS [53] and Wang, Sheng and Li's model [47]. Simple data encryption based on RSA is used in DP2AC [52] for data encryption.

4.4. Policy Specification and Decision-Making Process

Policy specification and decision-making processes depend on the network architecture and policy; and the role specifications in the access control model. The decision-making process is based on predefined roles and policies in RBAC-based models, such as Zhu's model [23], CA-RBAC [1] and BTG-RBAC [26], but in CB-RBAC, contextual information and roles are considered. BTG-RBAC used authorization and obligation roles to make access decisions based on users' requests in an emergency. The main disadvantage of using the RBAC model is that the data access roles and policies need to be defined in advance. Sometimes, it is hard to predict and predefine all the possibility of roles and policies for policy specification and the decision-making process.

In ABE-based access control models, such as FDAC [29], DFAC [41], DFG-AC [43] and A2C [45], attributes, such as location, role, *etc.*, are used to define policies and make access decisions on users' requests. The access policies are different based on the attributes and the unique key from each user. In the A2C model, not only an attributes-based key is used, but also contextual information and a behaviour trust value are used to make a flexible access decision in any situation. Therefore, to override a denial access policy in the A2C model, the key, behaviour trust value and contextual information are considered in order to make an effective access decision. In Wang, Sheng and Li's model [47], the private key and access list of the user are used to make an access decision at the sensor nodes, but for Zhou, Zhang and Fang's model [36], the private key and certificate are used for node deployment. In Al-Mahmud and Morogan's model [48], hash values of the user identity and the private key of the user are used to specify policy. DP2AC [52] used a blind signature to generate a token, which contains access privileges for the data. For PRICCESS [53], the ACL matrix is used to store roles

and policies. These policies and roles are stored based on a group of users and their access privileges. Therefore, each group of users has different access privileges based on their group's policy.

4.5. User Revocation

User revocation means that the users' service subscription is expired, the key of the user is compromised or the user changes to a different group intentionally. It has received less attention in WSNs. Only FDAC [29], DFAC [41] and DFG-AC [43] discussed user revocation in WSNs. In FDAC and DFAC, the life time of a sensor node is divided into many phases. In each phase, the master key of the network is updated by using a CP-ABE-based broadcast encryption scheme to prevent unauthorized access from the old users who leave the sensor network. Only users who still have access to the sensed data will receive the key update messages from the trusted authority. In DFG-AC [43], the system controller notifies and sends the updated membership list to a data aggregator, as well as to the network users that are listed on the membership list. When the data aggregator receives the notification message, it changes the attribute group key and re-encrypts the stored data with that key. Therefore, only the network users, who receive the update message, are able to access data from the sensor nodes.

4.6. Users' Privacy Preservation

DP2AC [52] and PRICCESS [53] provide privacy preservation for users who access data from the network. In DP2AC, the network owner generates the token by using a blind signature. No one will know the true identity of that user, including the network owner himself, because user information is not needed to generate the tokens. The ring signature is used in the PRICCESS protocol to provide the privacy of user information in WSNs. Anyone in a group can access data by using the group ring key instead of using his own identity and key. An alternative way to provide privacy preserving in WSNs is to use pseudo-random functions (PRF) [58]. In that approach, the user ID is computed with a PRF function to generate a random number. Therefore, no one in the network will know who the actual signer of the access request is.

Table 2 shows the comparison of access control models in WSNs based on the above discussion. The next section evaluates current access control models based on features and performance.

5. Evaluation of Access Control Model in WSNs

In this section, the criteria used for the comparison and evaluation of access control models are studied and a novel set of evaluation criteria is proposed. The current access control models in WSNs will be evaluated based on two aspects: features and performance evaluation.

5.1. Evaluation Based on Features

To make meaningful comparisons of the current access control models in WSNs, the evaluation framework is defined to compare and contrast current access control models by using the following features [27,59,60].

1. *Support Data Privacy*

   The need for data privacy is growing among all of the real-world applications in WSNs. Data privacy becomes more and more important in WSNs, when data are to be released to only authorized and legitimate users. The more data being disclosed, the more the owner of that data loses his own privacy.

2. *Support User Privacy*

   The need for user privacy is important in some applications. Sometimes, a user, who tries to access data from the network, does not want to share his detailed information with other users in the network. This means that the users' privacy preservation is needed to protect the privacy of user information in the network.

3. *Flexibility*

   No matter how perfect an access control system is, if it does not support accommodation to changes, such as insertion and deletion of the application systems, the access control model is not feasible to use in real-world applications. In WSNs, the user characteristics and the access context are changing continuously. Therefore, the access control decisions must be synchronised with continuously changing security conditions. It is desirable for the access control model to handle the dynamism of users and environments. Therefore, the access control model needs to be flexible enough to support changes and synchronise with the access control decisions.

4. *Support for Emergency Data Access*

   An ideal access control model needs to support data access, not only in normal situations, but also in an emergency situation. Many applications will benefit from such a provision.

5. *Context Sensitivity*

   An access control model is context sensitive when context information plays a role in making the appropriate access decision. This means that the contextual information is used in defining policies for making an access control decision dynamically.

6. *Granularity*

   There are two different types of granularity in access control, which are fine-grained and coarse-grained. Fine-grained means that the access control models should allow different roles for specific data accesses and provide a fine-grained reference to the subjects and objects. Coarse-grained means that groups of users and collections of objects often share the same access control requirements. The access control system should then offer support for authorization specific to the groups of users, objects and possibly actions.

These six supporting features listed above are used to evaluate the current access control models in WSNs. Table 3 shows a comparison of current access control models based on these features and qualities. The first row of the table describes evaluation criteria, and the first column lists access control models. Each cell in the table shows whether the model of that row has the feature of that column.

All of the access control models in WSNs provide data confidentiality and data privacy in normal conditions, but the users' privacy preservation is only supported in DP2AC and PRICCESS. The access control models that used ABE and contextual information to make access decisions provide flexibility in the system. Based on Table 3, all of the access control models in WSNs support authorization decisions and allow for changes, like roles, users, policy, *etc*. Among them, CA-RBAC, BTG-RBAC and A2C support emergency and immediate data access, but data privacy has not been discussed, apart from the adaptive access control model. There are few access control models that make authorization decisions based on context information. Approximately equal numbers of access control models support coarse-grained and fine-grained. As a summary, the authorization policy for each scheme is different, which means that all models are proposed to solve different problems and look from different points of view to fill the gaps in WSNs area. In addition, there is no access control model that provides data privacy in emergency and unexpected conditions, apart from A2C model.

Table 3. Comparison of access control models based on features in WSNs.

Access Control Models	Support Data Privacy	Support User Privacy	Flexibility	Support For Emergency Access	Context Sensitivity	Granularity
Zhu's Model [23]	Yes	No	No	No	No	Coarse-Grained
CA-RBAC [1]	Yes	No	Yes	Yes	Yes	Fine-Grained
BTG-RBAC [26]	Yes	No	Yes	Yes	No	Coarse-Grained
FDAC [29]	Yes	No	Yes	No	Yes	Fine-Grained
DFAC [41]	Yes	No	Yes	No	Yes	Fine-Grained
DFG-AC [43]	Yes	No	No	No	Yes	Fine-Grained
A2C [45]	Yes	No	Yes	Yes	Yes	Fine-Grained
Wang, Sheng and Li Model [47]	Yes	No	No	No	No	Coarse-Grained
Zhou, Zhang and Fang Model [36]	Yes	No	No	No	No	Coarse-Grained
Al-Mahmud and Morogan Model [48]	Yes	No	No	No	No	Coarse-Grained
DP2AC [52]	Yes	Yes	No	No	No	Coarse-Grained
PRICCESS [53]	Yes	Yes	No	No	No	Coarse-Grained

5.2. Evaluation Based on Performance

The performance evaluation is discussed based on computation cost, communication cost, memory usage and processing or execution time. Before we discuss the performance evaluation, we describe the hardware specifications and products that are used to deploy the access control engines and models for WSNs. Figure 7 shows the comparison of hardware specifications that are used in the proposed access control models. Based on Figure 7, the various platforms of sensor nodes are used. The CPU speed and size of the memory are also varied based on the sensor node's platform. However, all of the sensor nodes are chosen to use IEEE 802.15.4 as the communication protocol. Some of the proposed access control models in WSNs are not developed in practice, yet, but some of them are implemented in experiments.

Figure 7. A comparison of hardware specification.

Hardware Specification		Zhu's Model [23]	CA-RBAC [1]	FDAC [29]	Wang, Sheng and Li's Model [47]	PRICCESS [53]
Platform		Body Sensor Node TI MSPY30F149	Body Sensor Node TI CC2430	Imote2 & Tmote Sky	TelosB (TPR 2420)	Imote2
CPU		16 MHz/ 16-bit RISC processor	12 MHz/ 16-bit RISC processor	13-416 MHz	8 MHz/16-bit RISC processor	13-416 MHz
ROM		60 KB	128 KB	32 MB	48 KB	32 MB
RAM	SRAM	2 KB	4 KB	256 KB	10 KB	256 KB
	SDRAM			32 MB		32 MB
Communication Protocol		IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.4 extra Radios through SDIO & UART	IEEE 802.15.4	IEEE 802.15.4 extra Radios through SDIO & UART

Differently, A2C [45] has been designed and implemented in the simulation environment of Ponder2 [61] for wireless body sensor networks in medical applications. The simulation results show that fine-grained data access control is provided in this model, but there is no performance evaluation based on memory, CPU speed, *etc.* Therefore, we cannot make a fully comparative performance evaluation, but the performance evaluation of the developed access control models will be discussed briefly. The comparison has been made based on the results obtained from the implementation and evaluation outcomes of the proposed WSN access control models. In Figure 8, there are many blanks cells in the table. This means that the performance measurement of each model is varied and measured differently based on the design and what kind of security services are provided. It would be very useful for future research if some kind of benchmark could be produced to compare the performance of different WSN access control models.

Without such a benchmark, the performance evaluation for each model is quite different and is measured differently. The computation overhead for each access control model is different based on how the access control model has been designed and what was the purpose of the proposed model. The processing time of access decisions and authentication processes are different based on what kinds of method and approach are used in the proposed models. For example, in Zhu's model, the processing of authorization and obligation decisions takes about 81 μs and 62 μs, respectively. The processing time

of access control decisions in CA-RBAC is 33 ms, which excludes delays due to the communication overhead, length of the message, message collisions and verification of digital certificates. In Wang, Sheng and Li's model, the total access decision time is 14.13 s, which is relatively long, when compared with CA-RBAC. It includes the users perceived delay from sending out the access request to the sensor node, as well as the amount of time for the sensor node to make an access decision and to approve the users. Ten-point-one seconds is required for the authentication processing time in Wang, Sheng and Li's model. This seems to indicate that the proposed WSN models are not measuring the same thing.

Figure 8. A comparison of access control models based on performance Evaluation.

Performance Criteria			Zhu's Model [23]		CA-RBAC [1]	FDAC [29]			Wang, Sheng & Li's Model [47]		PRICCESS [53]				
Computation Overhead (µs, ms, s)	Processing Time of Access Decision		Autho-risation	Obliga-tion	33 ms	-			14.13 s		-				
			81 µs	62 µs											
	Processing Time of Authentication		-		-	-			10.1 s		-				
	Processing Time of Encryption	52-bytes (Text)	9.5 s		-	-			-		-				
		64-bytes (Text)	-		-	0.4 ms			-		0.39 ms				
	Processing Time of Decryption (52-bytes)		5.2 s		-	-			-		-				
	Processing Time of One Scalar Multiplication		-		-	Processing Speed			-		-				
						104 MHz	208 MHz	416 MHz							
						139 ms	69 ms	35 ms							
Energy Consumption (µJ, mJ, J)			-		-	8.74 mJ	-	-	Comp-utation Cost	Commu-nication Cost	m = Number of Group Users				
											m= 10	m= 20	m= 30	m= 40	m= 50
									54.4 mJ	594.8 µJ	0.35J	0.66J	0.98J	1.29J	1.45J
Memory Usage (KB)	ROM		2.88 KB		2.87 KB	-			2.01 KB		-				
	RAM		31.77 KB						46.01 KB						

It is also important to measure the processing time of encryption and decryption under the computation overhead. The processing delay of both TinyECC [62] -based encryption and decryption for 52-bytes message is 9.5 s and 5.2 s in Zhu's model. If a symmetric Skipjack cryptography [63] is used instead of TinyECC, the processing delay will be decreased dramatically from 9.5 s to 150 μs for encryption and from 5.2 s to 90 μs for decryption. The processing time of encryption for 64-bytes text message in the PRICCESS model is 0.39 ms, but there is no information about the processing time of decryption in this model. In FDAC, the computation overhead of one scalar multiplication (the sensor nodes need to execute one scalar multiplication on elliptic curves, one-way hash and one symmetric key data encryption for 64-bytes text message) on Imote2 is 139 ms when working with 104 MHz. For 208 MHz and 416 MHz, it took 69 ms and 35 ms for one scalar multiplication. The computation overhead of one scalar multiplication will be much lower, if the RSA-based algorithm is used instead of

the ECC-based algorithm. The processing time of encryption is 0.4 ms for the RSA-based algorithm to encrypt 64 bytes of random text.

Some access control models are mostly concerned with the energy consumption in WSNs, because battery power is used. Therefore, it is important to measure the energy consumption based on computation and communication cost. In Wang, Sheng and Li's model, the power consumption for communication is calculated based on the maximum current draw. The total computation and communication cost for one access control decision in this model is 55.1 mJ, which is 54.4 mJ for computation cost and 594.8 μJ for communication cost. In FDAC, the energy consumption cost for one scalar multiplication process in 104 MHz is 8.74 mJ. In PRICCESS, the energy consumption cost will be different based on the number of users in a group. The node verification cost for 10, 20, 30, 40 and 50 members in the group is 0.35 J, 0.66 J, 0.98 J, 1.29 J and 1.45 J.

Based on the hardware specification of the sensor node in Figure 5, there is a limited memory storage for each sensor node, but it will be different on the platforms. Therefore, the usage of memory for each sensor node has to be measured correctly and carefully. Comparing Zhu's model with Wang, Sheng and Li's model, the memory usage for authentication executable occupies 31.77 Kb and 46.01 Kb of ROM, respectively, but for RAM, 2.88 Kb and 2.01 Kb are occupied. The total memory requirement for the CA-RBAC model is 2.87 Kb.

Based on the above discussion, the comparison of the proposed WSN access control models is hard to clarify, especially in performance measurement, because these models are proposed and designed based on different requirements and different security services to fill the gaps of active application areas in WSNs. It also shows and indicates that various access control models are measuring different things. Further studies are needed to clarify and evaluate the performance measurement of WSN access control models. This means that the authors, or other researchers in the WSN community, should study and measure the performance of all of the proposed WSN access control models in a similar way. The next section will explain some potential research issues for the access control models based on the above comparison and evaluation results.

6. Potential Research Issues

The development of access control in WSNs is challenging, because memory and other resources are limited, but access control is an essential security service, which is necessary to prevent unauthorized access by malicious users in a WSN. Especially in medical and military applications, data access controls for legitimate users are important to provide in any situation, because it is hard to assume and predefine all of the possibilities of what will happen in the future and what kind of unexpected situations will occur in the system. Based on the above literature review of the current access control models in WSNs and WMSNs, key open research issues are identified as follows:

- Various access control models have been proposed; however, no systematic comparisons have been conducted on these models. Further evaluation and comparison is desirable to learn the security services, performance, reliability and efficiency of these access control models.

- Most of the proposed access control models for WSNs are focused on node authentication and query authentication, but users' data access control has received little attention. The control of the user to the sensed data at the sensor nodes merits more investigation.
- Current access control models need to be made much more flexible to make access decisions on the unexpected events, because it is hard to predefine all of the possibilities in a WSN. A new access control model is needed to address higher reliability, scalability, availability and accountability to prevent unauthorized user access and allow authorized users data access in unexpected and unpredictable cases.
- The performance of WSN access control models should be studied and measured carefully in the future. It would be useful to produce an appropriate benchmark for the WSN research community.
- It is also likely that more powerful sensor nodes will need to be designed in order to support the increasing requirements for computation and communication in the sensor nodes. This means that a powerful encryption and decryption method should be able to apply in the future.

7. Conclusion

In this paper, we present the security vulnerabilities, security requirements and a literature review of current access control models, and also, we discuss the performance evaluation and comparison of the proposed models in WSNs. Although research efforts have been made on cryptography, key distribution and management and access control models in WSNs, there are still some challenges to be addressed, like the selection of appropriate cryptographic methods. Furthermore, the design of access control models in WSNs must satisfy constraints, such as energy, computation capacity and memory. Access control is a critical security service in sensor networks and is essential to ensure that network services are offered only to legitimate users in WSNs. The comparison of current access control models showed that there is still lots of work to be done on access control models in WSNs, especially for emergency and immediate data access.

Author Contributions

HM drafted the initial manuscript. HX, BC and JAM amended and refined the structure, content, and language of the manuscript. All authors read and approved the final manuscript.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments.

Conflict of Interest

The authors declare no conflict of interest.

References

1. Garcia-Morchon, O.; Wehrle, K. Modular context-aware access control for medical sensor networks. In Proceedings of the 15th ACM symposium on Access control models and technologies (SACMAT '10), Pittsburgh, PA, USA, 9–11 June 2010; pp. 129–138.
2. Ngo, D.N. Deployment of 802.15.4 Sensor Networks for C4ISR Operations. PhD Thesis, Navy Postgraduate School, Monterey, CA, USA, 2006.
3. Faye, Y.; Niang, I.; Noël, T. A survey of access control schemes in wireless sensor networks. *World Acad. Sci. Eng. Technol.* **2011**, *5*, 814–823.
4. Vella, M.N. *Survey of Wireless Sensor Network Security*; Report; Texas A and M University-Corpus Christi, Computer Science Program, Texas A and M University Press: College Station, TX, USA, 2008.
5. Sen, J. A survey on wireless sensor network security. *Int. J. Commun. Netw. Inf. Secur.* **2009**, *1*, 55–78.
6. Ng, H.S.; Sim, M.L.; Tan, C.M. Security issues of wireless sensor networks in healthcare applications. *BT Technol. J.* **2006**, *24*, 138–144.
7. Wang, W.; Bhargava, B. Visualization of wormholes in sensor networks. In Proceedings of the 3rd ACM Workshop on Wireless Security (WiSe '04), Philadelphia, PA, USA, 26 September 2004; pp. 51–60.
8. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The sybil attack in sensor networks: Analysis & defenses. In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 26–27 April 2004; pp. 259–268.
9. Li, Z.; Gong, G. *A Survey on Security in Wireless Sensor Networks*; Technical Report; University of Waterloo: London, UK, 2008.
10. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: attacks and countermeasures. In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, USA, 11 May 2003; pp. 113–127.
11. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. *Computer* **2002**, *35*, 54–62.
12. Perrig, A.; Stankovic, J.; Wanger, D. Security in wireless sensor networks. *Commun. ACM* **2004**, *47*, 53–57.
13. Gligor, V.D. Handling new adversaries in wireless ad-hoc networks (transcript of discussion). In *Security Protocols XVI*; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6615, pp. 120–125.
14. Wang, Y.; Attebury, G.; Ramamurthy, B. A survey of security issues in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2006**, *8*, 20–23.
15. Alemdar, H.; Ersoy, C. Wireless sensor networks for healthcare: A survey. *Comput. Netw.* **2010**, *54*, 2688–2710.
16. Pathan, A.S.K.; Lee, H.-W.; Hong, C.S. Security in wireless sensor networks: Issues and challenges. In Proceedings of the 8th International Conference on Advanced Communication Technology, Pyeongchang, Korea, 20–22 February 2006; Volume 2.
17. Raymond, D.R.; Midkiff, S.F. Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Comput.* **2008**, *7*, 74–81.

18. Ferraiolo, D.F.; Kuhn, D.R. Role-based access controls. In Proceedings of the 15th National Computer Security Conference, Baltimore, MD, USA, 13–16 October 1992.
19. Sandhu, R.; Munawer, Q. How to do discretionary access control using roles. In Proceedings of the 3rd ACM Workshop on Role-Based Access Control, Fairfax, VA, USA, 22–23 October 1998.
20. Lampson, B. Protection. In Proceedings of the 5th Princeton Conference on Information Sciences and Systems, Princeton, NJ, USA, January 1971.
21. Samarati, P.; Vimercati, S. Access control: Policies, models, and mechanisms. In *Foundation of Security Analysis and Design*; Springer: Berlin Heidelberg, Germany, 2001; Volume 2171, pp. 137–196.
22. Zhao, G.; Chadwick, D.W. On the modeling of bell-lapadula security policies using RBAC. In Proceedings of the 2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE '08), Washington, DC, USA, 23–25 June 2008; pp. 257–262.
23. Zhu, Y.; Keoh, S.L.; Sloman, M.; Lupu, E.C. A lightweight policy system for body sensor network. *IEEE Trans. Netw. Serv. Manag.* **2009**, *6*, 137–148.
24. Zhu, Y.; Keoh, S.L.; Sloman, M.; Lupu, E.; Zhang, Y.; Dulay, N.; Pryce, N. Finger: An efficient policy system for body sensor networks. In Proceedings of 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Atlanta, GA, USA, 29 September–2 October 2008; pp. 428–433.
25. Morchon, O.G.; Wehrle, K. Efficient and context-aware access control for pervasive medical sensor networks. In Proceedings of 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mannheim, Germany, 29 March–2 April 2010.
26. Ferreria, A.; Correia, R.; Monterio, H.; Brito, M.; Antunes, L. Usable access control policy and model for healthcare. In Proceedings of 2011 24th International Symposium on Computer-Based Medical Systems (CBMS), Bristol, UK, 27–30 June 2011; pp. 1–6.
27. Ghani, N.A.; Selamat, H.; Sidek, Z.M. Analysis of existing privacy-aware access control for e-commerce application. *Glob. J. Comput. Sci. Technol.* **2012**, *12*, 1–5.
28. Al-Hamdani, W.A. Cryptography based access control in healthcare web systems. In Proceedings of 2010 Information Security Curriculum Development Conference (InfoSecCD '10), Kennesaw, GA, USA, 1–3 October 2010; pp. 66–79.
29. Yu, S.; Ren, K.; Lou, K. Fdac: Toward fine-grained distributed data access control in wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **2011**, *22*, 673–686.
30. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1983**, *26*, 96–99.
31. Malan, D.J.; Welsh, M.; Smith, M.D. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In Proceedings of the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, CA, USA, 4–7 October 2004.
32. Boneh, D.; Gentry, C.; Waters, B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Proceedings of the 25th annual international conference on Advances in Cryptology (CRYPTO'05), Berlin/Heidelberg, Germany, 20–24 August 2005; pp. 258–275.

33. Gaubatz, G.; Kaps, J.-P.; Sunar, B. Public key cryptography in sensor networks—Revisited. In *Security in Ad-hoc and Sensor Networks*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 2–18.
34. Gura, N.; Patel, A.; Wander, A.; Eberle, H.; Shantz, S.C. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In *Cryptographic Hardware and Embedded Systems—CHES 2004*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 119–132.
35. Wander, A.S.; Gura, N.; Eberle, H.; Gupta, V.; Shantz, S.C. Energy analysis of public-key cryptography for wireless sensor networks. In Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications (PERCOM '05), Kauai Island, HI, USA, 8–12 March 2005; pp. 324–328.
36. Zhou, Y.; Zhang, Y.; Fang, Y. Access control in wireless sensor networks. *Ad Hoc Netw.* **2007**, *5*, 3–13.
37. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.
38. Gentry, C. *Handbook of information Security*; John Wiley and Sons: Bakersfield, CA, USA, 2006.
39. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy, Washington, DC, USA, 20–23 May 2007; pp. 321–334.
40. Li, J.; Zhao, G.; Chen, X.; Xie, D.; Rong, C.; Li, W.; Tang, L.; Tang, Y. Fine-grained data access control systems with user accountability in cloud computing. In Proceedings of IEEE 2nd International Conference on Cloud Computing Technology and Science, Indianapolis, IN, USA, 30 November 2010.
41. Ruj, S.; Nayak, A.; Stojmenovic, I. Distributed fine-grained access control in wireless sensor networks. In Proceedings of 2011 IEEE International Parallel and Distributed Processing Symposium (IPDPS), Anchorage, AK, USA, 16–20 May 2011; pp. 352–362.
42. Chase, M.; Chow, S.S.M. Improving privacy and security in multi-authority attribute-based encryption. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009.
43. Hur, J. Fine-grained data access control for distributed sensor networks. *Wirel. Netw.* **2011**, *17*, 1235–1249.
44. Ye, F.; Luo, H.; Cheng, J.; Lu, S.; Zhang, L. A two-tier data dissemination model for large-scale wireless sensor networks. In Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom'02), Atlanta, Georgia, USA, 23–28 September 2002; pp. 148–159.
45. Maw, H.; Xiao, H.; Christianson, B. An adaptive access control model for medical data in wireless sensor networks. In Proceedings of 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom) (IEEE Healthcom 2013), Lisbon, Portugal, 9–12 October 2013.

46. Maw, H.A.; Xiao, H.; Christianson, B. An adaptive access control model with privileges overriding and behaviour monitoring in wireless sensor networks. In Proceedings of the 8th ACM International Symposium on QoS and Security for Wireless and Mobile Networks 2012 (ACM Q2SWinet 2012), Paphos, Cyprus, 24–25 October 2012.
47. Wang, H.; Sheng, B.; Li, Q. Elliptic curve cryptography based access control in sensor networks. *Int. J. Secur. Netw.* **2006**, *1*, 127–137.
48. Al-mahmud, A.; Morogan, M.C. Identity-based authentication and access control in wireless sensor networks. *Int. J. Comput. Appl.* **2012**, *41*, 18–24.
49. Shamir, A. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1985; Volume 196, pp. 47–53.
50. Johnson, D.; Menezes, A.; Vanstone, S. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63.
51. Wang, Y.; Wong, D.S.; Huang, L. A one-pass key establishment protocol for anonymous wireless roaming with PFS. In Proceedings of 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011; pp. 1–5.
52. Zhang, R.; Zhang, Y.; Ren, K. DP2AC: Distributed privacy-preserving access control in sensor networks. In Proceedings of the 28th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2009), Rio de Janeiro, Brazil, 19–25 April 2009; pp. 1251–1259.
53. He, D.; Bu, J.; Zhu, S.; Chan, S. Chen, C. Distributed access control with privacy support in wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 3472–3481.
54. Radu, C.; Govaerts, R.; Vandewalle, J. A restrictive blind signature scheme with applications to electronic cash. In Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security II, Essen, Germany, 23–24 September 1996; pp. 196–207.
55. Li, M.; Lou, W.; Ren, K. Data security and privacy in wireless body area networks. *Wirel. Commun.* **2010**, *17*, 51–58.
56. Bender, A.; Katz, J.; Morselli, R. Ring signatures: Stronger definitions, and constructions without random oracles. *J. Cryptol.* **2008**, *22*, 114–138.
57. Perrig, A.; Szewczyk, R.; Wen, V.; Culler, D.; Tygar, J.D. Spins: Security protocols for sensor networks. *Wirel. Netw.* **2001**, *8*, 189–199.
58. Boneh, D.; Waters, B. *Constrained Pseudorandom Functions and Their Applications*. Cryptology ePrint Archive; Report 2013/352; Springer: Berlin/Heidelberg, Germany, 2013.
59. Mohammad, A.; Khdour, T.; Kanaan, G.; Kanaan, R. Ahmad, S.B. Analysis of existing access control models from web services applications' perspective. *J. Comput.* **2011**, *3*, 10–16.
60. Sahafizadeh, E.; Parsa, S. Survey on access control models. In Proceedings of 2nd International Conference on Future Computer and Communication, Wuhan, China, 21–24 May 2010.
61. Twidle, K.; Dulay, N.; Lupu, E.; Sloman, M. Ponder2: A Policy System for Autonomous Pervasive Environments. Available online: http://http://pubs.doc.ic.ac.uk/ponder2-policy-pervasive/ponder2-policy-pervasive.pdf. (accessed on 9 May 2012).

62. Liu, A.; Ning, P. TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In Proceedings of 2008 International Conference on Information Processing in Sensor Networks, St. Louis, MO, USA, 22–24 April 2008; pp. 245–256.
63. Skipjack and KEA Algorithm Specifications. Available online: http://csrc.nist.gov/encryption/skipjack-kea.htm (accessed on 13 May 2013).

A.4 An Evaluation of Break-The-Glass Access Control Model for Medical Data in Wireless Sensor Networks

[Published in Healthcom'14: 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services]

An Evaluation of Break-The-Glass Access Control Model for Medical Data in Wireless Sensor Networks

Htoo Aung Maw, Hannan Xiao, Bruce Christianson and James A. Malcolm
School of Computer Science
University of Hertfordshire
Hatfield, United Kingdom
Email: (h.maw,h.xiao,b.christianson,j.a.malcolm)@herts.ac.uk

***Abstract*—Wireless Sensor Networks (WSNs) have recently attracted a lot of attention in the research community because it is easy to deploy them in the physical environment and collect and disseminate environmental data from them. The collected data from sensor nodes can vary based on what kind of application is used for WSNs. Data confidentiality and access control to that collected data are the most challenging issues in WSNs because the users are able to access data from the different location via ad-hoc manner. Access control is one of the critical requirements to prevent unauthorised access from users. The current access control models in information systems cannot be applied straightforwardly because of some limitations namely limited energy, resource and memory, and low computation capability. Based on the requirements of WSNs, we proposed the Break-The-Glass Access Control (BTG-AC) model which is the modified and redesigned version of Break-The-Glass Role-Based Access Control (BTG-RBAC) model. The several changes within the access control engine are made in BTG-RBAC to apply and fit in WSNs. We developed the BTG-AC model in Ponder2 package. Also a medical scenario was developed to evaluate the BTG-AC model for medical data in WSNs. In this paper, detail design, implementation phase, evaluation result and policies evaluation for the BTG-AC model are presented. Based on the evaluation result, the BTG-AC model can be used in WSNs after several modifications have been made under Ponder2 Package.**

I. Introduction

Wireless Sensor Networks (WSNs) have been an area of significant research for a decade because of the potential to change the way of living with applications in military surveillance, electronic medical record, medicine, disaster and emergency management, and many other areas. Recently, WSNs have become more widespread and more active in the research community. The nature of WSNs consist of a hundred or even a thousand of sensor nodes that have an ability to collect, store and transfer data between each other in the network. These days, the sensor nodes can even store and collect multimedia information themselves. A user, who has an appropriate permission, is able to access the collect data at the sensor nodes directly via ad-hoc manner. This means that the data security and control access to that data are essential to provide in WSNs when the users try to access collected data at the sensor nodes. Based on the requirements of application, the provision of security requirements can change. For the military and medical application, the data collected by sensor nodes need to be stored securely and allowed access only to the authorised users. Therefore, some kinds of security mechanism are required for WSNs to provide the security requirements such as confidentiality, integrity, authenticity, etc.

This paper focuses on an access control model in WSNs and Body Area Networks (BANs). The current access control models in information systems are not efficient enough to apply directly in WSNs and BSNs because of limitations such as limited memory, resource and power. These limitations impose unique security challenge. A new light-weight access control model is desired to provide the flexible making process of decision in WSNs. Towards addressing these requirements of WSNs, we developed a BTG-AC model. This is a modified and redesigned version of BTG-RBAC [1] to better fit for WSNs. It provides a flexible approach to the access control engine. The implementation results in Ponder2 framework [2] are also discussed. The remaining structure of this paper is explained as follows. Section 2 presents the related work. Section 3 discusses an overview of the BTG-AC model for WSNs. The development and implementation of the BTG-AC model can be seen in Section 4. Section 5 provides evaluation results based on a medial scenario. Section 6 concludes the paper with the suggestion for future work.

II. Related Work

An access control is a critical security service to prevent unauthorised access to certain network resources. In WSNs, users can enter a sensor field directly to access data at the sensor nodes. Different users may have different access privileges to access data at the sensor nodes based on their roles. Maw et al. [3] stated that a considerable number of access control models has been proposed for use in WSNs, though some of them are not yet implemented. Most of the current access control models in WSNs and Wireless Medical Sensor Network (WMSN) are based on traditional Role-Based Access Control (RBAC), which has been widely accepted as a policy access control model. Cryptography-based access control is designed for the untrusted environment, where the lack of global knowledge and control are defining characteristics. Cryptography is relied upon to control data access and to ensure data confidentiality and integrity. Cryptography methods in WSNs should meet the constraints of sensor nodes.

Yu et al. [4] proposed the Fine-grained Distributed Data Access Control (FDAC) model based on Attribute Based

978-1-4799-6644-8/14/$31.00 ©2014 IEEE

Encryption. The main idea of their approach is to provide a distributed data access control which is able to support fine-grained access control over sensor data. A network controller, which stores access structures, acts like a central distribution centre and distributes keys to users in FDAC. Only users with the right access structure and the right key can access data at the sensor nodes. The access structures will be different for each user depending on the access privileges of users. If the network controller is compromised by a malicious user, there will be no security provisioning in the system anymore.

Garcia-Morchon and Wehrle [5] proposed the Context-Aware Role-Based Access Control (CA-RBAC) model based on a modular context structure for WMSNs. The aim of the model is to provide context awareness and adapt its security properties to ensure the users' safety. Normally, an authorised doctor needs to verify his access control role in order to access the medical data of a patient but a nurse may not have the same level of privilege. When the system declares to be a critical or emergency case based on the modular context information, the doctor or nurse can take any action and can access data even though they may not be able to access that data in normal conditions. One of the disadvantages of this model is that there is no prevention or detection mechanism nor verification process to check a user's data access right, when the emergency occurs.

Maw et al. [6], [7] proposed an Adaptive Access Control (A2C) model with privilege overriding and behaviour monitoring to provide fine-grained access control for medical data in WSNs. This model has a similar structure to BTG-RBAC [1] but the main difference is that no human effort is needed to override rules and policies because of an introduction of the users' behaviour trust model, and the prevention and detection mechanism. In this model, the users may be able to override a denial of access, when unexpected events occur. In addition, the users' behaviour trust model is used to check the user's action, location, time, etc but there is no detailed information about the behaviour trust model. Without the behaviour trust model, the access decisions cannot be made effectively.

The current access control models in WSNs such as FDAC, CA-RBAC and A2C are mostly looking at how to avoid overly tight policy in the system. Sometimes, the overly tight access control policy might hold access for the appropriate users in unanticipated events. Ferreira et al introduced the BTG-RBAC engine [1], [8] to integrate BTG in the core RBAC model with obligations. They proposed to securely break access control in a controlled manner. The BTG-RBAC model was developed in Premis policy language with an Apache database and XML for Electronic Medical Records (EMRs). The BTG-RBAC model cannot be applied directly to WSNs because of limitations of WSNs. This means that the proposed access control model needs to be light-weight to apply in WSNs. Therefore, we redesigned and modified the BTG-RBAC model to become a light-weight access control model to fill the gaps of WSNs.

The proposed BTG-AC model has been developed in Ponder2 [2] that is a popular light-weight policy language for BANs and WSNs. Ponder2 is implemented as a Self Managed Cell (SMC) [9]. It is a set of hardware and software components forming an administrative domain. It is capable of self management. We assumed that SMC is performed and worked as the sensor node to evaluate the proposed BTG-AC with the example medical scenario. Ponder2 comprises a self-contained, stand-alone, general-purpose object management system with message passing between objects. It incorporates an awareness of events and policies and implements a policy execution framework. It has a high-level configuration and control language called PonderTalk and user-extensible managed objects are programmed in Java.

III. Break-The-Glass Access Control Model

Based on the requirements of WSNs, we modified and redesigned the framework of the BTG-RBAC model to fit in WSNs. Our model refer to as Break-The-Glass Access Control (BTG-AC) still has similar functions to those of the BTG-RBAC model. The main difference is that the BTG-AC model has been developed and implemented within the Ponder2 policy package for BANs and WSNs. The proposed BTG-AC model is to provide BTG action in access control engine for decision making process regarding access. It provides more flexible control of access to data in the event of emergency. The BTG action will perform within the users' traceability by extending the access control engine with obligations for auditing purposes.

Notwithstanding, an overview of BTG-AC in Ponder2 frame-work [2] can be seen in Figure 1. This shows that there are two main modules in the BTG-AC model: Policy Enforcement Point (PEP) and Policy Decision Point (PDP). The user requests will go through PEP and all the user formation will be forwarded to PDP for the decision making processes. There are limitations and issues for the BTG-AC model in Ponder2 language to fit in WSNs. These are discussed as follow:

- There is no BTG state variable in BTG-AC. This means that a fixed BTG state value is used.
- Initially the BTG state is set to FALSE but the state is set as TRUE if there is policy rule that allows a user to perform the BTG operation. The administrator can change the BTG state variable and create a new BTG state for the another or the same role.
- We have assumed that the authentication process is already provided for PEP in the BTG-AC model

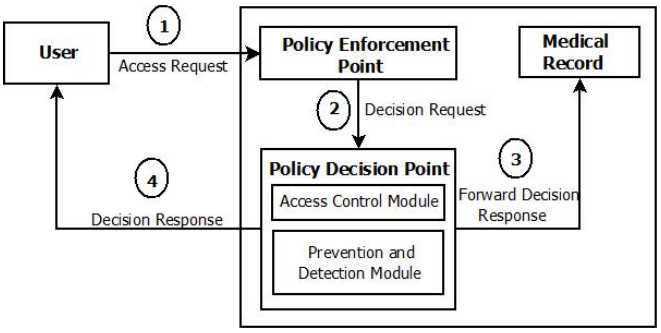


Fig. 1. Overview of the BTG-AC Model

The details information of PEP and PDP are explained next.

A. Policy Enforcement Point (PEP)

In BTG-AC, PEP performs as an authentication service provider between the users and sensor nodes. The authentication service is needed for the provision of security in the system especially when the access control model is allowing users to perform BTG action for data access in emergency situations. A user has to submit the information to PEP for the authentication process. When PEP receives the access request from the users, it will check the users' information such as their identity and cryptographic key. We assumed that the authentication service is provided through use of a users' normal log-in process before forwarding request to PDP. In future, we will work on the implementation of the authentication service in PEP by using Attribute-Based-Encryption (ABE) [10].

B. Policy Decision Point (PDP)

In BTG-AC, PDP is a main module. When PDP receives the decision request from PEP, the access control module will make an access decision. There are different predefined roles and policies in the access control module based on the users location and users' privileges. In the BTG-AC model, there is another module - a prevention and detection module - that keeps a record of all users' information for audit purposes. The two modules cooperate with each other to make the access decision with some flexibility but still within the required degree of prevention and detection. More details of the access control module, and prevention and detection module are explained next.

1) Access Control Module: The access control module is used to enforce the policies for the decision making process. The roles and policies are needed to predefine in advance. Whenever the decision request is forwarded by PEP, the access control module will check whether the information from that decision request is matched with predefined roles and policy. In the access control module, there are three different policies, namely authorisation, BTG and obligation policy. These three policies are developed and designed under the access control module that can be seen on Figure 2.

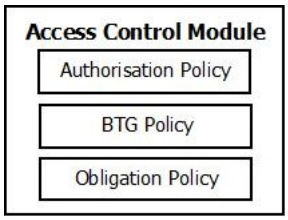


Fig. 2. The Access Control Module

If a user's criteria satisfies the access control policies, the access request will be granted. If they do not match, the access will be denied. In the BTG-AC model, BTG and the obligation policies are introduced to make access decisions in normal as well as emergency situations. A user can perform a BTG action for the targeted object - say, confidential medical record - in an emergency but some obligations will be triggered and performed at the same time. In normal access control models, the decision outcomes will be either permitted or denied access. The existing decision outcomes in the normal access control models are extended by introducing BTG and obligation policy in the access control engine. These decision outcomes are presented as follow:

- (Permit, $\emptyset$) $\rightarrow$ A user has permission to access the targeted object.
- (Permit, OBLGS) $\rightarrow$ A user is allowed to access the targeted object but an obligation is carried out when the access is given.
- (Deny, $\emptyset$) $\rightarrow$ A user request to access the targeted object is denied.
- (Deny, OBLGS) $\rightarrow$ Along side of a denied access, some obligations are performed.
- ($Permit^{(BTG)*(OBLGS)}$) $\rightarrow$ A user's request for access has been granted by performing BTG action and obligations such as "Write to Audit", " Trigger the Alarm" or "A Notification Message" are performed along with access decision.

Based on the above decision outcomes, it is clear that the introduction of BTG and obligation policy is beneficial for medical data in WSNs. The following section explains more details of the authorisation, BTG and obligation policy in that order.

- **Authorisation Policy:** An authorisation policy is used in BTG-AC to enforce an access decision. It also checks whether a user should be allowed to access the targeted object. In authorisation policy, the subject, target and action are checked to enforce the policy. This means that a user, who wants to perform some action on the target object that stores both normal and confidential medical information, has to possess a right access privilege. The access control module will check whether a user's access request has possessed appropriate access right that the subject is allowed to do at the targeted object.
- **Break-the-Glass (BTG) Policy**: A BTG policy is used to perform a BTG operation on a targeted object. To perform the BTG operation, the new role that describes who is allowed to perform a certain action at the targeted object, is added. The obligation policy is used along with the BTG operation allowing an administrator to take actions when the "glass is broken". The new role can be added into the access control module to present how the BTG state variable is reset to FALSE. The BTG state of the permission can be set from TRUE to FALSE or from FALSE to TRUE. The administrator defines the BTG policy for each situation where the BTG action is required by users in an emergency situation.
- **Obligation Policy**: An obligation policy is used along with authorisation and BTG policy in some situations. The obligation policy checks whether one or more conditions have been evaluated and if they have, they carried out one or more actions to be performed. In the BTG-AC model, after the authorisation policy has made the evaluation, some obligations are performed along with the decisions. Similarly the same happened when the BTG policy is activated and made

its decision. The obligation policy is linked with the prevention and detection module to store the user information and his access request as an audit log.

2) Prevention and Detection Module: A prevention and detection module can be used for detecting security violations and flaws in the defined application. It is used to prevent an unauthorised access in the system. Whenever the obligation policy is activated, actions such as write to audit, trigger the alarm, send a notification message to administrator or auditor, etc are performed. There are various methods to store the users' information for the audit log but an event-oriented approach is used to keep a record of the event when it happened, and user information related to that event. Thus, the proposed model can prevent legitimate use by illegitimate users and detect illegitimate use by authorised users.

IV. Development of The Break-The-Glass Access Control Model

The proposed BTG-AC model is an extended version of Ponder2 in which the BTG concept, obligation policy and prevention and detection mechanism are applied together. The interface for all the users such as doctors, nurses and other member of staff is developed in Java based on managed objects in Ponder2. The Java class file is loaded dynamically into SMC. The PEP and PDP are already implemented for the proposed BTG-AC model but the policies definition and expression of authorisation, BTG and obligation policy can vary depend on the requirements of application. The definition and expression of these three policies for medical data in Ponder2 is presented as follow.

A. Authorisation Policy

The terms of the authorisation policy can be changed based on the requirements of the application. In the BTG-AC model, the predefined authorisation policies will be slightly different based on the privileges and roles of the users. An example policy is explained as below:

Def: Permit-Policy
subject A User
role Doctor or Nurse
action Read
target Normal Medical Record

The above authorisation policy defines that a user -a doctor or a nurse- has a right to perform an action called 'read' on a normal medical record. This means that the subject can only access the targeted object, when he meets the criteria of the authorisation policy unless the BTG state variable is TRUE to make a positive decision for access in an emergency situation. Otherwise, the user request will be denied.

B. Break-The-Glass (BTG) Policy

A BTG policy provides a flexibility on decision making process regarding access for the emergency or urgent data access. Thus, the BTG policy allows a user access to confidential data even if he does not have the access right. We assumed that the BTG policy is already defined in advance for these kinds of situations to perform BTG action at the targeted object. If there is no BTG policy for that object, the user request will not be granted. The example BTG policy can be seen as follows:

Def: BTG Policy
subject Nurse
action Read
BTG Yes
target Confidential Medical Record
do Call Obligation Policy

The above BTG policy defines that a user - a nurse - can perform the BTG action to the targeted object but the obligation policy will be activated when the access is given to that user.

C. Obligation Policy

An obligation policy is used along with the authorisation and BTG policies to prevent unauthorised access and to detect security violations. The example of obligation policy is explained as follows:

Def: Audit-Log
on auditrecord
if BTG action is performed
do write.audit < subject, Time, Target, User Role >

The above obligation policy defines that it will be activated when the "glass is broken" for urgent and emergency data access. Thereafter, the users' information such as subject, targeted object and user role is stored as comma separated value (csv) in an audit log for further security purposes.

From the above discussion, it can be seen how the proposed BTG-AC was developed and how the policies for authorisation, BTG and obligation can be defined in Ponder2 for medical data in WSNs. The audit log is kept as comma separate value (csv) extension in the BTG-AC model. The next section will explain how the BTG-AC was evaluated based on a medical scenario that was also developed under Ponder2 package.

V. Evaluation of Break-The-Glass Access Control Model

In this section, a medical scenario is explained. It was developed under the Ponder2 package to evaluate the BTG-AC model for BSNs and WMSNs. We assumed that a SMC [9] is represented as the wearable sensor node. In the example scenario, each patient had his own BSN, which consisted of several sensors. The sensor nodes sense and collect information such as glucose level, temperature, heart rate, etc. We assumed that collected data were stored as the medical record in BSN. Users such as doctors and nurses were trying to access the medical record of the patients via mobile, personal digital assistant or personal computer. For example, sensors are able to interact with each other via IEEE 802.15.4 wireless links and interactions with other mobile phone and personal digital assistant from users via Wifi or Bluetooth. Each SMC had managed its own policy. These policies were specified and could be performed by each SMC.

In a medical scenario, there are two different types of data for each patient: normal medical records (ob^2) and

confidential medical records (ob^1). The access policies for users' access to these medical records will be different based on the access privileges and roles of the users. Also different security levels are required in these medical records. This means that the tight policies might be used for confidential medical records to provide data privacy. Nevertheless, the access to even confidential data can be essential in some circumstances. For example, the doctor should be able to access the confidential medical record of a patient when the nurse cannot but the decision can be changed to a positive decision if the nurse performs the BTG actions.

Subject	Role	Operation	Object	BTG	Obligations
Doctor	r^1	read	ob^1	-	oblg [Write to Audit]
Doctor	r^2	read	ob^2	-	-
Nurse	r^3	read	ob^1	BTG	-
Nurse	r^3	$O^{BTG(read)}$	ob^1	-	oblg [Notify Manager; Write to Audit; Trigger the alarm]
Nurse	r^4	read	ob^2	-	oblg [Write to Audit]
Staff	r^5	read	ob^2	BTG	-
Staff	r^5	$O^{BTG(read)}$	ob^2	-	oblg [Notify Manager; Write to Audit; Trigger the alarm]

TABLE I. EXAMPLE OF BTG-RBAC POLICY

Table 1 shows how the designed of BTG-AC model is developed for medical data in WSNs with predefined authorisation, BTG and obligation policies. In this table, the role (r^1) is related to a doctor. The doctor is allowed to access the confidential medical record (ob^1) of a patient but an obligation such as "Write to Audit" will be taken as an action when the decision has been made. This means that the management teams can check the audit log to detect security breaches of doctor. The role (r^2) allows access of the doctor to the normal medical record (ob^2) without obligation. This means that the stored data at the object (ob^2) is not as sensitive as object (ob^1). The roles and policies for other users such as nurses and other members of staff will be predefined differently.

In role (r^3), the nurse is not permitted to access the confidential data (ob^1) unless he performs the BTG action in that object for emergency data access but some obligations will be activated when "the glass is broken". This means that an extra BTG role is needed for the nurse. The role (r^4) allows the nurse to access the normal medical data (ob^2) but still one obligation action is triggered. The role (r^3) and (r^5) have a similar property. There is no way for other members of staff in the hospital to gain access to the confidential medical record (ob^1). There is a way for them to access the normal medical record (ob^2) but they have to "break the glass". The administrator or manager can easily check the audit log to detect illegitimate use from authorised users and to prevent legitimate use from unauthorised users.

A. Evaluation Framework Based on Example Scenario

We evaluate the BTG-AC model based on an example scenario that was developed under Ponder2 package. In this section, user interface, BTG interface, audit log interface for prevention and detection module and how the access decision was made based on different access policies are presented with following screen shots.

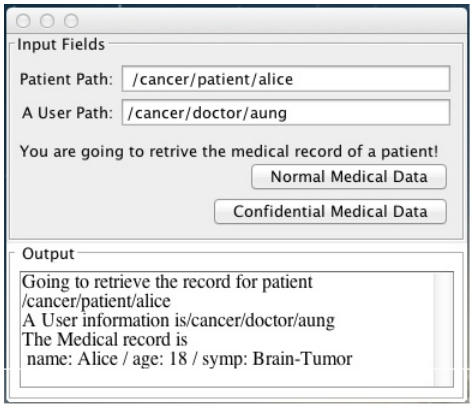


Fig. 3. User Interface for A Doctor

1) User Interface: To evaluated the BTG-AC model for medical data in WSNs, we developed the users' interfaces under Ponder2 package. Based on Figure 3, a doctor (Aung) tries to access the normal medical data of Alice. His access has been granted without any obligation. When he requests access to the confidential data, his requested information will be stored as an audit log to detect security breaches.

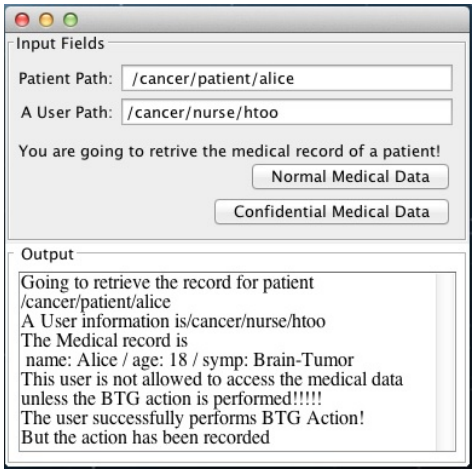


Fig. 4. User Interface for A Nurse

Different access policies are applied to a nurse. Figure 4 shows the interface of a nurse (Htoo). Based on Figure 4, the nurse can access the normal medical record of Alice but one obligation action is triggered and activated when the access is given. The nurse does not have access right regarding access to the confidential medical data unless the BTG policy is used to make an authorisation decision as in urgent and emergency circumstances. At the same time, obligations are triggered and activated. The management teams can check the audit log to prevent and detect security violations.

2) BTG Interface: We developed these simple interfaces for the BTG action. When a nurse wants to perform a BTG action

to access patients' confidential data, the BTG interface will appear. The user's attempt to gain access will be notified to the user and his/her management team and necessary actions will be taken for security. The confirmation message will appear twice before the access is given to the nurse. The interfaces for BTG action are shown in Figure 5.

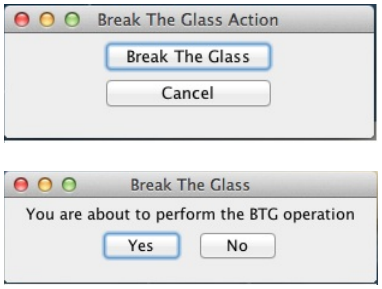


Fig. 5. Interfaces for BTG

3) Audit Log Interface: We developed the audit framework based on managed objects in Ponder2 package. The interface of an audit log can be seen in Figure 6. This Figure shows what kind of information and data are stored in the audit log. The first audit log shows that the nurse accessed the normal medical record of Alice. For the second log, the same nurse requested access to the confidential medical record by performing the BTG action and his or her access was granted. A doctor, who accessed a confidential medical record, was granted access as can be seen in the audit log of that patient. All the access requests to the medical records are recorded in which everyday is determine by the user' role. Based on the audit log, the management teams can check which users performed the BTG action and who among these will be granted access to the confidential medical records.

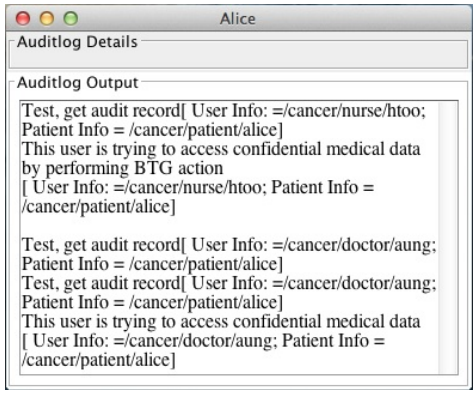


Fig. 6. Interface for Audit Log

B. Summary

Based on the evaluation results with a medical scenario, the BTG-RBAC model proposed by Ferreira et al [1] can be applied for medical data in WSNs after the framework and several changes within the access control engine are made. The BTG-AC model provides flexibility of decision making processes regarding access to medical records. The three policies such as authorisation, BTG and obligation cooperate with each other to make decisions about data access in the emergency situations. Based on the overall outcomes, the BTG-AC model can be applied in BSN and WSNs.

VI. Conclusion and Future Work

The overall contributions of this paper are the design and development of BTG-AC model for medical data in WSNs. The concepts of BTG, prevention and detection mechanism, and obligation provide more flexible access than other current access control models in WSNs. The BTG-AC model has been developed under Ponder2 package. All the modules - access control module and prevention and detection module - have been found to cooperate together to make an access decision and recorded a users' accountability to illegitimate data usage from authorised users as well as excluding illegitimate users for data access. One possible weakness of BTG-AC is that the human decision is needed to predefine BTG policy for each object. We are considered to redesign the BTG-AC model based on that weakness as future work. In addition, we will plan to develop the BTG-AC model within the actual sensor nodes for medical applications in WSNs.

References

[1] A. Ferreira, D. Chadwick, P. Farinha, R. Correia, G. Zao, R. Chilro, and L. Antunes, "How to securely break into rbac: The btg-rbac model," in *Proceedings of the 2009 Annual Computer Security Applications Conference*, ser. ACSAC '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 23–31.

[2] K. Twidle, E. Lupu, N. Dulay, and M. Sloman, "Ponder2 - a policy environment for autonomous pervasive systems," in *Proceedings of the 2008 IEEE Workshop on Policies for Distributed Systems and Networks*, ser. POLICY '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 245–246.

[3] H. A. Maw, H. Xiao, B. Christianson, and J. A. Malcolm, "A survey of access control models in wireless sensor networks," *Journal of Sensor and Actuator Networks*, vol. 3, no. 2, pp. 150–180, 2014. [Online]. Available: http://www.mdpi.com/2224-2708/3/2/150

[4] S. Yu, K. Ren, and W. Lou, "Fdac: Toward fine-grained distributed data access control in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 4, pp. 673–686, Apr. 2011.

[5] O. Garcia-Morchon and K. Wehrle, "Modular context-aware access control for medical sensor networks," in *Proceedings of the 15th ACM symposium on Access control models and technologies*, ser. SACMAT '10. New York, NY, USA: ACM, 2010, pp. 129–138.

[6] H. Maw, H. Xiao, and B. Christianson, "An adaptive access control model for medical data in wireless sensor networks," in *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom) (IEEE Healthcom 2013)*, Lisbon, Portugal, Oct. 2013.

[7] H. A. Maw, H. Xiao, and B. Christianson, "An adaptive access control model with privileges overriding and behaviour monitoring in wireless sensor networks," in *Proceedings of the 8H ACM Symposium on QoS and Security for Wireless and Mobile Networks*, ser. Q2SWinet '12. New York, NY, USA: ACM, 2012, pp. 81–84.

[8] A. Ferreira, R. Cruz-Correia, L. Antunes, P. Farinha, E. Oliveira-Palhares, D. W. Chadwick, and A. Costa-Pereira, "How to break access control in a controlled manner," in *Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems*, ser. CBMS '06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 847–854.

[9] E. Lupu, N. Dulay, M. Sloman, J. Sventek, S. Heeps, S. Strowes, K. Twidle, S.-L. Keoh, and A. Schaeffer-Filho, "Amuse: autonomic management of ubiquitous e-health systems," *Concurr. Comput. : Pract. Exper.*, vol. 20, no. 3, pp. 277–295, Mar. 2008.

[10] V. Goyal, A. Sahai, O. Pandey, and B. Waters, "Attribute-based encryption for fine-grained access control for encrypted data," *Wireless Network, IEEE*, 2006.

A.5 BTG-AC: Break-The-Glass Access Control Model for Medical Data in Wireless Sensor Network

[Submitted in IEEE Journal of Biomedical and Health Informatics]
(An Evaluation of Break-The-Glass Access Control Model for Medical Data in Wireless Sensor Networks (IEEE-Healthcom'14) paper was selected among the best papers and offered to submit a modified version to be published in a special issue of the International Journal IEEE-JBHI.)

BTG-AC: Break-The-Glass Access Control Model for Medical Data in Wireless Sensor Networks

Journal:	*IEEE Journal of Biomedical and Health Informatics*
Manuscript ID:	JBHI-00101-2015
Manuscript Type:	IEEE-Healthcom2014
Date Submitted by the Author:	16-Feb-2015
Complete List of Authors:	Maw, Htoo; University of Hertfordshire, School of Computer Science Xiao, Hannan; University of Hertfordshire, School of Computer Science Christianson, Bruce; University of Hertfordshire, School of Computer Science Malcolm, James; University of Hertfordshire, School of Computer Science
TIPS:	Access Control, Healthcare, Data Availability

BTG-AC: Break-The-Glass Access Control Model for Medical Data in Wireless Sensor Networks

Htoo Aung Maw, Hannan Xiao, Bruce Christianson and James A. Malcolm
School of Computer Science
University of Hertfordshire
Hatfield, United Kingdom
Email: (h.maw,h.xiao,b.christianson,j.a.malcolm)@herts.ac.uk

***Abstract*—Wireless Sensor Networks (WSNs) have recently attracted much interest in the research community because of their wide range of applications. An emerging application for WSNs involves their use in healthcare where they are generally termed Wireless Medical Sensor Networks (WMSNs). In a hospital, outfitting every patient with tiny, wearable, wireless vital sign sensors would allow doctors, nurses and other caregivers to continuously monitor the state of their patients. In such a scenario, patients are expected to be treated in reasonable time, so, an access control model is needed which will provide both real-time access to comprehensive medical records and detect unauthorised access to sensitive data. In emergency situations, a doctor or nurse needs to access data immediately. The loss in data availability can result in further decline in the patient's condition or can even lead to death. Therefore, the availability of data is more important than any security concern in emergency situations. To address that research issue for medical data in WSNs, we propose the Break-The-Glass Access Control (BTG-AC) model that is a modified and redesigned version of the Break-The-Glass Role-Based Access Control (BTG-RBAC) model to address data availability issue and to detect the security policy violations from both authorised and unauthorised users. Several changes within the access control engine are made in BTG-RBAC in order to make the new BTG-AC to apply and fit in WSNs. This paper presents the detailed design and development of the BTG-AC model based on a healthcare scenario. The evaluation results show that the concepts of BTG, prevention and detection mechanism, and obligation provide more flexible access than other current access control models in WSNs. Additionally, we compare the BTG-AC model with an adaptive access control model (A^2C) which has similar properties, for further evaluation. Alongside with the comparison, the advantages and disadvantages of BTG-AC over current WSN access control models are presented.**

I. Introduction

Wireless Sensor Networks (WSNs) have been an area of significant research for more than a decade because of the major potential applications in military surveillance, industrial control, medicine, disaster and emergency management, and many other areas. The nature of WSNs consist of hundreds or even thousands of sensor nodes that have an ability to collect, store and transfer data between each other in the network. These days, sensor nodes can store and collect multimedia information themselves. A user, who has an appropriate permission, is able to access the collected data at the sensor nodes directly via ad-hoc manner. Data security and access control to that data are essential to provide in WSNs when the users try to access collected data at the sensor nodes. Based on the requirements of application, the provision of security requirements can change. For the military and medical application, the data collected by sensor nodes need to be stored securely and allowed access only to the authorised users. Therefore, security mechanisms are required for WSNs to provide the security requirements such as confidentiality, integrity, authenticity, etc.

Most of the current WSN access control models are based on traditional Role-Base Access Control model (RBAC) [1] to control data access based on roles. The decision is binary: deny or permit access. The RBAC model has been widely accepted as a policy-based access control model and it is suitable for most commercial applications but roles and policies need to be predefined before the system can make decisions. Some WSN access control models used cryptographic methods for data storage and data access control but the systems still need to predefine attributes, roles and policies before deployment. It is, however, difficult to determine in advance all the possible needs for access in real world applications because there may be unexpected situations at any time.

There are many potential situations that cannot be defined in traditional RBAC and cryptography-based systems. For example, the roles and policies for emergency and unexpected situations cannot be defined in advance. When the system faces these kinds of situations, what will the system do? Does the system wait until the authorised user comes and logs in? Alternatively, in the medical scenario, does a nurse wait for a doctor who takes care of a patient, in order to retrieve that patient's medical record? In most of the emergency and urgent cases, the users cannot wait until someone comes in order to retrieve the necessary data. Given this, what is a possible method to provide a flexible approach in the access control engine? For real world applications, the system needs to be flexible enough to make decisions regarding data access based on unusual situations in addition to normally defined situations. Using the traditional RBAC model often cannot fulfil the requirements of real world applications in WSNs. Therefore, a new access control model is needed to provide a flexible policy to address the data availability issue and to detect the security policy violations [2] such as unauthorised information release.

To address the above research issue in WSN, we developed a Break The Glass Access Control (BTG-AC) model. This is a modified and redesigned version of Break-The-Glass Role-Based Access Control (BTG-RBAC) [3], [4] to better fit the requirements of WSNs. It provides a flexible approach to the access control engine for data availability purpose. The main contribution of this paper is the design and development of

a lightweight BTG-AC model to address the data availability issue and to detect the security policy violations from both authorised and unauthorised users in healthcare application.

The remaining structure of this paper is explained as follows. Section 2 presents the related work. Section 3 discusses an overview of the BTG-AC model for WSNs. The development and implementation of the BTG-AC model in Ponder2 framework [5] can be seen in Section 4. Section 5 evaluates BTG-AC based on a medical scenario. Section 6 presents the frameworks of the adaptive access control model (A^2C) which was proposed by Maw *et al.* [6] to make a comparison with the proposed BTG-AC model in WSNs. Additionally, this section reviews the advantages and disadvantages of BTG-AC over current WSN access control models. Section 7 concludes the paper with the suggestion for future work.

II. Related Work

Access control is a critical security service to prevent unauthorised access to network resources. In WSNs, users can enter a sensor field directly to access data at the sensor nodes. Different users may have different access privileges to access data at the sensor nodes based on their roles. Maw *et al.* [7] stated that a considerable number of access control models have been proposed for use in WSNs, though some of them are not yet implemented. Most of the current access control models in WSNs and Wireless Medical Sensor Network (WMSN) are based on traditional Role-Based Access Control (RBAC), which has been widely accepted as a policy access control model. The RBAC based access control models such as trust and centrality-based access control model [8], Maerien's model [9] and Gaurkar's model [10] are aimed to prevents a malicious node from joining the sensor network. Cryptography-based access control is designed for the untrusted environment, where the lack of global knowledge and control are defining characteristics. Cryptography is relied upon to control data access and to ensure data confidentiality and integrity. Cryptography methods in WSNs should meet the constraints of sensor nodes.

Yu *et al.* [11] proposed the Fine-grained Distributed Data Access Control (FDAC) model based on Attribute Based Encryption. The main idea of their approach is to provide a distributed data access control, which is able to support fine-grained access control over sensor data. A network controller, which stores access structures, acts like a central distribution centre and distributes keys to users in FDAC. Only users with the right access structure and the right key can access data at the sensor nodes. The access structures will be different for each user depending on the access privileges of users. If a malicious user compromises the network controller, there will be no security provisioning in the system anymore. Distributed fine-grained access control model [12] has a similar structure as FDAC but the main difference is that this model uses different distribution centres for key management to avoid a single point to failure problem. The same concept is applied to distributed fine-grained data access control for distributed sensor networks that was proposed by Hur [13]. The data aggregator is used in this model as central management object for data encryption and key distribution.

Garcia-Morchon and Wehrle [14] proposed the Context-Aware Role-Based Access Control (CA-RBAC) model based on a modular context structure for WMSNs. The aim of the model is to provide context awareness and adapt its security properties to ensure the users' safety. Normally, an authorised doctor needs to verify his access control role in order to access the medical data of a patient but a nurse may not have the same level of privilege. When the system declares to be a critical or emergency case based on the modular context information, the doctor or nurse can take any action and can access data even though they may not be able to access that data in normal conditions. One of the disadvantages of this model is that there is no prevention or detection mechanism nor verification process to check a user's data access right, when the emergency occurs.

Maw *et al.* [6], [15] proposed an Adaptive Access Control (A^2C) model with privilege overriding and behaviour monitoring to provide fine-grained access control for medical data in WSNs. In this model, no human effort is needed to override rules and policies because of the introduction of the users' behaviour trust model, and the prevention and detection mechanism. In this model, the users may be able to override a denial of access, when unexpected events occur. In addition, the users' behaviour trust model is used to check the user's action, location, time, etc. but there is no detailed information about the behaviour trust model. Without the behaviour trust model, the access decisions cannot be made effectively. This model is compared with the proposed BTG-AC model in session VI.

The current access control models in WSNs such as FDAC, CA-RBAC and A^2C are mostly looking at how to avoid overly tight policy in the system. Sometimes, the overly tight access control policy might hold access for the appropriate users in unanticipated events. Ferreira *et al.* introduced the BTG-RBAC engine [3], [4] to integrate BTG in the core RBAC model with obligations. They proposed to securely break access control in a controlled manner. The BTG approach can be easily applied in the existing architectures and systems. It is very useful for existing systems because it does not involve additional automated technology. It is intended to cover unanticipated and emergency situations and should not be used as a replacement for a help-desk. BTG-AC can make decisions regarding data access quickly without unreasonable administrative involvements and delays. The BTG-RBAC model was developed in Premis policy language with an Apache database and XML for Electronic Medical Records (EMRs). The BTG-RBAC model cannot be applied directly to WSNs because of limitations of WSNs. This means that the proposed access control model needs to be lightweight to apply in WSNs. Therefore, we redesigned and modified the BTG-RBAC model to become a lightweight access control model to fill the gaps of WSNs.

III. Break-The-Glass Access Control Model

Based on the requirements of WSNs, we modified and redesigned the framework of the BTG-RBAC model to fit in WSNs. Our model is referred to as Break-The-Glass Access Control (BTG-AC) and has similar functions to those of the BTG-RBAC model. The proposed BTG-AC model is to provide BTG action in access control engine for decision-making process regarding access in Body Sensor Networks and WSNs. It provides a flexible approach for data access control in the event of emergency. The BTG action will perform within

the users' traceability by extending the access control engine with obligations for auditing purposes.

Notwithstanding, an overview of BTG-AC can be seen in Figure 1. This shows that there are two main modules in the BTG-AC model: Policy Enforcement Point (PEP) and Policy Decision Point (PDP). The user requests will go through PEP and all the user formation will be forwarded to PDP for the decision-making processes. There are limitations and issues for the BTG-AC model in Ponder2 language to fit in WSNs. These are discussed as follow:

- There is no BTG state variable in BTG-AC. This means that a fixed BTG state value is used.
- Initially the BTG state is set to FALSE but the state is set as TRUE if there is policy rule that allows a user to perform the BTG operation. The administrator can change the BTG state variable and create a new BTG state for another or the same role.

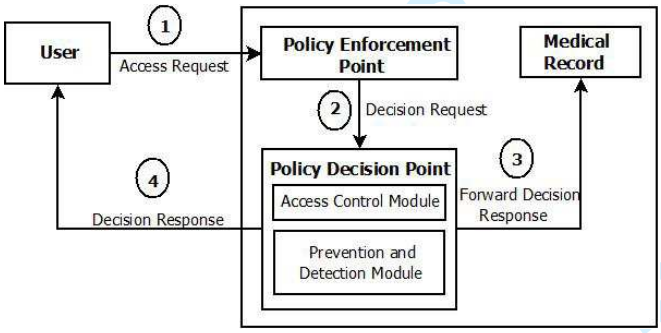


Fig. 1. Overview of the BTG-AC Model

The details of PEP and PDP are explained next.

A. Policy Enforcement Point (PEP)

In BTG-AC, PEP performs as an authentication service provider between the users and sensor nodes. The authentication service is needed for the provision of security in the system especially when the access control model is allowing users to perform BTG action for data access in emergency situations. A user has to submit the information to PEP for the authentication process. When PEP receives the access request from the users, it will check the users' information such as their identity and cryptographic key. We assumed that the authentication service is provided through use of a users' normal login process before forwarding request to PDP. In future, we will work on the implementation of the authentication service in PEP by using Attribute-Based-Encryption (ABE) [16].

B. Policy Decision Point (PDP)

In BTG-AC, PDP is a main module. When PDP receives the decision request from PEP, the access control module will make an access decision. There are different predefined roles and policies in the access control module based on the users' location and users' privileges. In the BTG-AC model, there is another module - prevention and detection module - keeps a record of all users' information for audit purposes. The two modules cooperate with each other to make the access decision with some flexibility but still within the required degree of prevention and detection.

1) Access Control Module: The access control module is used to enforce the policies for the decision-making process. The roles and policies need to be defined in advance. Whenever the decision request is forwarded by PEP, the access control module will check whether the information from that decision request is matched with predefined roles and policy. In the access control module, there are three different policies, namely authorisation, BTG and obligation policy. These three policies are developed and designed under the access control module that can be seen on Figure 2.

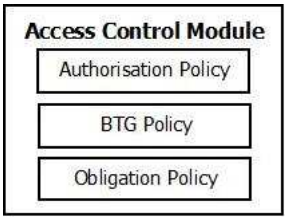


Fig. 2. The Access Control Module

In normal access control models, the decision outcomes will be either permitted or denied access. If a user's criteria satisfy the access control policies, the access request will be granted. If they do not match, the access will be denied. In the BTG-AC model, BTG and the obligation policies are introduced to make access decisions in normal as well as emergency situations. A user can perform a BTG action for the targeted object - say, confidential medical record - in an emergency but some obligations will be triggered and performed at the same time. The existing decision outcomes in the normal access control models are extended by introducing BTG and obligation policy in the access control engine. These decision outcomes are presented as follow:

- (Permit, $\emptyset$) $\rightarrow$ A user has permission to access the targeted object.
- (Permit, OBLGS) $\rightarrow$ A user is allowed to access the targeted object but an obligation is carried out when the access is given.
- (Deny, $\emptyset$) $\rightarrow$ A user request to access the targeted object is denied.
- (Deny, OBLGS) $\rightarrow$ Along side of a denied access, some obligations are performed.
- (Permit, (BTG)*(OBLGS)) $\rightarrow$ A user's request for access has been granted by performing BTG action and obligations such as "Write to Audit", "Trigger the Alarm" or "A Notification Message" are performed along with access decision.

Based on the above decision outcomes, it is clear that the introduction of BTG and obligation policy is beneficial for medical data in WSNs by extending the existing decision outcomes. The following section explains more details of the authorisation, BTG and obligation policies.

- **Authorisation Policy:** An authorisation policy is used in BTG-AC to enforce an access decision. It also

checks whether a user should be allowed to access the targeted object. In authorisation policy, the subject, target and action are checked to enforce the policy. This means that a user, who wants to perform some action on the target object that stores both normal and confidential medical information, has to possess a right access privilege. The access control module will check whether a user's access request has possessed appropriate access right that the subject is allowed to do at the targeted object.

- **Break-the-Glass (BTG) Policy**: A BTG policy is used to perform a BTG operation on a targeted object. To perform the BTG operation, the new role that describes who is allowed to perform a certain action at the targeted object, is added. The obligation policy is used along with the BTG operation allowing an administrator to take actions when the "glass is broken". The new role can be added into the access control module to present how the BTG state variable is reset to FALSE. The BTG state of the permission can be set from TRUE to FALSE or from FALSE to TRUE. The administrator defines the BTG policy for each situation where users in an emergency situation require the BTG action.
- **Obligation Policy**: An obligation policy is used along with authorisation and BTG policy in some situations. The obligation policy checks whether one or more conditions have been evaluated and if they have, they carried out one or more actions to be performed. In the BTG-AC model, after the authorisation policy has made the evaluation, some obligations are performed along with the decisions. Similarly, the same happened when the BTG policy is activated and made its decision. The obligation policy is linked with the prevention and detection module to store the user information and his access request as an audit log.

2) Prevention and Detection Module: A prevention and detection module can be used for detecting security violations and flaws in the defined application. It is used to prevent an unauthorised access in the system. Whenever the obligation policy is activated, actions such as write to audit, trigger the alarm, send a notification message to administrator or auditor, etc. are performed. There are various methods to store the users' information for the audit log but an event-oriented approach [17] is used to keep a record of the event when it happened, and user information related to that event. Thus, the proposed model can detect an unauthorised information release by authorised users.

IV. Development of The Break-The-Glass Access Control Model

The proposed BTG-AC model has been developed in Ponder2 [5] that is a popular lightweight policy language for BANs and WSNs. Ponder2 is implemented as a Self-Managed Cell (SMC) [18]. It is a set of hardware and software components forming an administrative domain. It is capable of self-management. We assumed that SMC is performed and worked as the sensor node to evaluate the proposed BTG-AC with the example medical scenario. Ponder2 comprises a self-contained, stand-alone, general-purpose object management system with message passing between objects. It incorporates an awareness of events and policies and implements a policy execution framework. It has a high-level configuration and control language called PonderTalk and user-extensible managed objects are programmed in Java.

The proposed BTG-AC model is an extended version of Ponder2 in which the BTG concept, obligation policy and prevention and detection mechanism are applied together. The interface for all the users such as doctors, nurses and other member of staff is developed in Java based on managed objects in Ponder2. The Java class file is loaded dynamically into SMC. The PEP and PDP are already implemented for the proposed BTG-AC model but the policies definition and expression of authorisation, BTG and obligation policy can vary depend on the requirements of application. The definition and expression of these three policies for medical data in Ponder2 are presented as follow.

A. Authorisation Policy

The terms of the authorisation policy can be changed based on the requirements of the application. In the BTG-AC model, the predefined authorisation policies will be slightly different based on the privileges and roles of the users. An example policy is explained as below:

Def: Permit-Policy
subject A User
role Doctor or Nurse
action Read
target Normal Medical Record

The above authorisation policy defines that a user (a doctor or a nurse) has a right to perform an action called 'read' on a normal medical record. This means that the subject can only access the targeted object, when he meets the criteria of the authorisation policy unless the BTG state variable is TRUE to make a positive decision for access in an emergency situation. Otherwise, the user request will be denied.

B. Break-The-Glass (BTG) Policy

A BTG policy provides flexibility on decision-making process regarding access for the emergency or urgent data access. Thus, the BTG policy allows a user access to confidential data even if he does not have the access right. We assumed that the BTG policy is already defined in advance for these kinds of situations to perform BTG action at the targeted object. If there is no BTG policy for that object, the user request will not be granted. The example BTG policy can be seen as follows:

Def: BTG Policy
subject Nurse
action Read
BTG Yes
target Confidential Medical Record
do Call Obligation Policy

The above BTG policy defines that a user (a nurse) can perform the BTG action to the targeted object but the obligation policy will be activated when the access is given to that user.

Policy	Subject	Role	Operation	Object	BTG	Obligations
1	Doctor	r_1	read	ob_2		
2	Doctor	r_2	read	ob_1		oblg [Write to Audit]
3	Nurse	r_3	read	ob_1	BTG	
4	Nurse	r_3	$O^{BTG(read)}$	ob_1		oblg [Notify Manager; Write to Audit; Reset BTG to FALSE after 30 mins]
5	Nurse	r_4	$reset^{BTG}$	ob_1		
6	Nurse	r_5	read	ob_2		oblg [Write to Audit]

TABLE I. EXAMPLE OF BTG-RBAC POLICY

C. Obligation Policy

An obligation policy is used along with the authorisation and BTG policies to prevent unauthorised access and to detect security violations. The example of obligation policy is explained as follows:

Def: Audit-Log
on auditrecord
if BTG action is performed
do write.audit < subject, Time, Target, User Role >

The above obligation policy defines what is a course of action that will be activated when the "glass is broken" for urgent and emergency data access. Thereafter, the users' information such as subject, targeted object and user role is stored as comma separated value (csv) in an audit log for further security purposes.

From the above discussion, it can be seen how the proposed BTG-AC was developed and how the policies for authorisation, BTG and obligation can be defined in Ponder2 for medical data in WSNs. The audit log is kept as comma separated value (csv) extension in the BTG-AC model. The next section will explain how the BTG-AC was evaluated based on a medical scenario that was also developed under Ponder2 package.

V. EVALUATION OF BREAK-THE-GLASS ACCESS CONTROL MODEL

A. Evaluation Scenario

In this section, a medical scenario is explained. It was developed under the Ponder2 package to evaluate the BTG-AC model for BSNs and WMSNs. We assumed that a SMC [18] is represented as a wearable sensor node. In the example scenario, each patient had his own BSN, which consisted of several sensors. The sensor nodes sense and collect information such as glucose level, temperature, heart rate, etc. We assumed that collected data were stored as the medical record in BSNs. Users such as doctors and nurses were trying to access the medical record of the patients via mobile, personal digital assistant or personal computer. For example, sensors are able to interact with each other via IEEE 802.15.4 wireless links and interactions with other mobile phone and personal digital assistant from users via Wifi or Bluetooth. Each SMC had managed its own policy. These policies were specified and could be performed by each SMC.

In a medical scenario, there are two different types of data for each patient: confidential medical records (ob_1) and normal medical records (ob_2). The access policies for users' access to these medical records will be different based on the access privileges and roles of the users. In addition, different security levels are required in these medical records. Tight policies might be used for confidential medical records to provide data privacy. Nevertheless, the access to even confidential data can be essential in some circumstances. For example, the doctor should be able to access the confidential medical record of a patient when the nurse cannot but the decision can be changed to a positive decision if the nurse performs the BTG actions.

In Table I, policy 1 states that the role r_1 is allowed to read object 2 (ob_2). As in policy 2, the doctor is allowed to access the confidential medical record (ob_1) based on r_2 but an obligation such as "Write to Audit" is activated. In policy 3, the nurse is not permitted to access the confidential data (ob_1) unless he or she performs the BTG action in that object for emergency data access, but the BTG variable needs to be TRUE meaning that BTG is enabled. Therefore, an extra BTG role is needed for the nurse (see policy 5). Additionally, policy 4 will be activated and at the same time, some obligations will be activated when "the glass is broken".

Policy 4 demonstrates that if policy 3 is allowed, the system will perform three obligations such as "write to audit", "notify to manager", "reset BTG variable to FALSE after 30 minutes". This implies BTG = TRUE, FALSE. Policy 5 is quite simple. It is allowed to reset the BTG variable to FALSE to TRUE or TRUE to FALSE. For policy 6, r_5 allows a user to read ob_1 but it will trigger one obligation that is "write to audit". The administrator or manager can easily check the audit log to detect any use from authorised users and to prevent any use from unauthorised users.

B. Evaluation Framework Based on Example Scenario

We evaluate the BTG-AC model based on the above example scenario and policy definition that was developed under Ponder2 package. In this section, user interface, BTG interface, audit log interface and how the access decision was made based on different access policies are presented with screen shots.

1) User Interface: To evaluate the BTG-AC model for medical data in WSNs, we developed the users' interfaces under Ponder2 package. Based on Figure 3, a doctor (Aung) tries to access the normal medical data of Alice. His access has been granted without any obligation. When he requests access to the confidential data, his access request has been granted

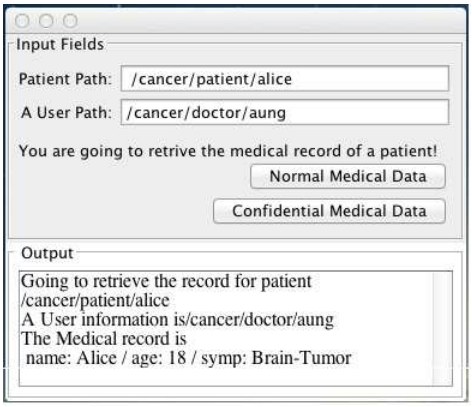


Fig. 3. User Interface for A Doctor

but his requested information will be stored as an audit log to detect security breaches.

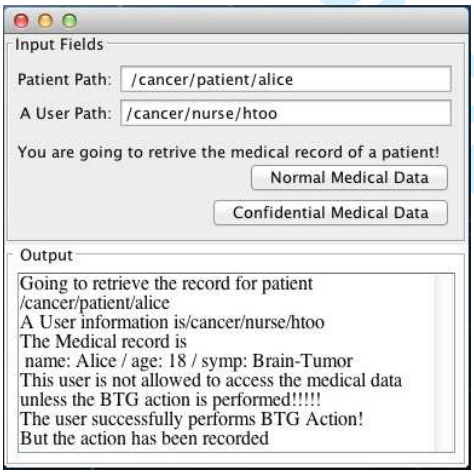


Fig. 4. User Interface for A Nurse

Different access policies are applied to a nurse. Figure 4 shows the interface of a nurse (Htoo). The nurse can access the normal medical record of Alice but one obligation action is triggered and activated when the access is given. The nurse does not have access right regarding access to the confidential medical data unless the BTG policy is used to make an authorisation decision in urgent and emergency circumstances. At the same time, obligations are triggered and activated. The management teams can check the audit log to prevent and detect security violations.

2) BTG: When a nurse wants to perform a BTG action to access patients' confidential data, a BTG interface will appear. The user's attempt to gain access will be notified to the user and his/her management team and necessary actions will be taken. The confirmation message will appear twice before the access is given to the nurse. Additionally, another simple authentication process is used to protect the privacy of patients' information by using normal log in process before the second confirmation box appears. The interfaces for BTG action are shown in Figure 5.

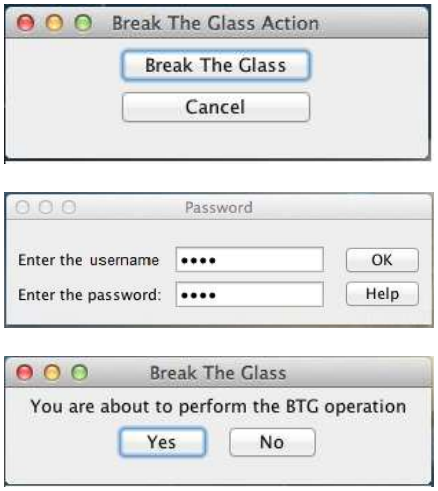


Fig. 5. Interfaces for BTG

3) Audit Log: We developed the audit framework based on managed objects in Ponder2 package. The interface of an audit log can be seen in Figure 6. This figure shows what kind of information and data are stored in the audit log. The first audit log shows that the nurse accessed the normal medical record of Alice. For the second log, the same nurse requested access to the confidential medical record by performing the BTG action and his or her access be granted. A doctor, who accessed a confidential medical record, was granted access as can be seen in the audit log of that patient. All the access requests to the medical records are recorded in which every day is determined by the user' role. Based on the audit log, the management teams can check which users performed the BTG action and who among these will be granted access to the confidential medical records.

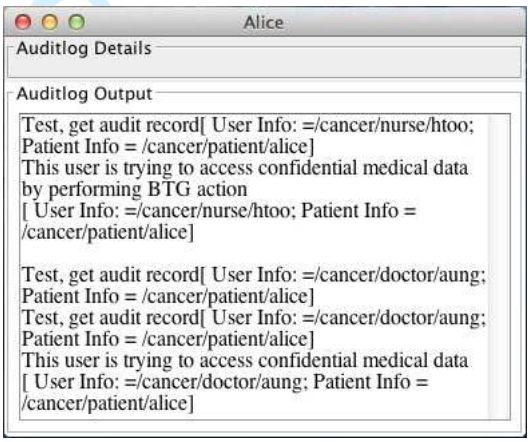


Fig. 6. Interface for Audit Log

C. Summary

Based on the evaluation results with a medical scenario, the BTG-AC model can be applied for medical data in WSNs after the framework and several changes within the access control engine are made. The BTG-AC model provides flexibility

of decision-making processes regarding access to medical records. The three policies such as authorisation, BTG and obligation cooperate with each other to make decisions about data access in the emergency situations.

VI. Comparison Between BTG-AC and A^{2}C Model

To make a full comparison with the proposed BTG-AC model, an adaptive access control model (A^{2}C) model is chose among current WSN access control model because it has similar properties as BTG-AC. As well, both models are developed in Ponder2 policy language. This section recapitulates both A^{2}C and BTG-AC models to make a comparison based on the evaluation criteria. Firstly, a brief discussion of the A^{2}C model is explained. Additionally, the evaluation criteria are discussed for both A^{2}C and BTG-AC models. This is followed by an exploration of advantages and disadvantages of BTG-AC over current access control models in WSNs.

A. Adaptive Access Control Model (A^{2}C)

The A^{2}C model was proposed by Maw *et al.* [15] to provide a flexible access decision in WSNs. This is incorporated the concept of possibility-with-override [19], [20] into WSN for hard-to-define and unanticipated situations. Possibility-with-override means users might be able to override a denial of access, when unexpected events occur. The A^{2}C model also uses user behaviour monitoring and trust model to check users' actions, location, time, etc. Whenever users try to access data at the sensor nodes, all user behaviour and users' information will be kept by prevention and detection mechanism as an audit record to detect and prevent abnormal and unauthorised access. The overview diagram of the A^{2}C model can be seen on Figure 7.

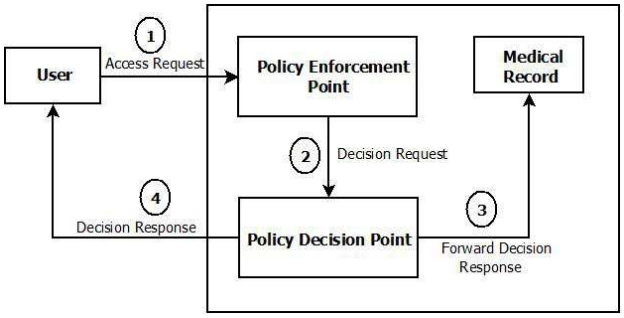


Fig. 7. An Overview of Implementation Framework

There are similarities between A^{2}C and BTG-AC model. There are two main modules in the proposed access control model: Policy Enforcement Point (PEP) and Policy Decision Point (PDP). Whenever a user requests the access to an object, an access request will go through PEP for the authentication process and then it will forward a decision request to PDP for decision-making process. PDP makes the access decision on user request based on defined policy. The decision response will be forwarded internally to the target. In addition, PDP will forward the decision response to the users, whether they have the privileges to access data at the sensor nodes or not.

The main difference between A^{2}C and BTG-AC models is that the user behaviour trust module is introduced in PDP

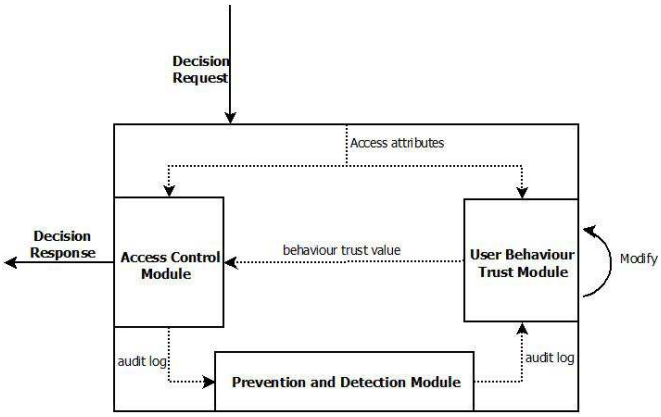


Fig. 8. Policy Decision Point

as shown in Figure 8. Therefore, there are three modules inside PDP unlike BTG-AC (see Figure 1). These modules are the access control module, prevention and detection module, and user behaviour trust module. After PEP forwards the decision request to PDP, the information such as user, action, environment and context information will be forwarded to the access control module and the user behaviour trust module. The user behaviour trust module will calculate the trust value. The overall structure of users' behaviour trust module is shown in Figure 9.

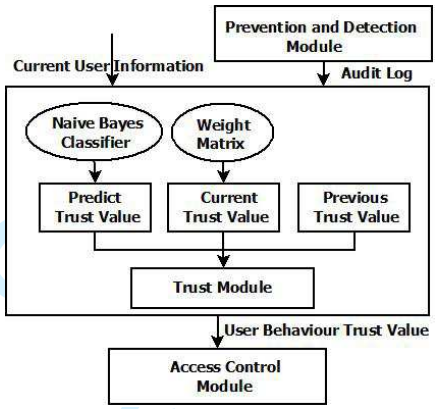


Fig. 9. A Framework of User Behaviour Trust Module

To determine the user behaviour trust value, the previous, predicted and current value of user behaviour trust will be used. Current trust value will be calculated and evaluated based on the user information that is forwarded by the PEP. The previous trust value is stored in the trust module. For predicting user behaviour trust value, Naive Bayes and Bayesian classification algorithm [21], [22] will be used. Predicting user behaviour is important and significant in forming a trustworthy network. For the classification algorithm, the audit record from the prevention and detection module will be used. There might be more than two classifiers to predict the user behaviour trust value. After the evaluation and calculation behaviour trust, that value will be forwarded to the access control module. The access control module will use the trust value from the user behaviour trust module and the other information, which is forwarded by PEP, to make access decisions on the user request

based on the authorisation policy, the overriding policy and the obligation policy.

B. Evaluation Based on Features

In this section, the comparison of the A^{2}C and BTG-AC models are made based on the evaluation criteria including the network architecture model, the concepts and approaches, the decision outcomes, the access control policy and role, the data confidentiality and data privacy, and the data availability.

1) Network Architecture Model: Access control models can be different based on their network architecture model when the cryptographic keys, roles, policies and attributes are distributed to users from the trusted authority or controller. The A^{2}C model is based on a distributed approach to make and adjust access decisions dynamically. This means that each sensor is deployed with the access control engine to make an effective local decision within itself based on the users' request and the sensor is required to store access policies. Unlike A^{2}C, the BTG-AC model is based on a centralised approach because each sensor node cannot store all the possible situations and BTG operations in the system. The disadvantage is that there might be a single point of failure in the BTG-AC model.

2) Concepts and Approaches: The A^{2}C and BTG-AC models use different concepts and approaches to fill the research gaps and the requirements of the application in WSNs. One similarity between these two WSN access control models is that both aim to provide data availability in emergency and unanticipated situations. An outline of the concepts and approaches for these two models can be seen in Table II.

A^{2}C	**BTG-AC**
- Discretionary Overriding of Access Control	- Role Based Access Control
- User Behaviour Trust Model	- Break-The-Glass concept
- Prevention and Detection Mechanism	- Prevention and Detection Mechanism

TABLE II. THE CONCEPTS AND APPROACHES FOR A^{2}C AND BTG-AC

There is limited local decision-making capability in current WSN access control models because it is impossible to define the possibility of denied and permitted access for all situations, especially in WMSNs and WSNs. The A^{2}C model is based on the concept of discretionary overriding of access control by Rissanen *et al.* [19]. The system defines permitted and denied access policies for normal situations and leaves the possibility-with-override for emergency and unusual situations as the default to address the data availability issue. In the A^{2}C model, the behaviour trust model is introduced to monitor the behaviour information as well as to compare with previous and predefined users' behaviour pattern. A prevention and detection mechanism is used in both models to prevent the unauthorised information release and to detect security violations that can occur in the system anytime. The concepts of the A^{2}C model can provide both data availability and data privacy but there is a lack of information for the behaviour trust model.

Unlike A^{2}C, the BTG-AC model uses core RBAC with obligation and BTG concept to make decisions regarding access for emergency and unanticipated situations with details information for each components. The BTG-AC model needs predefined access roles and policies in advance for any situation. The authorisation decision-making process is made within the core RBAC engine based on the inputs of the current section, the requested operation and the target object. The main idea of the Break-The-Glass concept is to allow the users emergency and urgent access to the system when a normal authentication process does not perform or work perfectly. In BTG-AC, BTG action is based on predefined user accounts. The system is managed in a manner that can make data access available in emergency situations with minimum of human interactions.

The BTG approach can be easily applied in the existing architectures and systems. It is very useful for existing systems because it does not involve additional automated technology. It is intended to cover unanticipated and emergency situations and it should not be used as a replacement for a help-desk. BTG-AC can make decisions regarding data access quickly without unreasonable administrative involvements and delays. When an emergency or BTG account is activated in the system, it can alert the security administrator for that event for auditing purposes. This means that the monitoring process is required as an extra checkpoint to detect security violations. The proposed approach is well suited for the emergency decision-making process, but after an emergency in which a BTG account has been used, that account has to be deleted or disabled to prevent a replay attack. Therefore, human interactions are still involved in the system. The advantage of the BTG-AC model is that it can provide data availability service in emergency situations with a certain level of prevention and detection.

3) Access Control Policy: In this subsection, the access control policies defined in both A^{2}C and BTG-AC are presented. Similar access control policies are used from both models to make an effective comparison.

Table III shows how the access control policies are defined in the A^{2}C model for the same medical scenario in section V. In policy 1, a doctor is allowed to read the normal medical record (ob_2) without obligation. In policy 2, the doctor is allowed to read the confidential medical record (ob_1) of a patient but an obligation such as "Write to Audit" will be taken as an action when the decision has been made. Therefore, the management teams can check the audit log to detect security breaches that can occur by the authorised users. This means that the stored data at the ob_2 is not as sensitive as ob_1. The roles and policies for other users such as nurses and other members of staff will be predefined differently. Policy 1 and policy 2 are the same in Table I for BTG-AC.

In policy 3, the nurse is not allowed to access the confidential data (ob_1) unless the associated user overrides the access policy for emergency data access, but some obligations will be activated. Based on policy 3, the users (U* represents the group of nurses) can override access policy. If he or she overrides based on policy 3, his or her behaviour trust value will be lower than normal data access. Access will only granted to that user when his behaviour trust value is great than three. Otherwise, his or her access to the confidential data will be denied. Policy 4 allows the nurse to access the normal medical data (ob_2); however, one obligation action is triggered. Policies 5 and 3 have a similar property. There is a chance for member

Policy	Subject	Role	Operation	Object	Override	Obligations
1	U_1	Doctor	read	ob_2	-	-
2	U_1	Doctor	read	ob_1	-	oblg [Write to Audit]
3	U_*	Nurse	$Override^{(read)}$ (if T $>$ 3)	ob_1	Override	oblg [Notify Manager; Write to Audit; Trigger the alarm]
4	U_2	Nurse	read	ob_2	-	oblg [Write to Audit]
5	U_*	Staff	$Override^{(read)}$ (if T $>$ 3)	ob_2	Override	oblg [Notify Manager; Write to Audit; Trigger the alarm]

TABLE III. EXAMPLE OF DEFINED POLICY FOR THE A^{2}C MODEL

of staff from hospital to access the normal medical record (ob_2) but they have to override access policy. The administrator or manager can easily check the audit log to detect illegitimate use from authorised users and to prevent legitimate use from unauthorised users.

The complete BTG-AC policy can be seen in Table 1 and discussion in section V. The policy definitions for both A^{2}C and BTG-AC have a similar structure. The weakness of the BTG-AC model is that an additional role for a BTG policy is needed for each user to perform BTG operation and an additional account is needed for emergency access. As a constraint, the BTG role needs to be considered in advance and predefined before the system is running in real-time.

4) Decision Outcomes: In both A^{2}C and BTG-AC models, the existing decision outcomes in current access control models such as permitted access and denied access are extended into five different outcomes. The decision outcomes for the BTG-AC model are already discussed in the previous section. For the A^{2}C model, the decision outcomes are extended because of the discretionary overriding process with the user behaviour trust value and the prevention, and detection mechanism. These decision outcomes are explained as follows:

- Permitted Access: A user access request has been permitted.
- Denied Access: A user access request has been denied. The user is not allowed to access the resources.
- Permitted Access with Obligation: A user access request has been permitted but an obligation is executed when data access is given to that user especially for important and confidential information.
- Permitted Access with Overriding and Obligation: A user does not have privilege to access the resources but his or her request will be granted if he or she overrides policy within some constraints. The obligation policies are activated when access is granted to the user.
- Denied Access with Overriding and Obligation: A user access will be denied, if he or she tries to override the policy and does not satisfy some thresholds from that policy. At the same time, the obligations such as write to audit, etc. will be performed.

Based on the above decision outcomes, it is clear that the introduction of different concepts and approached can provide a flexible approach in the access control engine by extending the decision outcomes. Both A^{2}C and BTG-AC models add a finer grained level of control in access control engine for emergency situations.

5) Data Availability and Data Privacy: Both the A^{2}C and BTG-AC models are designed for making access decisions dynamically and efficiently in emergency and unanticipated situations. In the A^{2}C model, the decisions regarding access can be evaluated and adjusted dynamically, based on policies such as authorisation, obligation and overriding. Especially in emergency situations, the user behaviour trust value and the overriding policy are used to adjust access decisions to provide data availability in emergency and unanticipated situations. BTG-AC has similar properties to the A^{2}C model but human interaction is still needed to define for BTG operation; the BTG role also needs to be predefined in advance for emergency situations. Users need extra roles for breaking the glass for unexpected situations and need an additional emergency account to do so for unexpected and unanticipated situations. Another advantage of the BTG-AC model over the A^{2}C model is that a simple user log in process is used as an additional security provisioning to protect the privacy of the patient information.

6) Summary: A comparison of the BTG-AC model with related works are expressed in Table IV based on the evaluation criteria. The centralised access control management is used in BTG-AC, FDAC and CA-RBAC, but for A^{2}C and DFG-AC, the distributed access control management is used. The existing decision outcomes such as permitted access and denied access are extended in both BTG-AC and A^{2}C and these are only two models that address data availability issue and detect security policy violation by using the prevention and detection mechanism.

Access Control Model	Network Architecture	Decision Outcomes	Data Availability	Prevention and Detection Mechanism
BTG-AC	Centralised	5	Yes	Yes
A^{2}C [6]	Distributed	5	Yes	Yes
FDAC [11]	Centralised	2	No	No
CA-RBAC [14]	Centralised	2	Yes	No
DFG-AC [12]	Distributed	2	No	No

TABLE IV. A COMPARISON OF THE BTG-AC MODEL WITH RELATED MODELS

Advantage	Disadvantage
- Administrator can manage policy such as (create a new role, edit an existing role, etc). - It can be used easily in existing systems and architectures. - It provides data availability based on BTG policy for emergency situations. - BTG state can be defined based on time period. - Audit log can be checked by security administrator. - It detects security policy violations from authorised users.	- A security administrator needs to be involved in some processes. - The BTG option or account needs to be disabled and deleted once the account is activated. - A new BTG account is needed after the old account is used. - The storage is costly because of an additional role for BTG.

TABLE V. ADVANTAGES AND DISADVANTAGES OF BTG-AC

C. Advantages and Disadvantages over Current WSN Access Control Models

The highlights for the advantages and disadvantages of BTG-AC over current WSN access control models can be seen in Table V. The BTG-AC model can manage policy such as creating a new role and editing an existing role and it can be used easily in existing systems and architectures. This model can provide data availability in normally defined situations as well as emergency situations; however, in the BTG-AC model the BTG state and account need to be opened and defined in advance for emergency access. The BTG-AC model can provide data availability with certain constraints and limitations. Additionally, the BTG-AC model can detect security violations in the systems by checking the audit record in the prevention and detection mechanism. The main contribution of the BTG-AC model is that data availability and data privacy can be provided in both defined situations and some emergency situations for effective treatment of patients in the real time environment.

Alongside with the advantages, there are some drawbacks in the proposed BTG-AC model. The disadvantages of the BTG-AC model can be seen on Table V. Data availability is provided in BTG-AC, but some limitations apply for data access in emergency situations. A system administrator needs to open an emergency account for users in advance for BTG operation and emergency access. In addition, the BTG or emergency account can be used one time only to prevent replay attacks. The user needs to reopen the emergency account for another attempt. If this is not done, the system administrator needs to open and activate the emergency account for all users. This means that some kinds of administration processes are needed in BTG-AC for emergency situations. The storage might be costly because an additional role is needed for each user to use a BTG account. An alternative way is to use data aggregator as centralised access management to reduce the storage space in actual sensor nodes.

VII. CONCLUSION AND FUTURE WORK

The overall contributions of this paper is the design and development of a lightweight BTG-AC model for medical data in WSNs to address the data availability issue and to detect the security policy violations from both authorised and unauthorised users. The concepts of BTG, prevention and detection mechanism, and obligation provide more flexible access than other current access control models in WSNs. The BTG-AC model has been developed under Ponder2 package. All the modules - access control module and prevention and detection module - have been found to cooperate to make access decisions and record a users' accountability to detect security violations from authorised users. Additionally, the A^2C framework, which has similar properties as BTG-AC, is briefly discussed to make a meaningful comparison and compared with BTG-AC. One possible weakness of BTG-AC is that the human decision is needed to predefine BTG policy for each object. We are considering to redesign the BTG-AC model to overcome that weakness in future work. We plan to develop the BTG-AC model within the actual sensor nodes for medical applications in WSNs. In addition, we will work on the implementation of the authentication service by using Attribute-Based-Encryption.

REFERENCES

[1] G. Zhao and D. W. Chadwick, "On the modeling of bell-lapadula security policies using RBAC," in *Proceedings of the 2008 IEEE 17th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, ser. WETICE '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 257–262. [Online]. Available: http://dx.doi.org/10.1109/WETICE.2008.34

[2] J. Anderson, "Information in a multi-user computer environment," in *Advances in Computers*, 1973.

[3] A. Ferreira, D. Chadwick, P. Farinha, R. Correia, G. Zao, R. Chilro, and L. Antunes, "How to securely break into rbac: The btg-rbac model," in *Proceedings of the 2009 Annual Computer Security Applications Conference*, ser. ACSAC '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 23–31.

[4] A. Ferreira, R. Cruz-Correia, L. Antunes, P. Farinha, E. Oliveira-Palhares, D. W. Chadwick, and A. Costa-Pereira, "How to break access control in a controlled manner," in *Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems*, ser. CBMS '06. Washington, DC, USA: IEEE Computer Society, 2006, pp. 847–854.

[5] K. Twidle, E. Lupu, N. Dulay, and M. Sloman, "Ponder2 - a policy environment for autonomous pervasive systems," in *Proceedings of the 2008 IEEE Workshop on Policies for Distributed Systems and Networks*, ser. POLICY '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 245–246.

[6] H. A. Maw, H. Xiao, and B. Christianson, "An adaptive access control model for medical data in wireless sensor networks," in *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom) (IEEE Healthcom 2013)*, Lisbon, Portugal, Oct. 2013.

[7] H. A. Maw, H. Xiao, B. Christianson, and J. A. Malcolm, "A survey of access control models in wireless sensor networks," *Journal of Sensor and Actuator Networks*, vol. 3, no. 2, pp. 150–180, 2014. [Online]. Available: http://www.mdpi.com/2224-2708/3/2/150

[8] J. Duan, D. Gao, C. H. Foh, and H. Zhang, "Tc-bac: A trust and centrality degree based access control model in wireless sensor networks," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2675–2692, Nov. 2013. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2013.05.005

[9] J. Maerien, S. Michiels, C. Huygens, D. Hughes, and W. Joosen, "Access control in multi-party wireless sensor networks," in *Wireless Sensor Networks*, ser. Lecture Notes in Computer Science, P. Demeester, I. Moerman, and A. Terzis, Eds. Springer Berlin Heidelberg, 2013, vol. 7772, pp. 34–49.

[10] S. Gaurkar and P. K. Ingole, "Access control and intrusion detection for security in wireless sensor network," *Internal Journal of Scientific and Technology Research.*, vol. 16, no. 2, jun 2013.

[11] S. Yu, K. Ren, and W. Lou, "Fdac: Toward fine-grained distributed data access control in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 4, pp. 673–686, Apr. 2011.

[12] S. Ruj, A. Nayak, and I. Stojmenovic, "Distributed fine-grained access control in wireless sensor networks," in *IPDPS*, 2011, pp. 352–362.

[13] J. Hur, "Fine-grained data access control for distributed sensor networks," *Wirel. Netw.*, vol. 17, no. 5, pp. 1235–1249, Jul. 2011. [Online]. Available: http://dx.doi.org/10.1007/s11276-011-0345-8

[14] O. Garcia-Morchon and K. Wehrle, "Modular context-aware access control for medical sensor networks," in *Proceedings of the 15th ACM symposium on Access control models and technologies*, ser. SACMAT '10. New York, NY, USA: ACM, 2010, pp. 129–138.

[15] H. A. Maw, H. Xiao, and B. Christianson, "An adaptive access control model with privileges overriding and behaviour monitoring in wireless sensor networks," in *Proceedings of the 8H ACM Symposium on QoS and Security for Wireless and Mobile Networks*, ser. Q2SWinet '12. New York, NY, USA: ACM, 2012, pp. 81–84.

[16] V. Goyal, A. Sahai, O. Pandey, and B. Waters, "Attribute-based encryption for fine-grained access control for encrypted data," *Wireless Network, IEEE*, 2006.

[17] R. Sandhu, , and P. Samarati, "Authentication, access control and audit," *ACM Computing Surveys (CSUR)*, 1996.

[18] E. Lupu, N. Dulay, M. Sloman, J. Sventek, S. Heeps, S. Strowes, K. Twidle, S.-L. Keoh, and A. Schaeffer-Filho, "Amuse: autonomic management of ubiquitous e-health systems," *Concurr. Comput. : Pract. Exper.*, vol. 20, no. 3, pp. 277–295, Mar. 2008.

[19] E. Rissanen, B. Sadighi, and M. Sergot, "Towards a mechanism for discretionary overriding of access control," *International Association for Cryptographic Research*, 2004.

[20] R. Sandhu and Q. Munawer, "How to do discretionary access control using roles," *RBAC '98 Proceedings of the third ACM workshop on Role-based access control*, 1998.

[21] M. Momani, K. Aboura, and S. Challa, "Rbatmwsn: Recursive bayesian approach to trust management in wireless sensor networks," in *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, Dec 2007, pp. 347–352.

[22] W. Yuan, D. Guan, S. Lee, and Y. Lee, "A dynamic trust model based on naive bayes classifier for ubiquitous environments," in *Proceedings of the Second international conference on High Performance Computing and Communications*, ser. HPCC'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 562–571.

A.6 TBA^2C: Trust-Based Adaptive Access Control Model for Medical Data in Wireless Sensor Networks

[To be submitted in IEEE Journal of Biomedical and Health Informatics]

TBA^2C: Trust-Based Adaptive Access Control Model for Medical Data in Wireless Sensor Networks

Htoo Aung Maw, Hannan Xiao, Bruce Christianson and James A. Malcolm
School of Computer Science
University of Hertfordshire
Hatfield, United Kingdom
Email: (h.maw,h.xiao,b.christianson,j.a.malcolm)@herts.ac.uk

***Abstract*—Wireless Sensor Networks (WSNs) have recently attracted much interest in the research community because of their wide range of applications. One emerging application for WSNs involves their use in healthcare where they are generally termed Wireless Medical Sensor Networks (WMSNs). In the healthcare industry, patients are expected to be treated in reasonable time and any loss in data availability can result in further decline in the patient's condition or can even lead to death. Therefore, the availability of data is more important than security concerns. The overwhelming priority is to take care of the patient, but the privacy and confidentiality of that patient's medical records cannot be neglected. In current healthcare applications, there are many problems concerning security policy violations such as unauthorised denial of use, unauthorised information modification and unauthorised information release of medical data in the real world environment. Current WSN access control models used the traditional Role-Based Access Control (RBAC) or cryptographic methods for data access control but the systems still need to predefine attributes, roles and policies before deployment. It is, however, difficult to determine in advance all the possible needs for access in real world applications because there may be unanticipated situations at any time. This paper proceeds to study possible approaches to address the above issues and to develop a new decentralised access control model to fill the gaps in work done by the WSN research community. To address the conflict between data availability and data privacy, this paper proposes the Trust-based Adaptive Access Control (TBA^2C) model that integrates the concept of trust into the access control engine. A simple user behaviour trust model is developed to calculate the behaviour trust value which measures the trustworthiness of the users and that is used as one of the defined thresholds to override access policy for data availability purpose. The proposed model can also protect data privacy because only a user who satisfies the relevant trust threshold can get restricted access in emergency and unanticipated situations. Moreover, the introduction of trust values in the enforcement of authorisation decisions can detect abnormal data access even from authorised users. Ponder2 is used to develop the TBA^2C model. The proposed TBA^2C model is the first to realise a flexible access control engine and to address the conflict between data availability and data privacy by combining the concepts of discretionary overriding, the user behaviour trust model, and the prevention and detection mechanism.**

I. Introduction

Wireless Sensor Networks (WSNs) have attracted much interest in the research community because of their wide range of applications. An emerging application for WSNs involves their use in healthcare where they are generally termed as Wireless Medical Sensor Networks (WMSNs). In a hospital, outfitting patients with tiny, wearable, wireless vital sign sensors would allow doctors, nurses and other caregivers to monitor continuously the state of their patients. More importantly in an emergency scenario, the same technology would enable medics to care more effectively for large numbers of casualties. Moreover, unlike many sensor network applications, the healthcare application cannot make use of traditional in-network aggregation[1] [13] since it is not generally meaningful to combine data from multiple patients. In such a scenario, centralised data management cannot be effected.

In the healthcare industry, security is the degree of protection against danger, loss, damage and criminal activity. There are many problems concerning unauthorised information release of medical data in the real world environment. Based on the Health Insurance Portability and Accountability Act (HIPAA) [55], unauthorised information release is the second highest (35 percent) cause of large security breaches in the healthcare industry. Another six percent is caused by hacking and IT incidents. There were several high-profile breaches of users' privacy and data confidentiality when the California Health Department reported on incidents involving patient medical records at UCLA medical Centre. It found that more than 100 hospital workers had been accessing the medical records of 1,041 patients. Some hospital workers were passing information of hospitalised celebrities to the tabloid media and in some cases to insurance companies.

According to another report [19], 1,754 separate Parkland Hospital employees viewed the medical record of a famous person whilst staying in Parkland Hospital. It is unknown how many of the hospital staff had a legitimate reason to view that patient's record but it would not be more than a few dozen.

[1]In-network aggregation deals with this distributed processing of data within the network. Data aggregation techniques are tightly coupled with how data is gathered at the sensor nodes.

Wang *et al.* [54] mention that security breaches may be detrimental to patient health or even life threatening. At the same time, there is a need to access all the patient information in order to accurately evaluate patient health and provide better treatment. Normally, healthcare professionals want to meet emergency needs without security concerns; however, security must be addressed and included for a solution to be completed. Aside from the obvious security considerations with sensitive patient data, both data availability and data privacy need to be addressed.

In current healthcare applications [17], there is a lack of security incident responses and reports, and a lack of access control models. Ferreira *et al.* [3] reviewed a decade (2002-2012) of published literature on access control models for the medical industry. There are more than three dozen papers published on access control models for the healthcare industry; however, only a few of the proposed models have been implemented in practice. There are no well-considered threat models for the access control models that reside in both paper and electronic medical record systems for healthcare applications. Wang *et al.* [54] mentioned that, in theory, access control solved the problems of which users can or cannot access medical records. In practice, some large organisations still face problems when policy becomes unmanageable and consequently users circumvent controls.

In the healthcare industry, patients are expected to be treated in reasonable time. Therefore, an access control model should provide real-time access to comprehensive medical records. In emergency situations, a doctor or nurse needs to access data immediately. Any loss in data availability can result in further decline in the patient's condition or can even lead to death. Therefore, the availability of data is more important than security concerns. The overwhelming urgency is to take care of the patient; however, the privacy and confidentiality of that patient's medical records cannot be neglected. Thus, careful consideration in defining flexible policy is required to solve the conflict between data privacy and data availability in this real world application. Additionally, it should also detect unauthorised information release of patient medical records from both authorised and unauthorised users because security breaches can happen at any time.

Security policy violations in multi-user systems were categorised by Anderson [4] into three categories: unauthorised information release, unauthorised information modification and unauthorised denial of use. It is difficult to address the above violations in an access control policy for the healthcare application because an overly "loose" policy might permit access to inappropriate users, but an overly "tight" policy might prevent access from the appropriate users. The aim of this paper is to present new ways to provide a flexible approach to access control engine in WSNs and WMSNs.

To address the above issues, this paper proposes a new framework for access control engines to fill the needs and requirements of WSNs and WMSNs. A TBA^2C model is developed to address the access control related issues such as how to provide a flexible approach in an access control engine for both defined and unanticipated situations, how to detect security violations, and how to address the conflict between data privacy and data availability. To address the conflict between data availability and data privacy, a simple user behaviour trust model is developed to calculate the behaviour trust value which is used as one of the defined thresholds in access policy. The trust model can also protect data privacy because only the user who satisfies the relevant trust threshold, can get a restricted access even in emergency and unanticipated situations. Notwithstanding, the TBA^2C model is easy to adapt with other trust models in WSNs.

The main contribution to the WSN research community that this work makes is the Trust-Based Adaptive Access Control model (TBA^2C) model itself. The introduction of overriding policy based on a user behaviour trust value and contextual information is the main novel element of the proposed TBA^2C model. The novel usage of the discretionary overriding concept with user behaviour trust in adjusting decisions regarding data access for emergency and unanticipated situations is a new concept. The combination of the discretionary overriding concept and the behaviour trust model is a possible solution that helps to address the conflict between data availability and data privacy by using the behaviour trust value as one of the defined thresholds in the access policies. Only the trusted user, who satisfies these thresholds including trust value, can get a restricted access in emergency and unanticipated situations. Additionally, the usage of user behaviour monitoring and the prevention and detection mechanism can detect security policy violations such as unauthorised information release, unnecessary overriding process and abnormal data access from both authorised and unauthorised users. Moreover, the use of a behaviour trust value in an authorisation policy is a novel approach to detect abnormal data access from authorised users.

The remaining structure of this paper is explained as follows. Section II reviews the related works. Section III discusses a user behaviour trust model to apply in the access control engine. Section IV presents a TBA^2C model for WSNs. A threat model for TBA^2C with an example medical scenario can be seen in section V. Section VI discusses the implementation tool and simulation test scenario to evaluate the proposed TBA^2C model. Section VII concludes the paper with suggestions for future work.

II. Related Works

This section gives an overview of the related work laying out the background to this paper. It primarily reviews research in the field of access control models and trust schemes in WSNs.

A. Access Control in WSNs

Most of the access control models in WSNs and WMSNs are based on traditional Role-Based Access Control (RBAC), which has been widely accepted as a policy access control model. Applications based on RBAC have been implemented and widely deployed by commercial companies and education industries. Cryptography-based access control is a new access control model that is designed for the untrusted environment, where lack of global knowledge and control are defining characteristics. Cryptography methods in WSNs should meet the constraints of sensor nodes such as limited power, resources and memory shortage. Therefore, choosing the suitable cryptography method is important in WSNs. Maw *et al.* [34] mentioned that a considerable amount of access control models has been proposed for use in WSNs, though some of them are not yet implemented. In this section, the existing proposed models that are similar to the proposed approach are explained and discussed.

The distributed PRIvacy-preserving aCCESS control (PRICCESS) protocol [18] is proposed to provide privacy preserving distributed access control in WSNs. The PRICCESS model used Access Control List (ACL) to store the access permission of user groups in the network controller. For ACL, roles need to be predefined in advance based on RBAC. Garci-Morchon *et al.* [16] pointed out that RBAC model is not good enough to use in WSNs because in the traditional RBAC model, the roles and policies have to be predefined in advance. Instead Garci-Morchon and Wehrle [16] proposed the Context-Aware Role-Based Access Control model for WMSNs, in which an access control decision will be made based on the modular contextual information such as normal, emergency and critical, to ensure the users' safety. In this model, there is no prevention or detection mechanism and no verification process to check user's data access, when the critical situation occurs.

The Break-the-Glass Access Control (BTG-AC) model is proposed by Maw *et al.* [31] for medical data in WSNs. The main objective of the BTG-AC model is to provide availability of data access in the emergency situation but the users need to be kept in the log and will be audited by both internal and external auditor for being Break-the-Glass to get access to patient's medical records. The major disadvantages of this model is that the human process is involved in BTG action.

Yu *et al.* [57] proposed the Fine-grained Data Access Control (FDAC) model which is based on Attribute-Based Encryption (ABE) [9]. The main idea of their approach is to provide a fine-grained access control over sensor data and is resilient against attacks such as user colluding and node compromising. Their model is based on centralised approach because only a network controller is managed for key management. If the network controller is compromised, there will be no security provisioning in the network. Therefore, a single point of failure can be occurred.

To avoid a single point of failure, Ruj *et al.* [47] proposed an access control scheme based on Multi-authority Attribute Based Encryption. Their objective is to provide fully distributed data access control by using several Distribution Centres (DCs). All the access structures from each DC, which need to satisfy the attributes from sensor nodes, are ANDed together to get a complete access for the single user. There is no detailed explanation of how to combine all the access structures together. Without the combining approach, the user has to store all the access structures in order to access different types of data from the sensor network.

Based on the above discussion, there are a couple of access control models, such as BTG-AC and CA-RBAC which are designed to support availability of data access in emergency cases but there is no prevention, and detection mechanism and authentication service to prevent authorised usage as well as privacy of the data from both internal and external users. In addition, an overly "loose" policy without prevention and detection mechanism might grant permitted access to the inappropriate users. There are several access control models like FDAC and Ruj's model that are designed to provide fine-grained data access in WSNs but there is no consideration of making access decisions effectively based on the users' circumstances. On the other hand, an overly "tight" policy might prevent permitted access from the appropriate users in unanticipated events. Therefore, a new access control model is needed to consider the flexible approach for making access decisions effectively. It is clear that availability to access data at any time and privacy of data by providing a flexible access control policy is vital in WSNs.

TBA^2C has similar structure as BTG-AC but the main difference is that the decisions can be made effectively based on dynamic changes of users' behaviour. It supports a flexible access control policy to provide both data confidentiality and data availability when it is required. The proposed access control model is aimed to achieve flexibility of the access control engine is to override access policy with user behaviour trust value and contextual information, whenever unexpected events occur. The overriding considers a user's behaviour trust value and adapts a certain level of prevention and detection mechanism to provide both availability and privacy. Therefore, the proposed TBA^2C model had a great advantage over current access control models because of introducing of overriding access policy based on user's behaviour trust model, contextual information and prevention and detection mechanism.

B. Trust in WSNs

Trust plays an important role in networks and human life environments. In the context of a network, trust is used to help its components to decide whether another member,

node or device from the same network is being inattentive, uncooperative or compromised. Fernandez-Gago [14] states that trust becomes quite important in self-configurable and autonomous systems such as WSNs and WMSNs. Having different definitions in security related literatures "trust" in this chapter is considered as the trustworthiness of users based on highly dynamic and unpredictable characteristic of their behaviour.

Trust in WSNs can be classified into different categories based on the needs of the application. The classification of trust [49] is explained as follow:

- Direct Trust: Direct trust is the trust that a subject holds of another service provider without any intermediate service provider or entity.
- Indirect Trust: Indirect trust is the trust that a subject holds of one service provider through some other service provider or entity.
- Full Trust: A subject is said to have full trust of a service provider if that subject trusts all the services provided.
- Partial Trust: A subject is said to have partial trust of a service provider, if that subject trusts some of the services provided.
- Recommended Trust: Recommended trust is the trust of one entity of another that is recommended by other entities.
- Authentication Trust: Authentication trust is the trust of an entity of the authenticity based on an identity certificate signed by a certificate authority.
- Communication Trust: Communication trust means that the trust is calculated between the sensor nodes based on their cooperation of routing messages to other nodes in the network [41].
- Data Trust: Data trust is the trust that is based on the actually sensed data of the sensors [39].

Regarding the above categorisation of trust, direct and indirect trust are commonly used in trust calculations of sensor nodes [40], [39] to check whether the nodes are trustworthy or not based on Bayesian network [11] and Naive Bayes classification algorithms [58]. For reputation-based trust calculation [42], [15], trust are used in key management and network management. Authentication trust is mostly used in policy-based trust management systems [49]. The communication and data trust proposed by Momani [41], is used to calculate trust between sensor nodes. sTherefore, trust can be divided in six groups regarding the aspects of requirements in WSNs: trust-based routing management or protocol; trust-based intrusion detection; trust-based key management; trust-based malicious node detection; and group-based and reputation-based trust management for network. Table I shows the taxonomy of trust-based schemes in the published literatures for WSNs.

Trust can also resolve security related routing issues. Several trust management schemes [52], [7], [1], [24], [43] are proposed to detect suspicious transmission and identify malicious nodes for disseminating information in the network. For example, trust-based routing management only allows the trusted sensor nodes to participate in the routing. Direct trust and indirect trust are mostly used to evaluate each node's trustworthiness based on trust metrics (i.e. Quality of Service (QoS) characteristics such as data packets forwarded, control message forwarded, availability based on bacon or Hello message, etc.) and weight factors. One of the trust algorithms for routing management calculates the direct trust based on Geometric Mean [37] of the QoS characteristics. The indirect (second-hand) information may be particularly useful when there is no direct interaction, i.e. when the situation is risky, then the indirect trust plays major role in the formation of trust on any node.

Trust-based intrusion detection schemes such as [5], [6], [7] are used to effectively deal with selfish or malicious nodes and to improve QoS in WSNs. The trust-based intrusion detection schemes considered the effect of both social trust (such as honesty[2]) and QoS trust (such as competence, reliability and task completion capability) to detect malicious nodes.

Trust-based key management schemes [23], [25], [26] based on cryptographic method are proposed to provide a secure communication channel in WSNs. Since sensor nodes collect personal medical data, security and privacy are important services in this kind of networks. It is aimed to securely and efficiently generate and distribute session keys based on biometrics (such as electrocardiogram [28]) or identity-based encryption [2] between the sensor nodes and the base station to secure end-to-end transmission.

The aim of trust-based malicious node detection is to minimise communication and storage overhead, and to improve reliability in WSNs. Direct and indirect trust are mostly used in malicious node detection methods to calculate the trust value of each node based on weighted running average approach [38]. Direct trust method [20] consists of the following steps:

- Behaviour of the node is monitored periodically.
- In each period the numbers of good and bad behaviour of the node are recorded.
- Based on the numbers of good and bad behaviour, trust is calculated periodically.

Indirect trust is calculated based on recommendation (second hand information) obtained from trustful neighbours. Additionally, the communication and data trust are also used to detect malicious node based on Bayesian network.

The group-based trust management scheme for clustered

[2]The honesty trust is the trust that measure through evidences of dishonesty such as false self-reporting and abnormal trust recommendations.

Trust based Schemes in WSNs	
Trust-based Schemes	References
Trust-based routing management or protocol	[52], [7], [1], [24], [43], [56], [44]
Trust-based intrusion detection	[5], [6], [7]
Trust-based key management	[23], [25], [26], [28]
Trust-based malicious node detection	[22], [61], [20], [40]
Group-based trust management	[48], [60]
Reputation-based trust management	[42], [15], [51]

TABLE I: A taxonomy of trust-based schemes in WSNs

WSNs such as [48], [60] is aimed to detect and prevent selfish, faulty and malicious nodes, to minimise the memory overhead, and to reduce the communication overhead by making sensor nodes only communicate with the cluster head. The trust value calculation in cluster head is based on weighted running average, so that the recent trust value can be given more weight in the overall trust calculation.

Distributed Reputation-based Beacon Trust System (DRBTS) [51] is aimed at providing a method by which bacon nodes[3] can monitor each other and provide information so that sensor nodes can choose whom to trust, based on a quorum voting approach [50]. In order to trust a bacon node's information, a sensor must get votes for its trustworthiness from at least half of their common neighbours. Ganeriwal and Srivastava [15] propose a framework where each sensor node maintains reputation metric representing past behaviour of other nodes, which are then used as an inherent aspect in predicting future behaviour. This approach is based on a Bayesian formulation, specifically a beta reputation system [21], for the algorithm steps of reputation representation, updates, integration and trust evolution. Overall, reputation-based trust management are employed in WSNs to deal with malicious and unreliable nodes based on first and second hand information from the neighbours.

Based on the above discussion, most of the trust schemes in WSNs are using weight factors, so that the direct trust or recent trust can be given more weight in the overall trust calculation. Direct trust, indirect trust and trust that based on QoS characteristics are commonly used in trust calculations of sensor nodes to check whether the nodes are trustworthy or not based on Bayesian network, Naive Bayes and geometric mean. Regarding the above facts, there is no existing trust model that evaluates trust based on users' behaviour information. This means that none of the existing trust models can be readily related to the decision-making process in the access control engine. The evaluation of trust for users based on their behaviour information is significant in forming a trustworthy network and is a new research issue in WSNs. Therefore, we propose a user behaviour trust model to use in WSNs and WMSNs in order to measure behaviour trust of the user from the system perspective to enhance access decisions. Unlike existing trust models in WSNs, the proposed model is aimed at calculating the trust value of each user regarding whether the users are trustworthy or untrustworthy, based on highly dynamic characteristics of their behaviour information.

[3]A beacon node assists other sensor nodes to determine their location.

III. A User Behaviour Trust Model

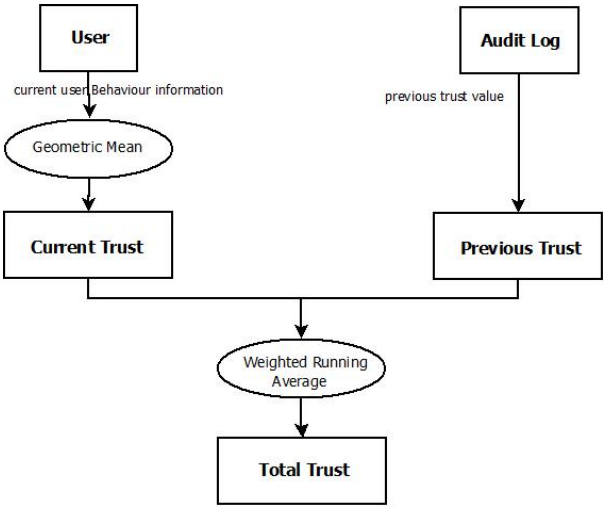


Fig. 1: Overview of the Trust Model

A user behaviour trust model that uses current user behaviour information and previous trust values to calculate user trustworthiness from the system perspective is proposed and introduced in WSNs. The current trust value is the geometric mean [37] of information obtained from the user's current access requests to an object, such as user's role, location and time. The main reason of using the geometric mean is that it compares different attributes - finding a single "figure of merit" for these attributes - when each attribute has different numeric ranges. The concept of using geometric mean to calculate the direct trust based on QoS characteristics of a sensor node for routing management motivates us to reproduce a simple calculation for current trust evaluation based on a user's behaviour information such as the role and the contextual information from the access request. The user's behaviour information can be considered as user's characteristic and calculated based on geometric mean formula. The geometric mean equation can be seen as follow:

$$(\prod_{i=1}^{n} a_i)^{\frac{1}{n}} = \sqrt[n]{a_1 * a_2 * ..... * a_n} \quad (1)$$

For the previous trust value, the total trust value of the user from the previous transaction is used. This means that the total trust value of users does not rely completely on the evaluation of current trust. The traditional weighting approach [38] is used to calculate the total trust value of a user based on the current trust and the previous trust. The weight factor is commonly used in the trust calculation, so that the recent behaviour characteristics can be given more weight in the overall trust calculation. If total behaviour trust value is higher than the defined threshold, the user is trustworthy enough to perform an action on a certain object. When it goes under the defined threshold, the user becomes an untrustworthy person and the system may decline his access to a specific object. An overview of the user behaviour trust model can be seen in Figure 1. There are three sub-modules: current trust, previous trust and total trust.

A. Current Behaviour Trust Value (T^{cur})

A user's behaviour information (such as the role and the contextual information from the access request) is used to calculate the current trust value of the user. The formula for the evaluation of current behaviour trust based on geometric mean is shown below:

$$\mathbf{T}^{cur} = (\prod_{i=1}^{n} a_i)^{\frac{1}{n}} \tag{2}$$

where,
n = Number of Attributes
a = Attribute

Based on the users' behaviour information (such as location, role and time), the above equation is substituted as follow:

$$\mathbf{T}^{cur} = \sqrt[3]{T^{Lo} * T^{Ro} * T^{Ti}} \tag{3}$$

where,
T^{cur} = Current Trust Value
T^{Lo} = Trust Value for Location
T^{Ro} = Trust Value for User's Role
T^{Ti} = Trust Value for Time Range

Equation 3 shows that the current behaviour trust value is evaluated based on three different attributes: location; user's role; and user's time range. Each attribute has a defined value between 1 and 4 because we consider three different conditions in the proposed model. The defined value of each attribute is evaluated differently. Based on the geometric mean, the maximum value of current behaviour trust can be up to 4 and the lowest value can be 1.

In the proposed model, the physical location of a user (location of subject), which department that user is from (department of subject) and where is the targeted data that the user tries to access (department of object) are considered as the evaluation criteria for the location attribute. Table II represents an example data set to evaluate the trust value of location for a user.

Department of Subject	**Department of Object**	**Location of Subject**	$\mathbf{T}^{Lo}$
A	A	A	4
A	A	B	3
A	B	A	2
A	B	B	1

TABLE II: An Evaluation Criteria for Location Attribute

Based on Table II, if the department of the subject, the location of the subject and the department of the object are the same (in this case "A" department), the trust value of location for a user is defined as 4 that is a maximum value. If the user works in department "A" and tries to access data which stores the same department "A" but his actual location is from another department ("B"), his trust value is set as 3. If the object is stored in "B" department but both department of subject and location of subject are from "A" department, the trust value is defined as 2 because the user tries to access data which is stored in the different department. In last case, the trust value of location for a user is the lowest 1 when the location of subject and the department of object are different compared to the department of the subject.

The defined trust value for a user's role is reflected based on their responsibility and duty. For the doctor, the trust value for user's role is set as 4 but for the nurses, it is defined as 2. The trust value can be different for other roles (such as administration staff, laboratory staff, etc.) but we only consider doctors' and nurses' roles. In general, if the current user's time range is within the system defined time frame, the trust value of the time criteria $\mathbf{T}^{Ti}$ is set between 1 to 4. In a medical application, some users work in the daytime and some in the night time. Therefore, the defined trust value for time criteria can change based on users' working schedule or time framework. Example conditions for time criteria can be seen in Table III.

Ti	$\mathbf{T}^{Ti}$
$12 \leq$ Ti < 18	4
$6 \leq$ Ti < 12	3
$18 \leq$ Ti < 24	2
$0 \leq$ Ti < 6	1

TABLE III: An Evaluation Criteria for Time Attribute

Based on the above discussion, the evaluation for each criterion is considered separately based on the requirements of the application for the current behaviour trust. The proposed current trust module can easily be extended with additional attributes for extra critera for evaluation of trust.

B. Previous Trust Value (T^{pre})

In the proposed model, the previous trust value is used as one of the supporting factors for total trust evaluation when

the user requests at the next attempt. The user trust values from the previous transactions are used as the previous trust value of the users. T^{pre} is equivalent to the total trust value of users from the previous transactions.

C. Total Trust Value (T^{total})

The total behaviour trust value checks whether the user is trustworthy or untrustworthy to perform some actions based on his or her current and previous behaviour trust values. The total trust value is a function of current and previous trust values. The proposed model also uses the traditional weighting approach as in [38], [2] to combine current and previous trust to form the total trust per relation in the system, as shown in equation 4.

$$\mathbf{T}^{total}\mathbf{(n)} = (\ \alpha\ *\ \mathbf{T}^{cur}\mathbf{(n)}) + (\ \beta *\ \mathbf{T}^{pre}\mathbf{(n)}) \quad (4)$$

where,
T^{total}(n) = Total Trust Value of the nth Transaction
$T^{cur}(n)$ = Current Trust Value of the nth Transaction
T^{pre}(n) = Previous Trust Value of the nth Transaction
α = Constant Weighting Factor ($0 \leq \alpha \leq 1$) to the current trust
β = Constant Weighting Factor (1 - α) to the previous trust

α is a weighting given to the current trust and β to the previous trust where $\alpha + \beta = 1$ and $0 \leq \alpha, \beta \leq 1$. Weights can be assigned using different approaches. Depending on the application, sometimes the current trust may be given more weight and the previous trust may be given less weight i.e. $\alpha > \beta$, and vice-versa. Additionally, the traditional weighting approach is commonly used in the overall trust calculation in WSNs regarding direct and indirect trust. If there is no previous behaviour trust, the current behaviour trust value is used as the total behaviour trust value. Based on the evaluation of the total behaviour trust value of a user, the levels of trustworthiness can be expressed as follows:

- A user is trustworthy if $T^{total} \geq T^{threshold}$
- A user is untrustworthy if $T^{total} < T^{threshold}$

Currently, a simple method is used to differentiate whether a user is trustworthy or untrustworthy based on the total trust. If the total trust value of the user is higher than the defined threshold ($T^{threshold}$) which is 2.5 based on the arithmetic mean[4] [12] of previous trust and current trust, he is a trustworthy person, but when the total trust value is under the defined threshold, that person is deemed an untrustworthy person. After the evaluation of total behaviour trust value for that user, that value will be forwarded to the access control module for decisions regarding data access. Using behaviour trust values can enhance the decision-making process at the access control module. The behaviour trust module assists the decision-making process regarding whether the user is trustworthy or un-trustworthy to perform some actions in the specific targeted objects.

[4]The arithmetic mean is used as a good measure of central tendency, compared to $\alpha = \beta = 0.5$.

D. Data Flow Chart

The data flow chart for the behaviour trust module can be seen in Figure 2. When the user behaviour trust module receives user requested information (U^{info}), the current behaviour trust module evaluates the current user's information. After that, the system checks whether the user has previous interaction by checking his previous behaviour trust value. If it is the first attempt for that user, where T^{pre}(n) is inapplicable, the current behaviour trust value is used as the total behaviour trust value.

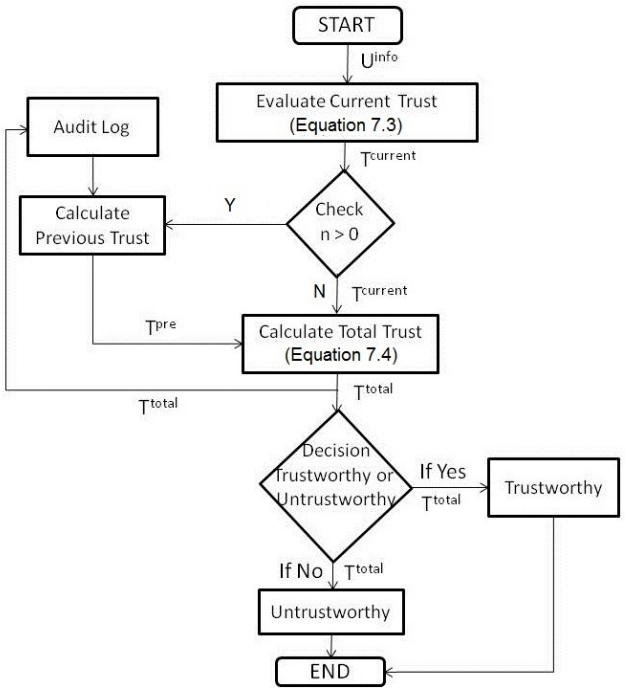


Fig. 2: Flow Chart of the Trust Model

If T^{pre}(n) is greater than zero, both current and previous trust values are forwarded to the main trust engine to calculate the total behaviour trust based on equation 4. The total trust value will be forwarded to the access control module for decisions regarding data access. All the users' information and trust value are kept as an audit log.

E. Evaluation of Trust Algorithm

The user behaviour trust algorithm is evaluated based on numerical analysis in MATLAB [30] to check and show how the total trust value of users vary given different users' behaviour information or attributes. The trust algorithm is calculated with random variables[5] that represent the trust value of three different attributes such as trust value for location, users' role and time range. Random variables are useful when solving and complex problems related to probability (whether the users can be trusted or not trusted).

[5]A random variable is a process that assigns values of an attribute to different cases.

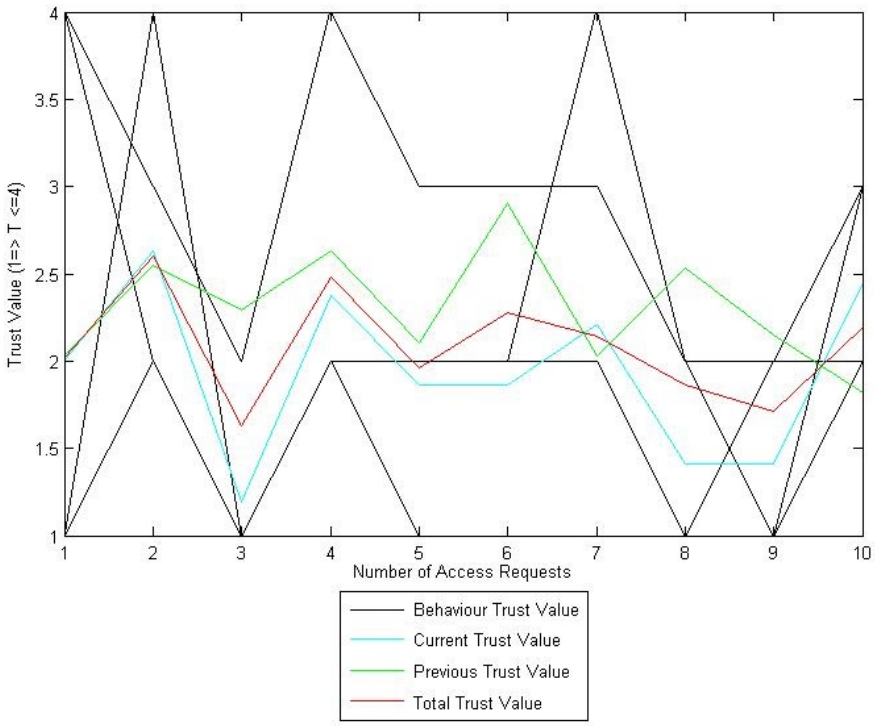


Fig. 3: Behaviour Trust Evaluation

The trust algorithm can be seen as follows:

Calculate Total Trust (T^{total}, T^{cur}, T^{pre}, T^{Lo}, T^{Ro}, T^{Ti}, α, β)
U^{info} = Current User Information
T^{total} = Total Trust Value
T^{pre} = Previous Trust Value
T^{cur} = Current Trust Value
T^{Lo} = Trust Value for Location
T^{Ro} = Trust Value for User's Role
T^{Ti} = Trust Value for Time Range
α and β = Constant Weighting Factor ($0 \leq \alpha, \beta \leq 1$)
For T^{Lo},
T^{Lo_u}= randi(4,1,10);
For T^{Ro},
T^{Ro}= randi(4,1,10);
For T^{Ti},
T^{Ti}= randi(4,1,10);
For Current Trust (T^{cur}),
$T^{cur}(n) = \sqrt[3]{T^{Lo} * T^{Ro} * T^{Ti}}$
For Total Trust (T^{total}),
if $T^{pre}(n)$ = NA,
$T^{cur}(n) = T^{total}$ (n)
Return $T^{total}(n)$;
else $T^{pre}(n) = T^{total}(n-1)$;
$T^{total}(n) = (\alpha * T^{cur}(n)) + (\beta * T^{pre}(n))$
Return $T^{total}(n)$;

Figure 3 shows the numerical analysis of trust algorithm based on users' behaviour pattern in MATLAB. The green line presents the previous trust value of the user and the red line represents the total trust value of the users. The blue line represents the current behaviour trust of the user; the black lines represent the trust value of three different attributes such as location; user's role; and user's time range. These attributes were simulated by using the "randi" [30] function based on uniformly distributed pseudo-random integers to generate the random integers. This function generates different variables that are used as the defined trust value for location of user, value for location of targeted object, value for user's role and value for time range, for the current trust evaluation. "randi(4,1,10)" represents the numerical number between 4 to 1 for the transactions (10). Therefore, it shows that the current trust value of a user varies based on the dynamic changes of his or her behaviour information. Overall, it shows that the trust value of users can be evaluated and calculated based on highly dynamic characteristics of their behaviour information. Additionally, Figure 3 demonstrates that the total trust value of a user does not only rely on the current trust value that evaluate based on the users' behaviour information from recent transaction but also depends on the previous trust values.

F. Summary

This section discussed a simple user behaviour trust model with figures and diagrams. The proposed model is developed and designed based on the geometric mean and weight running average to calculate the trust value of the user. The results obtained from the evaluation of trust algorithms based on numerical simulation in MATLAB show that the trust value of the users can vary based on the current users' behaviour information and the previous trust value. The proposed model is developed to cooperate with access control engines and to be used as one of the policy evaluation criteria for making access decisions effectively and dynamically. The proposed model is designed based on the user behaviour information (such as location, role and time) that can be easily obtained from any data access request. This means that, there is no essential requirement regarding the behaviour information or attributes and it can be easily adapted in current access control engines. Additionally, the introducing of trust model in access control engines can help to address the conflict between data privacy and data availability because only the trusted users can get the restricted access in emergency and unanticipated situations.

IV. TBA^2C: Trust-Based Adaptive Access Control Model

Trust-Based Adaptive Access Control (TBA^2C) is an extended version of the adaptive access control model that proposed by Maw et al. [32], [33] by introducing a user behaviour trust model from the previous section in the access control engine. TBA^2C is aimed at protecting the privacy of the users' information and the privacy of the patients' information allowing only trusted users to have a restricted access in emergency and unanticipated situations. The TBA^2C model is incorporated the concepts of the possibility-with-override [45] into WSNs for hard-to-define and unanticipated situations regarding data availability purpose. Possibility-with-override means users may be able to override the denial of access when unanticipated situations occur. It is combined with the user behaviour trust model to enforce access decisions effectively and efficiently at the access control engine. The user behaviour trust model is employed to evaluate the total behaviour trust value of the users based on their role, department, time, etc. In addition, the trust value is used as an extra condition in the authorisation policy to detect abnormal data access from authorised users. Therefore, TBA^2C is an emerging concept that builds on the concepts of the user behaviour trust model, the prevention and detection mechanism, and the possibility-with-override concept to provide a flexible policy that is not too permissive nor too strict in the access control engine and to adjust the access decisions effectively based on the user behaviour trust values.

There are three main modules in TBA^2C namely: Policy Enforcement Point (PEP), Policy Decision Point (PDP) and user's behaviour trust module. The overview of TBA^2C can be seen on Figure 4. A brief discussion of PEP, PDP and user behaviour trust module are explained next.

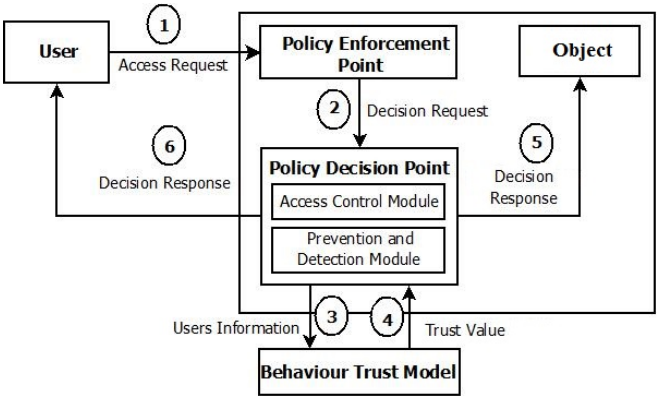


Fig. 4: Overview of TBA^2C Model

A. Policy Enforcement Point (PEP)

PEP provides an authentication service between users and sensor nodes. Whenever PEP receives an access request, it authenticates the user by checking the user information such as user identity and cryptographic key before it forwards the decision request to the PDP. The assumption is made that Attribute-Based Encryption (ABE) [9] based authentication service and key distribution are already provided in the PEP of the proposed model.

B. Policy Decision Point (PDP)

PDP is a main module in the proposed model inside which the access control module and a prevention and detection module are implemented, and makes access decisions based on the authorisation policy, the obligation policy and the overriding policy in Ponder2. The PDP uses information such as users' role, action and context along with these policies for the decision-making process. After the access control module has made decisions regarding data access, PDP sends back a response message to the user and forwards the decision internally to the targeted object.

1) Access Control Module: The access control module is the main module in the proposed TBA^2C model. All the defined access policies such as authorisation, obligation and overriding are integrated with that module. An effective access decision can be made in any circumstances based on the defined access policies and user behaviour trust value.

- Authorisation Policy
  An authorisation policy defines whether a subject is authorised to execute an action on a targeted object. In the authorisation policy, subject, target, condition and action define an access role. Subject means a user, who is trying to access the targeted object. Whenever

the access control module receives a decision request, it will check conditions and make decisions based on the authorisation policies. An example of authorisation policy is shown below:

Def: Permit-Policy
subject nurse
action read
target ob_2
condition department = Cancer
and time is between 9am to 17pm
if trust value is < 2.5
call obligation policy

The above permit-policy adds an extra condition (trust criterion) to detect abnormal data access from authorised users. It defines the nurse from the "Cancer" department has the right to access the medical record of patient from the same department (ob_2). Unlike the previous models, the trustworthiness value of the user is checked as additional condition in the authorisation policy. The nurse still has an data access even if his trust value is lower than defined value but the system assumes an abnormal data access and performs a course of action by activating the obligation policy.

- Obligation policy
  An obligating policy defines the actions to be performed if certain conditions are met. One of the objectives of using the obligation policy is to provide finer-level access control than mere permitted and denied decisions. After the access decision is made based on authorisation and overriding policies, some obligation policies are activated when the access is given to the user.

Def: Obligation-Policy
Target Em_log
if policy type is override
do write.audit $<$ subject, Time, Target, Behaviour Trust Value, Department, Decision Outcome $>$
and Trigger-alarm
and Notification Message

Based on the above policy, if there is an overriding process, the obligation policy becomes active and keeps the user information as an audit log and some actions such as triggering an alarm and sending notification message to administrator are performed.

- Overriding Policy
  An overriding policy is introduced to provide flexible access in TBA^2C. The overriding policy uses the behaviour trust value and the contextual information to make decisions regarding access in unexpected and emergency situations. The overriding policy checks one or more conditions for access decisions and makes the policy evaluation based on users' behaviour trust value to adjust decisions for unanticipated situations.

Def: Overriding-Policy
subject nurse
action read
target ob_1
condition trust value is ≥ 2.5
and department = Heart
and time is between 9am to 17pm
call Obligation-Policy

Regarding the above policy, a nurse from "Heart" department may access the medical record of a patient from "Cancer" department (ob_1) but he needs to meet conditions such as trust, department and time to override the denied access. An important factor is that the user behaviour trust value has to be equal or higher than the defined value which is 2.5 to override it. Alongside the authorisation decision, the obligation policy will be activated whether the access has been granted or denied.

2) Prevention and Detection Module: The main idea of introducing a prevention and detection mechanism [10], [8], [46] is to protect the privacy and confidentiality of data by storing users' information, actions, etc. as an audit log for the purpose of detecting security violations. For an audit log to be usable, it should:

- Be available through a usable interface for the auditors or the administrators.
- Contain sufficiently detailed information to get a picture of what has happened.

Regarding the above facts, the audit log is to record the event and specify 1) when it occurred, 2) the user information associated with that event and 3) the results of the decision-making process. An audit log can assist in detecting security violations and flaws in the system by detecting any suspicious access from users. In the audit log format, the subject is a user who tries to access a medical record from the targeted object with an authorisation decision. In the audit log, the contextual information such as time and department are also recorded. The format of the audit record is shown as follows:

Auditlog := [Subject + Time + Target + Department + Decision Outcomes]

There are two different audit logs in the proposed model. These are:

- Access Log - every time a medical record is opened an entry is created in the access log containing information about the users, the patient and the document being accessed.
- Emergency Log - an entry is created in this log whenever a restricted access is permitted or denied using the overriding process.

These two logs are stored as Comma Separated Value (CSV) extension, so it can be easily checked and monitored by system administrators. Therefore, the prevention and detection module is used in the proposed model to keep a record of all the users' access information as an audit log for detecting security policy violations.

C. A User Behaviour Trust Module

A user behaviour trust model from the previous chapter is used in the TBA^2C model. This module uses current user information and previous trust values to calculate the user trustworthiness value from the system perspective. The current trust value is obtained from the user's current access request to an object, such as user's role, department, time and targeted objects. The total trust value of the user is stored in a log as the previous trust value for the user's next attempt. The trust value is not only used in the overriding process but also in the normal authorisation process to detect abnormal data access from authorised users.

D. Outcomes of the Decision-Making Process

In the proposed TBA^2C model, the decision-making processes regarding data access are based on the authorisation, obligation and overriding policies. There are five possible decision outcomes based on existing policies. These are discussed as follows.

- Permitted Access: A user access request has been granted, if he or she has the right privileges to access data at the sensor nodes. For example: A nurse has the right to access medical records of patients from the same department.
- Denied Access: A user access request has been denied. The user is not allowed to access the resources because he does not have the right to access data. For example: A nurse does not have the right to access medical records of patients from other departments.
- Permitted Access with Obligation - A user access request has been granted but the obligation policy is activated automatically to take some actions when data access is given to that user especially for important and confidential information.
- Denied Access with Obligation - A user does not have access privilege to the resources and his or her restricted access has been denied. Additionally, the obligation policy is activated to take an action after the authorisation decision is made.
- Permitted Access with Overriding and Obligation - A user does not have access privilege to the resources but the restricted access will be granted if he or she overrides the access policy within some constraints, such as contextual information. Additionally, the obligation policy is activated to detect unnecessary overriding processes by authorised users when the overriding policy is used for decision evaluation.

V. Threat Model

The attacker-centric based threat model [36] is respected and commonly used. Defence strategy is of course, improved if there is a reasonable understanding of how attackers think. By thinking like attackers and being aware of their likely tactics, the system can be more effective when applying countermeasures[6]. Several threats that can be faced in the applications can be categorised based on the goals of the attacks. Knowledge of these threats can help to organise a security strategy and might be able to help plan responses to these threats. In this section, the threat model is categorised based on STRIDE [35]. We analysed the STRIDE model in the medical scenario as follows:

- **Spoofing**: Spoofing is attempting to gain access to a system by using a false identity. This can be accomplished using stolen user credentials or false information. After the attacker successfully gains access as a legitimate user, elevation of privileges can begin. Example: A nurse pretends to be a doctor.
- **Tampering**: Tampering is the unauthorised modification of data but we did not address it explicitly in this dissertation. Same considerations apply to write as to read.
  Example: A nurse or doctor edits the medical record of a patient illegitimately.
- **Repudiation**: Repudiation is the ability of users to deny that they performed specific actions. Without adequate auditing, repudiation attacks are difficult to prove. The issue of repudiation is concerned with a user denying that he performed an action. The defence mechanism is needed in place to ensure that all user activity can be tracked and recorded. Lack of auditing and logging of changes made to data threatens the ability to identify when changes were made and who made those changes. Example: A nurse denies that he has edited the medical record.
- **Information disclosure**: Information disclosure is the unwanted exposure of private data. Sensitive data need to be stored securely to prevent a malicious user from gaining access to and reading the data. The disclosure of confidential data can occur when sensitive data can be viewed by unauthorised users. Only authenticated and authorised users should be able to access the data that is specific to them. Access to data should be restricted to users.
  Example: Other staff members from the hospital try to read the medical record.
- **Denial of Service**: Denial of service is the process of making system resources unavailable.
  Example: A common application layer DoS attack will send multiple simultaneous requests for data access. These requests will most likely put the access control under DoS condition and the user will likely be unable to access the medical record.
- **Elevation of privileges**: Elevation of privilege occurs when a user with limited privileges assumes the identity of a privileged user to gain access to a data resource.
  Example: A nurse tries to access restricted data by using the fault identity.

[6]A countermeasure is an action or technique that can reduce a threat and an attack by eliminating or preventing it.

Threat	Countermeasure
Spoofing	Strong Authentication (Attribute Based Encryption (ABE))
Tampering	Strong Authorisation (ABE and Access Control)
Repudiation	Audit Trials (Audit Record or Log)
Information Disclosure	ABE and Access Control
Denial of Service	Access Control
Elevation of Privilege	Access Control

TABLE IV: Possible Threats and Countermeasures

Based on the above discussion, these threats and attacks are trying to violate the security services such as confidentiality, integrity, authenticity, repudiation, etc. These threats and attacks should be protected by using security mechanisms or countermeasures. A countermeasure is a safeguard that addresses a threat and mitigates risk. Table IV lists the security threats that can violate the security services and the possible countermeasures to defend against them in the proposed TBA^2C model.

VI. Implementation and Evaluation of TBA^2C

In this section, we explain how the proposed TBA^2C model is implemented in Java based Ponder2 policy language [53] and evaluated with a medical scenario.

A. Implementation Tools and Environments

There are a variety of development tools for WSNs available in the current WSN research community. Two policy languages, Ponder2 and WSN Authorisation Specification Language (WASL) [29], are designed specifically for resource and memory limited devices like sensor nodes. Ponder2 is a popular policy language to use in Body Sensor Networks (BSNs) and much published literature on WSNs is based on Ponder2. It comprises a self-contained, stand-alone, general-purpose object management system with message passing between objects, incorporates an awareness of events and policies, and implements a policy execution framework.

Ponder2 has a high-level configuration and control language called PonderTalk and user-extensible managed objects that are programmed in Java. Ponder2 is implemented as Self-Managed Cell (SMC) [27], which is a set of hardware and software components forming an administrative domain. This means that Ponder2 is capable of self management. Everything in Ponder2 is a managed object loaded dynamically into the SMC from a library, thereby producing the factory managed object (Java class). The proposed model is implemented in the Ponder2 policy language, which is suitable to use in small devices such as sensor node.

B. Simulation Test Scenario

A medical application is developed to show how the proposed model is fit and how the policy evaluation is done for overriding access based on user behaviour trust value and other information. In WMSNs, each patient has his or her own Body Sensor Network (BSN) that consists of several sensors. Sensor nodes implanted in the patient's body continuously monitor glucose level, oxygen, etc. They transmit collected data to a local wireless PDA (data aggregator) or store it locally. The assumption is made that sensed data are stored in the data aggregator, as the medical record with other personal information in BSN.

Users such as doctors and nurses try to access medical records of patients via mobile, personal digital assistant or personal computer. For example, sensors can interact with each other via IEEE 802.15.4 wireless links and interactions with other mobile phones and personal digital assistants from users via Wi-Fi or Bluetooth. Each BSN manages its own policies relating to what kind of actions such as read, write, etc can be performed but for simplicity only read operation is discussed throughout this paper. The department that where the doctors or nurses are from, is used when the users try to interact with other BSNs or request to join a patient's BSN for data access. Regarding users' access privileges, data access to a patient's information and medical record will be different. Therefore, access control policies are different based on the users' responsibility, role and department. Figure 5 expresses the overview diagram of how to apply the TBA^2C model in healthcare applications for BSNs and WMSNs. Based on Figure 5, the step-by-step process of user access to the targeted object is explained as follows:

1) A user sends an access request to the targeted object in the system.
2) PEP authenticates the user and forwards users' attributes to a user behaviour trust module. Simultaneously it sends a decision request to PDP for decisions regarding data access.
3) The user behaviour trust module calculates the trust value of the user based on current trust and previous trust. Thereafter, it sends the behaviour trust value to PDP. We assume that the behaviour trust module is deployed in another sensor node that is centrally located to calculate the trustworthiness value of the users.
4) PDP calls the access control engine and passes through the details (such as the requested operation, the targeted object, the contextual information and the behaviour trust value) to make decisions regarding data access.
5) The access control engine returns permitted access or permitted access with obligation or permitted access with overriding and obligation; (or denied access or denied access with overriding and obligation, in which case a denied message is sent from PDP to the user and the request terminates here).
6) PDP forwards the decision response to the targeted

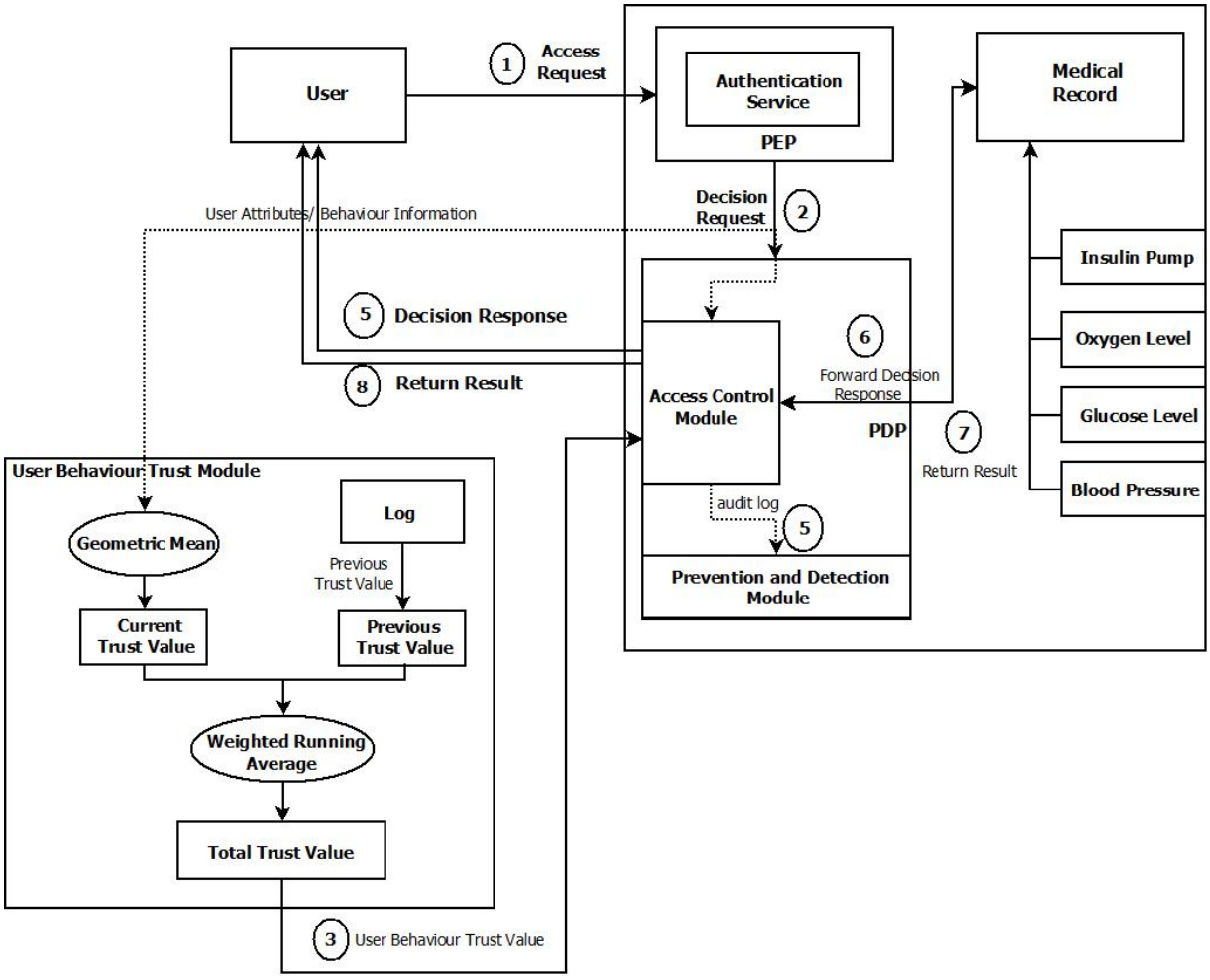


Fig. 5: Overview of TBA^2C with Medical Application in Body Sensor Network

object.

7) The targeted object returns the results.
8) PDP returns the results to the user.

The following policies in Table V are identified and developed to evaluate the proposed model. In Table V, "ob_1" represents the medical record of a patient from "Heart" department and "ob_2" is the medical of the patient from "Cancer" department. "$Oblg_1$" performs a course of action (Sending Notification Message) but for "$Oblg_2$", courses of actions (Sending Notification Message and Triggering Alarm) are performed. "T" represents the trust value of a user. In policy 1, the doctors from "Heart" department have the right to access the medical record of patient (ob_1), which stores collected data from implanted sensors and personal information, from the same department ("Heart"). Policy 2 allows the doctors to access the medical record of the patient (ob_2) from "Cancer" department. Policy 1 and 2 for the doctors are needed regarding data access to the medical records of patients from both "Cancer and Heart" departments. The policies for nurses are slightly different. In policy 3, the nurses from "Heart" departments can access the medical record of a patient (ob_1) who is in their department. Unlike doctors, the nurses can only access the medical record of the patient from the same department. Policy 3 and 4 are different. Policy 4 is for the nurses who work in "Cancer" department to access their patients' medical records.

In policy 5, 6, 7 and 8, an additional condition (trust criterion) is added in policy 1 to 4 to detect abnormal data access from authorised users. Simultaneously, the obligation policy is activated when the user trust value is lower than 2.5 but the users can still access the medical record. In policy 9, the nurse from "Heart" department is not allowed to access the medical data (ob_2) of patient from another department (Cancer) unless the nurse overrides the access policy for emergency data access. If his behaviour trust value is higher than or equal to 2.5, the nurse's overriding will be successful and the restricted access will be granted to him. Otherwise, his restricted access will be denied. In either case, the obligation policy will be activated to take a course of action. Policy 10 is for the nurse from "Cancer" department

Policy	Role	Department	Time	Condition	Operation	Oblg	Object
1	Doctor	Heart	Any	N.A.	read	N.A.	ob_1
2	Doctor	Heart	Any	N.A.	read	N.A.	ob_2
3	Nurse	Heart	Any	N.A.	read	N.A.	ob_1
4	Nurse	Cancer	Any	N.A.	read	N.A.	ob_2
5	Doctor	Heart	Any	(if T $<$ 2.5)	read	$Oblg_1$	ob_1
6	Doctor	Heart	Any	(if T $<$ 2.5)	read	$Oblg_2$	ob_2
7	Nurse	Heart	Any	(if T $<$ 2.5)	read	$Oblg_1$	ob_1
8	Nurse	Cancer	Any	(if T $<$ 2.5)	read	$Oblg_1$	ob_2
9	Nurse	Heart	9am $<$ and $<$ 17pm	(if T $\geq$ 2.5)	override^{read}	$Oblg_2$	ob_2
10	Nurse	Cancer	9am $<$ and $<$ 17pm	(if T $\geq$ 2.5)	override^{read}	$Oblg_2$	ob_1
11	Admin	Audit	Any	N.A.	read	N.A.	Ac_{log}
12	Admin	Audit	Any	N.A.	read	N.A.	Em_{log}

TABLE V: Example of Defined Policy

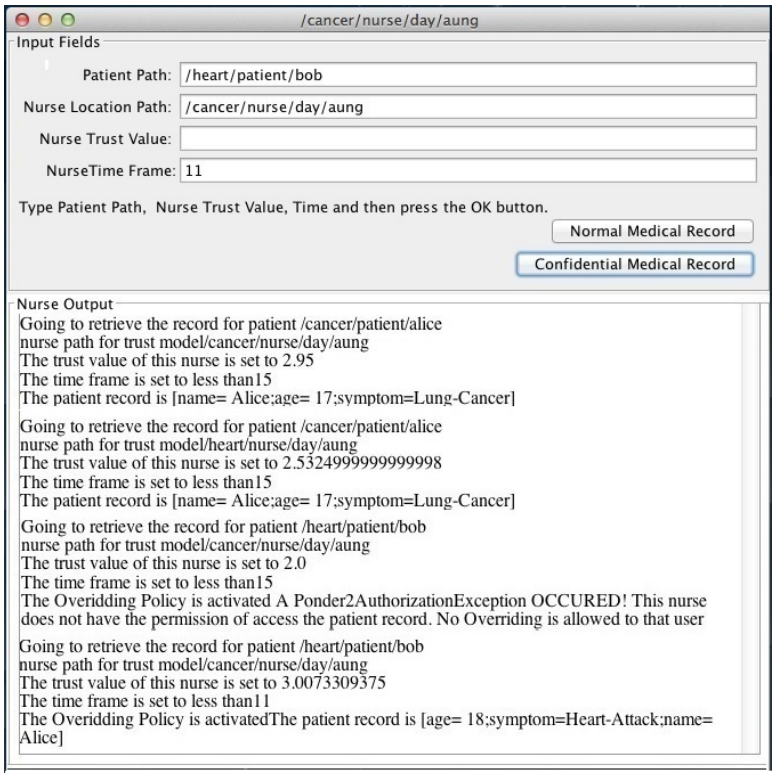


Fig. 6: User Interface and Decision Outcomes of A Nurse

for the overriding process. The administrator from "Audit" department can easily check both access and emergency log to detect security policy violations and abnormal data access regarding policy 11 and 12.

To evaluate and address the conflict between availability and privacy, the above medical scenario is considered because it is a very security oriented application in the real world environments. The idea of developing a framework for the medical scenario is to identify any weaknesses and security flaws of the proposed model. Figure 5 expresses the overview diagram of how to apply TBA^2C model in medical application for BSNs and WMSNs. We developed the medical application to show how the proposed model is fitted and how the policy evaluation is done for overriding access based on user's behaviour trust value and contextual information.

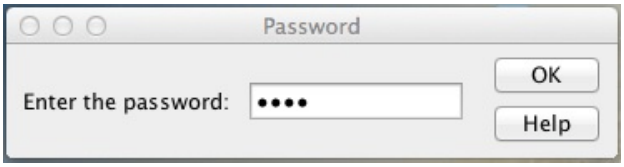


Fig. 7: Authentication Process for Overriding Process

C. Experimental Results and Discussion

Figure 6 shows the interface and decision outcomes of a nurse "Aung", who works as a day nurse in "Cancer" department, as observed from his path (/cancer/nurse/day/aung). Additionally, the location path for the nurse is used as the current location of the users to show that the trust value of the user can be varied based on the location and time range.

In the first case, the nurse from "Cancer" department tried to access the medical data of a patient (ob_2) from his department within time range. His access was approved and his trust value was calculated and recorded (2.95) because he satisfied a normal authorisation policy. In the second case, he tried to access the same data (ob_2) but his physical location is different from where he works and the time range. The total trust value of the user is slightly decreased (2.53) from the previous case but he can still access the data because of the normal authorisation policy.

In the third case, the nurse tried to access the medical record of a patient (ob_1) from another department (Heart) but he needed to override the policy to access the data. For the overriding process, his trust value needs to be higher than 2.5, which is the defined value in the system. Regardless of these outcomes, the obligations such as the triggering of an alarm and sending of a notifying message will be activated and performed. If his trust value is not high enough, the system message will appear in the interfaces as "The nurse does not have the permission to access the medical record. No overriding access is allowed to that user". In this case, his access request is denied but the courses of actions are still performed regarding auditing purpose.

In the final case, the user satisfies the defined thresholds from the overriding policy but here is an additional phase to provide further security services in the proposed model. This means that a user needs to re-authenticate to gain access to confidential medical data. The authentication interface and the confidential medical record interface can be seen in Figures 8 and 7. Overall, his access has been granted because of his behaviour trust value and contextual information as well as the authentication phase in the final case. Figure 6 not only shows the interface of the nurse but also explains how the access decisions are made based on authorisation, obligation and overriding policies with the total behaviour trust value of the users.

VII. Conclusion

This paper has designed and developed a dynamic trust-based adaptive access control model to enhance the decision making processes in WSNs and WMSNs. The main contribution to the WSN research community that this work makes is the Trust-Based Adaptive Access Control model (TBA^2C) model itself. The introduction of overriding policy based on a user behaviour trust value and contextual information is the main novel element of the proposed TBA^2C model. The novel usage of the discretionary overriding concept with user behaviour trust in adjusting decisions regarding data access for emergency and unanticipated situations is a new concept. The combination of the discretionary overriding concept and the behaviour trust model is a possible solution that helps to address the conflict between data availability and data privacy by using the behaviour trust value as one of the defined thresholds in the access policies. Only the trusted user, who satisfies these thresholds including trust value, can get a restricted access in emergency and unanticipated situations. In future, ABE based encryption is considered to be applied in TBA^2C for user's authentication process. Additionally, the ABE approach will use to encrypt the collected and sensed data at sensor nodes to provide data confidentiality. Even the TBA^2C model is capable of working with other trust models in WSNs, the predicted user's behaviour trust value is considered as another possible factor to extend the proposed user behaviour trust model. In future, Naive Bayes classification algorithm [59], [58] is considered to apply in the user behaviour trust model for the predicted behaviour trust. In future, we plan to develop the proposed TBA^2C model within the actual sensor nodes for medical applications in WSNs. Overall, the proposed TBA^2C model is easy to adapt with other concepts to provide further security services in WSNs.

References

[1] Efthimia Aivaloglou and Stefanos Gritzalis. Hybrid trust and reputation management for sensor networks. *Wirel. Netw.*, 16(5):1493–1510, July 2010.

[2] Abdullah Al-mahmud and Matei Ciobanu Morogan. Article: Identity-based authentication and access control in wireless sensor networks. *International Journal of Computer Applications*, 41(13):18–24, March 2012. Published by Foundation of Computer Science, New York, USA.

[3] Ferreira Ana, Ricardo Cruz-correia, Antunes Lus. B, and Chadwick A. Access control: how can it improve patients' healthcare. Technical report, Student Health Technology Information, University of Kent, 2007.

[4] J. Anderson. Information in a multi-user computer environment. In *Advances in Computers*, 1973.

[5] Idris M. Atakli, Hongbing Hu, Yu Chen, Wei-Shinn Ku, and Zhou Su. Malicious node detection in wireless sensor networks using weighted trust evaluation. In Hassan Rajaei, Gabriel A. Wainer, and Michael J. Chinni, editors, *SpringSim*, pages 836–843. SCS/ACM, 2008.

[6] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho. Trust-based intrusion detection in wireless sensor networks. In *Communications (ICC), 2011 IEEE International Conference on*, pages 1–6, June 2011.

[7] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *Network and Service Management, IEEE Transactions on*, 9(2):169–183, June 2012.

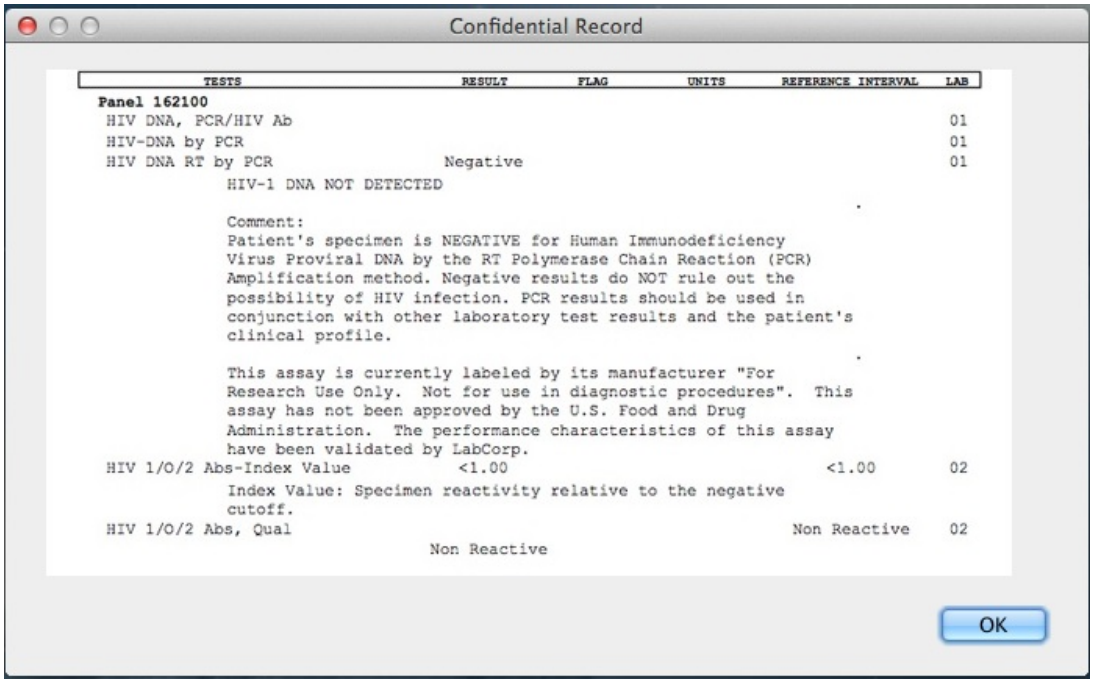


Fig. 8: A Confidential Medical Record

[8] Elisa Bertino and Gabriel Ghinita. Towards mechanisms for detection and prevention of data exfiltration by insiders: Keynote talk paper. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, pages 10–19, New York, NY, USA, 2011. ACM.

[9] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, SP '07, pages 321–334, Washington, DC, USA, 2007. IEEE Computer Society.

[10] Jeremiah Blocki, Nicolas Christin, Anupam Datta, and Arunesh Sinha. Audit mechanisms for privacy protection in healthcare environments. In *Proceedings of the 2Nd USENIX Conference on Health Security and Privacy*, HealthSec'11, pages 10–10, Berkeley, CA, USA, 2011. USENIX Association.

[11] Kian Ming Adam Chai, Hai Leong Chieu, and Hwee Tou Ng. Bayesian online classifiers for text classification and filtering. In *Proceedings of the 25th annual international ACM SIGIR conference on Research and development in information retrieval*, SIGIR '02, pages 97–104, New York, NY, USA, 2002. ACM.

[12] Yadolah Dodge. Weighted arithmetic mean. In *The Concise Encyclopedia of Statistics*, pages 565–566. Springer New York, 2008.

[13] E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi. In-network aggregation techniques for wireless sensor networks: a survey. *Wireless Communications, IEEE*, 14(2):70–87, April 2007.

[14] M.C. Fernandez-Gago, R. Roman, and J. Lopez. A survey on the applicability of trust management systems for wireless sensor networks. In *Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2007. SECPerU 2007. Third International Workshop on*, pages 25–30, July 2007.

[15] Saurabh Ganeriwal and Mani B. Srivastava. Reputation-based framework for high integrity sensor networks. In *Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN '04, pages 66–77, New York, NY, USA, 2004. ACM.

[16] Oscar Garcia-Morchon and Klaus Wehrle. Modular context-aware access control for medical sensor networks. In *Proceedings of the 15th ACM symposium on Access control models and technologies*, SACMAT '10, pages 129–138, New York, NY, USA, 2010. ACM.

[17] H. A. Greene and D. Wright. Security lessons learned from hipaa enforcement. *3rd USENIX Workshop on Health Security and Privacy, HealthSec '12*, 2012.

[18] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen. Distributed access control with privacy support in wireless sensor network. *IEEE Transactions on wireless communications*, 2011.

[19] Devon M. Herrick, Linda Gorman, and John C. Goodman. Health Information Technology: Benefits and Problems. Technical Report 327, April 2010.

[20] F. Ishmanov and Sung Won Kim. A secure trust establishment in wireless sensor networks. In *Electrical Engineering and Informatics (ICEEI), 2011 International Conference on*, pages 1–6, July 2011.

[21] Audun Josang and Roslan Ismail. The beta reputation system. In *In Proceedings of the 15th Bled Electronic Commerce Conference*, 2002.

[22] N. Karthik and V.R.S. Dhulipala. Trust calculation in wireless sensor networks. In *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, volume 4, pages 376–380, April 2011.

[23] N. Lewis, N. Foukia, and D.G. Govan. Using trust for key distribution and route selection in wireless sensor networks. In *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE*, pages 787–790, April 2008.

[24] Ke Liu, Nael Abu-Ghazaleh, and Kyoung-Don Kang. Location verification and trust management for resilient geographic routing. *Journal of Parallel and Distributed Computing*, 67(2):215 – 228, 2007.

[25] Tao Liu, De-Jun Chen, and Ming-Zheng Zhou. Pair-wise key update in wireless sensor networks based on reputation model. In *Electronics, Communications and Control (ICECC), 2011 International Conference on*, pages 1558–1561, Sept 2011.

[26] Tao Liu and Ming-Zheng Zhou. A key management scheme in wireless sensor networks based on behavior trust. In *Progress in Informatics and Computing (PIC), 2010 IEEE International Conference on*, volume 1, pages 556–559, Dec 2010.

[27] E. Lupu, N. Dulay, M. Sloman, J. Sventek, S. Heeps, S. Strowes, K. Twidle, S.-L. Keoh, and A. Schaeffer-Filho. Amuse: autonomic management of ubiquitous e-health systems. *Concurr. Comput. : Pract. Exper.*, 20(3):277–295, March 2008.

[28] Mohammed Mana, Mohammed Feham, and Boucif Amar Bensaber. Trust key management scheme for wireless body area networks. *I. J. Network Security*, 12(2):75–83, 2011.

[29] D. W. Marsh, R. O. Baldwin, B. E. Mullins, R. F. Mills, and M. R. Grimalia. A security policy language for wireless sensor network. *Journal of Systems and Software*, 2009.

[30] MATLAB. *MATLAB and Statistics Toolbox Release 2012b(R2012b)*. The MathWorks Inc., Natick, Massachusetts, 2012.

[31] H.A. Maw, Hannan Xiao, B. Christianson, and J.A. Malcolm. An evaluation of break-the-glass access control model for medical data in wireless sensor networks. In *e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on*, pages 130–135, Oct 2014.

[32] Htoo Maw, Hannan Xiao, and Bruce Christianson. An adaptive access control model for medical data in wireless sensor networks. In *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom) (IEEE Healthcom 2013)*, Lisbon, Portugal, October 2013.

[33] Htoo Aung Maw, Hannan Xiao, and Bruce Christianson. An adaptive access control model with privileges overriding and behaviour monitoring in wireless sensor networks. In *8th ACM International Symposium on QoS and Security for Wireless and Mobile Networks 2012 (ACM Q2SWinet 2012)*, Paphos, Cyprus, October 2012.

[34] Htoo Aung Maw, Hannan Xiao, Bruce Christianson, and James A. Malcolm. A survey of access control models in wireless sensor networks. *Journal of Sensor and Actuator Networks*, 3(2):150–180, 2014.

[35] J.D. Meier, Mackman Alex, Dunner Michael, Vasireddy Srinath, Escamilla Ray, and Murukan Anandha. Threats and countermeasures. *Microsoft Developer Network*, June 2003.

[36] D.P. Mirembe and M. Muyeba. Threat modeling revisited: Improving expressiveness of attack. In *Computer Modeling and Simulation, 2008. EMS '08. Second UKSIM European Symposium on*, pages 93–98, 2008.

[37] Maher Moakher. A differential geometric approach to the geometric mean of symmetric positive-definite matrices. *SIAM J. Matrix Anal. Appl*, 26, 2005.

[38] M. Momani. *Bayesian Methods for Modelling and Management of Trust in Wireless Sensor Networks*. PhD thesis, University of Technology, Sydney, 2008.

[39] M. Momani, K. Aboura, and S. Challa. Rbatmwsn: Recursive bayesian approach to trust management in wireless sensor networks. In *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, pages 347–352, Dec 2007.

[40] M. Momani, S. Challa, and R. Alhmouz. Bnwsn: Bayesian network trust model for wireless sensor networks. In *Communications, Computers and Applications, 2008. MIC-CCA 2008. Mosharaka International Conference on*, pages 110–115, 2008.

[41] M. Momani, S. Challa, and R. Alhmouz. Can we trust trusted nodes in wireless sensor networks? In *Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on*, pages 1227–1232, May 2008.

[42] Mohammad Momani and Subhash Challa. Gtrssn: Gaussian trust and reputation system for sensor networks. In Tarek Sobh, editor, *Advances in Computer and Information Sciences and Engineering*, pages 343–347. Springer Netherlands, 2008.

[43] Luminita Moraru, Pierre Leone, Sotiris Nikoletseas, and José D. P. Rolim. Near optimal geographic routing with obstacle avoidance in wireless sensor networks by fast-converging trust-based algorithms. In *Proceedings of the 3rd ACM Workshop on QoS and Security for Wireless and Mobile Networks*, Q2SWinet '07, pages 31–38, New York, NY, USA, 2007. ACM.

[44] K. Nagarathna, Y.B. Kiran, J.D. Mallapur, and S. Hiremath. Trust based secured routing in wireless multimedia sensor networks. In *Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International Conference on*, pages 53–58, July 2012.

[45] Erik Rissanen, BabakSadighi Firozabadi, and Marek Sergot. Towards a mechanism for discretionary overriding of access control. In Bruce Christianson, Bruno Crispo, JamesA. Malcolm, and Michael Roe, editors, *Security Protocols*, volume 3957 of *Lecture Notes in Computer Science*, pages 312–319. Springer Berlin Heidelberg, 2006.

[46] L. Rostad and O. Edsberg. A study of access control requirements for healthcare systems based on audit trails from access logs. In *Computer Security Applications Conference, 2006. ACSAC '06. 22nd Annual*, pages 175–186, Dec 2006.

[47] Sushmita Ruj, Amiya Nayak, and Ivan Stojmenovic. Distributed fine-grained access control in wireless sensor networks. In *IPDPS*, pages 352–362, 2011.

[48] R.A. Shaikh, H. Jameel, B.J. d'Auriol, Heejo Lee, Sungyoung Lee, and Young-Jae Song. Group-based trust management scheme for clustered wireless sensor networks. *Parallel and Distributed Systems, IEEE Transactions on*, 20(11):1698–1712, Nov 2009.

[49] Sarbjeet Singh. Trust based authorization framework for grid services. *Journal of Emerging Trends in Computing and Information Sciences*, 2(3), March 2011.

[50] Dale Skeen. A quorum-based commit protocol. Technical report, Ithaca, NY, USA, 1982.

[51] A. Srinivasan, J. Teitelbaum, and Jie Wu. Drbts: Distributed reputation-based beacon trust system. In *Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on*, pages 277–283, Sept 2006.

[52] Sapon Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy. Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks. In *Performance, Computing, and Communications, 2004 IEEE International Conference on*, pages 463–469, 2004.

[53] Kevin Twidle, Emil Lupu, Naranker Dulay, and Morris Sloman. Ponder2 - a policy environment for autonomous pervasive systems. In *Proceedings of the 2008 IEEE Workshop on Policies for Distributed Systems and Networks*, POLICY '08, pages 245–246, Washington, DC, USA, 2008. IEEE Computer Society.

[54] Yifei Wang, Sean W. Smith, and Andrew Gettinger. Access control hygiene and the empathy gap in medical IT. Technical Report TR2012-713, Dartmouth College, Computer Science, Hanover, NH, January 2012.

[55] Maruca William. A peek behind the OCR wall of shame. Technical report, Legal Issue, Developments and Other Pertinent Information Relating to the Creation, Use and Exchange of Electronic Health Records, 2007.

[56] Zhiying Yao, Daeyoung Kim, and Yoonmee Doh. Plus: parameterised localised trust management-based security framework for sensor networks. *Int. J. Sen. Netw.*, 3(4):224–236, June 2008.

[57] S. Yu, K. Ren, and W. Lou. Fdac toward fine-grained distributed data access control in wireless sensor networks. *IEEE Transaction on Parallel and Distributed Network*, 2011.

[58] Weiwei Yuan, Donghai Guan, Le Xuan Hung, Youngkoo Lee, and Sungyoung Lee. A trust model with dynamic decision making for ubiquitous environments. In *Networks, 2006. ICON '06. 14th IEEE International Conference on*, volume 1, pages 1–6, 2006.

[59] Weiwei Yuan, Donghai Guan, Sungyoung Lee, and Youngkoo Lee. A dynamic trust model based on naive bayes classifier for ubiquitous environments. In *Proceedings of the Second international conference on High Performance Computing and Communications*, HPCC'06, pages 562–571, Berlin, Heidelberg, 2006. Springer-Verlag.

[60] Junqi Zhang, R. Shankaran, M.A. Orgun, V. Varadharajan, and A. Sattar. A dynamic trust establishment and management framework for wireless sensor networks. In *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, pages 484–491, Dec 2010.

[61] Junqi Zhang, R. Shankaran, M.A. Orgun, V. Varadharajan, and A. Sattar. A trust management architecture for hierarchical wireless sensor networks. In *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, pages 264–267, Oct 2010.

Appendix B

A Literature Review

B.1 Introduction

In this chapter, the published literatures for WSN area are reviewed based on following criteria; security oriented applications, development tools, quantitative research method for access control roles and policies, and trust-based security mechanisms.

B.2 Applications in WSNs

A WSN is envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring such as Great Duck (bird observation on Great Duck island), earthquake monitoring, ocean water monitoring, wind turbine, Grape monitoring, parts assembly, patients monitoring, traffic monitoring, tracking military vehicles, etc [73]. Based on above current deployment of applications in WSNs, these applications can be categorized into public sector, military, medical, environmental monitoring, industrial, emergency rescue mission, automotive and agricultural. Among these applications, the military, surveillance, border patrol and medical applications are two most security-oriented fields of WSNs and they received most of the attention from researchers.

- **Military Application**: WSNs can use in the military sector for a number of purposes such as enemy tracking, monitoring military activities and battlefield surveillance. The rapid deployment, self-organize and fault tolerance characteristics of sensor networks make them a very promising sensing technique for military Command, Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance

(C4ISR) [101]. In military applications, the sensor nodes are used to collect information of enemies, tracking military vehicles, etc. Sensed and stored data at the sensor nodes are highly confidential and kept secretly. So, data confidentiality is needed to provide and control access to that data should be managed by using some security and access control mechanisms. Privacy of source-location is another issue which needs to consider for sensor nodes because they are not protected by tamper-proof and tamper-evident. If the attackers know the location of sensor nodes in WSNs, they can physically attack these sensor nodes by damaging and smashing them.

- **Surveillance Application**: In a surveillance scenario, the sensor nodes are used to enhance and complement existing surveillance systems against crime and terrorist attacks. Large scale networks of sensors can extend the ability of law-enforcement agencies to monitor areas, public events, private properties and borders. Multimedia data will be useful when incidents such as accidents, theft, criminals, etc. are happened in the real world environment. Multimedia content such as video streams and images, along with advanced signal processing techniques, will be used to locate missing persons or to identify criminals and terrorists. This means that the confidentiality of collected and stored data in the sensor nodes must be maintained. The access to that data recourse should be carefully considered to prevent unauthorised usages from both illegitimate and legitimate users. Only authorised users can access the data from those sensor nodes. Sometimes, the users might need to access data for emergency situations, when the person who has an access privilege to access that data, is not available. It is important to provide data availability service as well as data confidentiality in emergency situations.

- **Border Patrol Application**: Border patrol systems [126] have recently gained attention to address the concerns that are related to national security. The major challenge in protecting the borders of one country is the need of human involvement in patrolling the premises. The traditional border control systems consist of security checkpoints and border troops. This kinds of systems are suffered from intensive human involvement if manual patrolling is considered. A WSN can be used in border patrol application to reduce the human interactions. The border patrol application based on Hybrid Wireless Sensor Network which consists of wireless multimedia sensor networks [4], [3] and wireless underground sensor network [5], [6], can accurately detect and track the borders intrusion with minimum human involvement. In border patrol application, the collected data by the camera or video sensor nodes may need to keep secretly and

access to that data might be prohibited to unauthorised users. Additionally, the communication channels need to be secured to transfer collected data within the Hybrid Wireless Sensor Network. Therefore, a light-weigh security mechanism is needed to consider for this kind of application.

- **Medical Application**: Nowadays, WSNs are rapidly growing and overcoming new application area in medical or healthcare domain. Wireless sensors for healthcare domain are becoming smaller and more powerful to use in a wide range of medical applications such as health monitoring, chronic disease management and measuring user vital signs. Wireless Medical Sensor Network (WMSN) is another form of WSNs, which used in medical and healthcare domain. In WMSN, sensors are attached with human body to monitor healthcare information like ECG, blood pressure, etc. A medical staff can access, collect and record medical data directly from a patient's sensor for remote health care monitoring services. Garcia-Morchon [43] mentioned that user's medical data lead to security and privacy concerns. So, the security services such as confidentiality, integrity, authenticity, non repudiation, are required to provide in healthcare applications. In addition, control access to patient's medical data becomes serious issue in WMSN because there might be a number of medical staffs and family members, who try to interact with medical data.

The above four applications area are more active than other applications. Among these four applications area, the medical and military areas are most security-oriented applications in the real world. Currently, we developed a medical application to show that how the proposed access control model is fitted into these areas and how the policy overriding can be done based on users' behaviour trust value. On the other hand, we investigate the usability and accountability of the proposed model based on the medical application.

B.3 Development Tools for WSNs

There are two different type of development tools in WSNs named as simulator and emulator. Simulators are mostly used for modelling and developing of WSNs. For real world implementation and testing, an emulator is used with simulator to get an accurate result for WSN based applications. There are variety of development tools for WSNs in the current WSN research community. Among them, a several popular simulation and emulation tools for WSNs are discussed.

B.3.1 Simulator for WSNs

Simulation is the most popular, feasible and effective approach to develop, design and test network protocols in WSNs. A simulator is universally used to develop for network protocols especially in the beginning phase of network designs. The cost for simulating hundreds or even thousands of nodes is very low and also it can be done within the short amount of executing time by using the simulator. Some simulators are designed for general wireless networks and some are designed especially for WSNs. The simulator achieves to accurate security protocols or network models, and to predict the behaviour of real world environment in different scenarios. A few network simulators for general wireless networks and WSNs are discussed as follows.

- NS-2 [131]

  NS-2 stands for Network Simulation Version 2 and it can be run on both Linux and Window operating system but Cygwin is needed to run NS-2 in Window platform. NS-2 simulator is a popular tool among others in wired and wireless networks. NS-2 supports a considerable amount of protocols in all layers. Ad-hoc and WSN based security protocols are also supported by NS-2 tool which is easy to modify and improve codes for simulation because it is an open source model as well as it save the cost of simulation. NS-2 is especially aimed for general network simulation and it does not consider the characteristics of WSNs and its hardware constraints. There is a scalability problem for WSN in NS-2 because if the number of nodes are increased, the tracing file will be too large and too big to manage and handle.

- OMNeT++ [134]

  OMNeT++ supports module programming language and it can run on both Linux and Window operating system. OMNeT++ is a popular general network simulation tool for both wired and wireless networks. Most of the frameworks and simulation models in OMNeT are open source code. The advantage of using OMNeT++ is that it provides a powerful graphic user interface that makes tracing and debugging more easier than other simulation tools. OMNeT++ provides MAC layer protocols for both wired and wireless networks but for WSNs, a limited number of protocols are considered and developed. The disadvantage of this simulation tool is that the existing functions and properties are not good enough to design the network protocols especially, when there are lots of constraints and limitations in WSNs.

- SENS [127]

The abbreviation of SENS is Sensor, Environment and Network Simulator that involves four main interchangeable and extensible components for physical, environmental, network and application layer. A physical component is used to read sensed information. An application component simulates the software of sensor node. Additionally, it communicates with network component to manage incoming and outgoing data packets. SENS provides the performance evaluation tools for development of the applications but for routing protocol module, there is no manual or documentation for the public usage.

- Ponder2 [129]

  Ponder2 is a popular policy language to use in Body Sensor Network (BSN). Ponder2 comprises a self-contained, stand-alone, general-purpose object management system with message passing between objects. It incorporates an awareness of events and policies and implements a policy execution framework. It has a high-level configuration and control language called PonderTalk and user-extensible managed objects that are programmed in Java. Ponder2 is implemented as Self Managed Cell (SMC) [78] that is a set of hardware and software components forming an administrative domain. This means that, Ponder2 is capable of self management. Everything in Ponder2 is a managed object that has to be loaded dynamically into the SMC from a library, thereby producing the factory managed object (Java class).

B.3.2 Emulator for WSNs

Imran [57] mentioned that an emulator is a hybrid scheme which combines both software and hardware where some components are implemented in the real sensor nodes and some are developed in a simulation program or a simulator. The emulator is implemented in real sensor nodes, thus it may provide better security services and performance than using the simulation program only. Some of the emulators provide highly scalability. At the same time, it can emulate the numerous number of sensor nodes. A summary of horizontal and vertical analysis at diffreent phases based on current WSN simulators and emulators is shown in Figure B.1. There are several emulators for WSNs which are explained with their advantages and disadvantages.

- TOSSIM[69]

  TOSSIM is an emulator that is based on TinyOS (Tiny Operating System) [68] especially designed for WSNs. TinyOS is an open source embedded operating system

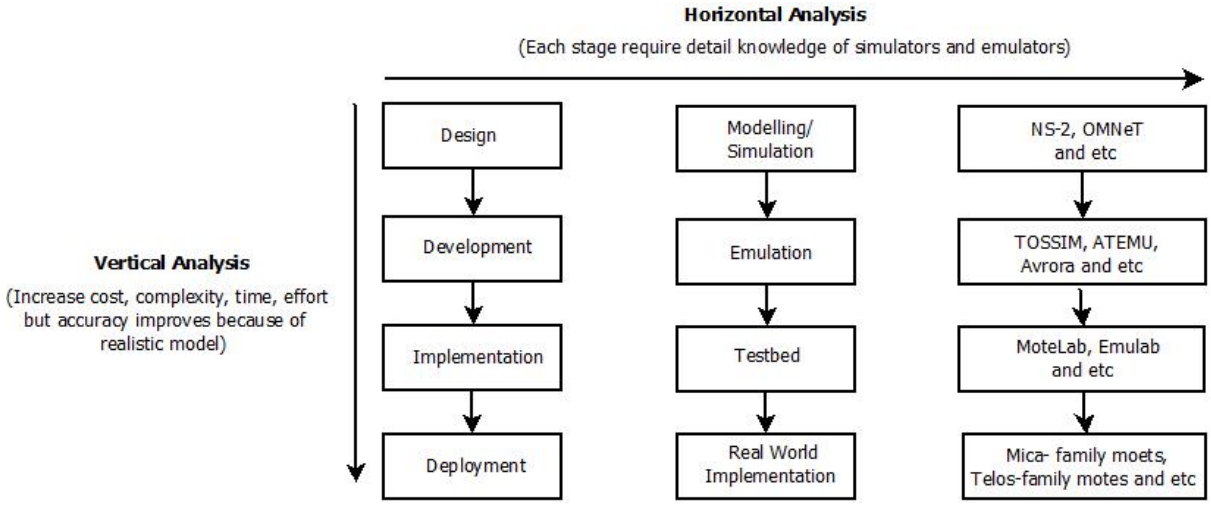


Fig. B.1 A Summary of Horizontal and Vertical Analysis at Different Phases

(Source: M. Imran, A. M. Said and H. Hasbullah
A Survey of Simulators, Emulators and Testbeds for Wireless Sesnor Network [57])

which targets to use with embedded devices or hardware. TOSSIM is a discrete event network simulator based on Python and C++ programming platforms. TOSSIM provides on-line documents, open resources and graphic user interface namely; TinyViz which is very convenient for a user to interact with electronic devices. TOSSIM is a powerful network emulator for WSNs because it supports hundreds or even thousands of sensor nodes simulation. Most of the WSN researchers used TinyOS and TOSSIM for radio module and code execution because it can simulate an accurate result for real world situations. There are some limitations of using TOSSIM. Every sensor nodes need to run on NesC [46] - an embedded programming language - which is event-driven, component-based and implemented based on TinyOS. TOSSIM can only emulate the same type of homogeneous applications. This means that TOSSIM is designed for WSNs simulation but it needs the same type of sensor node because it does not support for cross platforms. In addition, the simulation results for energy consumption cannot be true and accurate.

- ATEMU[105]

  ATEMU is introduced to provide a fine-grained approach based network emulator that developed and improved over TOSSIM. ATEMU achieves to balance between hardware devices and network simulation. ATEMU is also compatible with both Mica family motes and Telos family motes which are two popular powerful sensor nodes

in WSNs. ATEMU can simulate over cross platform sensor nodes, hardware and applications. A graphic user interface is provided to debug and monitor code execution processes. ATEMU can give an accurate simulation result for WSNs but the simulation time is much longer than other tools. Unlike TOSSIM, the documentations are not well noted and there is no latest version of network simulation tool and documents. Therefore, it is hard to follow the documentation that is not well noted and presented.

- Avrora[17]

  Avrora is designed for a WSN over java platform. Alike ATEMU, Avrora allows to simulate cross platform of sensor nodes, application and hardware devices. This means that it supports both Micas and Telos motes for simulation. Avrora was developed by University of California, Angles Compilers Group. Avrora was built on the advantages over both TOSSIM and ATYMU tools to reduce the drawbacks. A graphic user interface is not supported in Avrora but it provides the open source codes and well-noted on-line documents. Avrora emulator is an instruction-level simulator so, the code can be run instruction by instruction. Therefore, the execution time is faster and better as well as it provides scalability. Avrora provides much flexible than TOSSIM and ATEMU because it was implemented in Java. The disadvantages of Avarora are there is no graphic user interface to trace and debug the executable code, and the network management algorithms cannot be simulated because it doesn't provide network communication tools.

B.4 Quantitative Research Method for Access Control

In this section, the quantitative research survey of access control roles and policies in the medical industry which is carried out by Ferreira [37] is briefly discussed. The following roles and policies are essential for medical scenario but in general, these roles and policies can be easily applied in other application areas.

B.4.1 Legislative Access Control Rules

Legislative and regulation need to be put into practice. Based on Health Care Professionals' (HCPs) responsibility and patient rights, and consent, the following legislative access control rules are extracted within the access control policies. Although some are very generic,

these rules constitute some of the access control policies to adjusts according to the need of real world requirements. The rules based on HCPs are extracted as follows:

- Patient's consent must be sought where required.
- Medical data should only be collected and processed by HCPs or individuals or bodies working on behalf of HCPs.
- Appropriate measures must be available to protect against unauthorised access.
- Providers of information, communication and health services should under all circumstances must be identifiable including final owner or provider.

The following rules are represented for the patients based on legislative recommendations:

- Access to medical data by patients may be refused, limited or delayed under some circumstances (i.e, defined by the HCPs).
- Every person shall be enabled to have access to his/her medical data either directly or through a HCP.

B.4.2 Access Control Rules

The general access control roles and policies for both HCPs and Patients are discussed as follows:

Rules for HCPs

- Access in Emergency Situation
  - Specific roles must be able to adjust decisions regarding data access (read only) in emergency situations.
  - Logging and audit should be provided at all time that integrated with above role.
- System Access (Authentication)
  - Different types of authentication mechanism must be available to adapt according to users' need (Most common are login/password + biometrics).

- Logging and Monitoring
  - Audit must be available and secured at all times.
  - Necessary to provide alert features to avoid problems with the authentication mechanisms.
- Access Control Roles
  - It must be possible to define alerts for the number of accesses based on specific users or roles.
  - The responsible person must be alerted if someone or some role reaches that limit.
  - The definition of access control roles must be fine-grained.
  - The head of the department (responsible role) must be able to assign one or more people to alter some access permission for some roles.
- Who Decide who accesses what
  - There must be a representative for each role who can define or change the policies for that role.
- Problems with The Policies Alterations and adaptations
  - Roles must be able to change and adapt accordingly.
  - Permission to modify a role must be provided for specific circumstances.
  - All the above rules must be logged and registered as same conditions that handle in emergency situations (someone gets a message of changes and revises its appropriateness).
- Security
  - Necessary to provide alert features for the different services on a system (to prevent and detect downtime in a faster way).

Rules for Patient

- Access by Patient
  - Patients must be able to access their record, either paper or electronically, with the help of HCPs.
- Illiteracy and Ignorance
  - Patients must be able to access their record, either paper or electronically, as a summarised record.
- Legislation and Rights
  - Patients must be able to access their record, either paper or electronically, without any modifications.
- System Access (Authentication)
  - Different types of authentication mechanisms must be available to be adapted according to the users' need (most common are login/password + biometrics.)
- Access Control Roles
  - Access control roles must exist depending on the professional category or type of information.
  - The role must exist the option for patients to define access control roles in some situations.
  - There must exist the option of defining access control roles for several different cases. For example, groups of people that could define these access control roles could be: a doctor with a patient, a doctor with a family member (when a patient cannot do it), only the family assisting doctor, etc.
- Security
  - IT support roles must exist in order to deal with problems more rapidly and efficiently (e.g., logged time response, alert to responsible people when time is expired, etc)

Overall, the above roles and policies are needed to consider when a new access control model is designed and developed especially for medical or other complicated applications but in general, these roles and policies should be able to apply in other application area in WSNs.

B.5 Conclusion

Based on the above discussion, a WSN is very active in several application areas such as medical, military, border patrol, health care, etc. Additionally, choosing a right tool is an essential in WSNs based on the requirements of the application and time period. Finally, to propose a new access control model for a WSN, the basis access control roles or policies are needed to define in advance for a medical application.

Appendix C

An Overview of Implementation Phase

A detailed development process of an example medical scenario with the proposed access control model is discussed in this appendix. The example medical scenario is already explained under applications for Wireless Sensor Network section. The proposed access control model is an extended version of Ponder2. The hierarchical structure of Ponder2 package with the proposed model is shown in Figure C.1.

There are lots of different modules under main Ponder2 package. The main module is SRC known as source file of Ponder2. In the SRC module, there are two different files: Ponder2 (Java Package) and Ponder2 (resource). In Ponder2 (Java package), all the Java source codes are stored. All the Java codes of user interfaces for an example medical scenario are stored under the “Hospital” folder and the main Java files for all the users such as doctor, nurse, patient, patient family are located in “Managedobject” folder.

Everything in Ponder2 is a Managed Object. A Managed Object has to be loaded dynamically into the SMC from a library, thereby producing a factory managed object(Java class). This is the same as any object oriented system where the class has to be loaded before instances can be created. All the policies definition are stored under the ”Policy” folder. Under Ponder2 (Resource) folder, the “Pondertalk” source files are stored. A user interface of nurse is called by Poundertalk file as follow.

```
//Setting for patient in the example/hospital/scenario
newauthpol := root/factory/authpolicy.
//load the managed object for a patient
factory := root load: "PatientMO1".
```

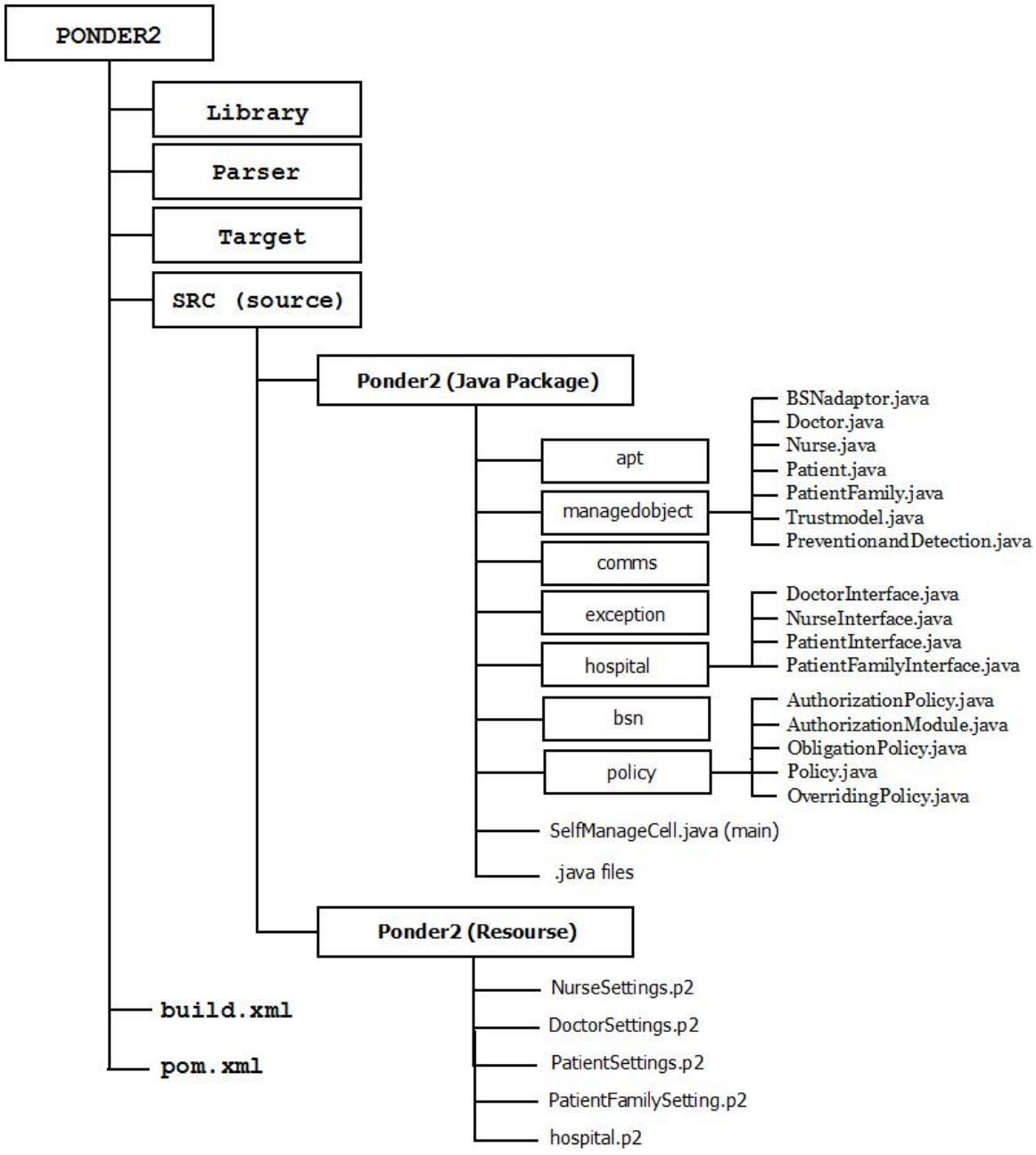


Fig. C.1 A Hierarchical Structure of Ponder2

The following coding are part of coding from the "Patient-Setting.p2" file under Ponder2 (resource). In the following code, the patient interface is loaded by PonderTalk command and created the interfaces for the patients. Two patient interfaces are created named as Bob and Alice with certain information. Currently, the information for each patient is limited

to name, age, symptom and location. We can add extra information regarding the patients by editing codes in Java and Pondertalk file. We can also add more patients to test the accountability of the application by putting extra code in “Patient-setting.p2” file. It will be the same for doctors, nurses and patient families. All the interface of users will be called by Pondertalk command “load” and created. “load” command is a factory command to load a Java managed object file for SMC.

```
    //instantiate a PatientMO object
bob := factory createname: "Bob" age:"18" symp:"Heart-Attack" path: "/patient/heart/bob".
root/patient/heart at: "bob" put: bob.
alice := factory createname: "Alice" age:"17" symp:"Lung-Cancer" path: "/patient/cancer/alice".
root/patient/cancer at: "alice" put: alice.
```

Ponder2 is combination of three different languages such as Extensible Markup Language (XML), pondertalk syntax and Java. Ponder2 project is based on Apache Marven project. “Pom.xml” is used to build the whole Ponder2 project but “build.xml” is used to compile the SMC. To compile a medical example, the following code is added in “build.xml” file.

```
target: Medical-Scenario (scenario 3)
<target name="Medical-Scenario" depends="build" description="–> Runs the SMC with
access policy">
<antcall target="run">
<param name="autharg" value="-auth allow" />
<param name="bootarg" value="-boot boot.p2 -boot hospitaldomain.p2 -boot ex3/tut1.p2
-boot eca1.p2 -boot scenario3/nurse-settings.p2 -boot scenario3/patient-settings.p2 -boot
scenario3/doctor-settings.p2 -boot scenario3/audit.p2 -boot scenario3/patient-family-setting.p2"
/>
</antcall>
</target>
```