RESEARCH ON DESIGN AND IMPLEMENTATION OF SECURE ATTRIBUTE-BASED ENCRYPTION FRAMEWORK FOR BODY SENSOR NETWORKS

By

TAN YAR LING

A dissertation submitted to the Department of Electrical and Electronic Engineering,
Faculty of Engineering and Science,
Universiti Tunku Abdul Rahman,
in partial fulfillment of the requirements for the degree of
Master of Engineering and Science
April 2014

ABSTRACT

RESEARCH ON DESIGN AND IMPLEMENTATION OF SECURE ATTRIBUTE-BASED DATA ENCRYPTION FRAMEWORK FOR BODY SENSOR NETWORKS

Tan Yar Ling

Recent advances of today's computing technologies and wireless sensor networks have brought remarkable progress on current electronic healthcare system. The current electronic healthcare devices are lightweight and low-power consumption. These types of sensors enable the monitoring of human health condition as well as early detection of potential illnesses. Body sensor network (BSN) is composed of a set of sensors attached on human body to collect vital signs. Vital signs collected are such as heart rate and 3D motion. These vital signs will be sent to the healthcare provider by networks (e.g. internet) and stored in the storage server. Due to the importance of privacy and confidentiality of the vital signs, vital signs need to be protected by encryption before sending them to the healthcare provider's storage server.

The objectives of this work are to carry out a thorough study of attribute-based encryption (ABE) and its application to body sensor network (BSN) and to design and deploy an attribute-based encryption for body sensor network in connected health system.

One of the current disadvantages of data encryption is the limitation upon user's ability to selectively share their encrypted data by healthcare professionals at a fine-grained level. Thus, in our work, key-policy attribute-based encryption (KP-ABE) scheme is used as the encryption scheme to encrypt the vital signs. In KP-ABE, the data are encrypted with a set of descriptive attributes while the private key of the authorized personnel is embedded with a set of access structure. Private Key generator (PKG) is a trusted third party and it generates and issues the private key to the authorized personnel. The BSN framework consists of wearable sensors that records vital signs on a patient, a computing device that collects the vital signs and performs encryption onto the vital signs and send the encrypted vital signs to the healthcare storage server. Hospital personnel will retrieve and decrypt the encrypted vital signs using their private key. This facilitates differential access rights provision to the hospital personnel. Furthermore, it allows flexibility in specifying the access rights of authorized hospital personnel over the encrypted data. Then, they will be able to view the health condition and make some basic medical diagnostics for their patients.

In this dissertation, a study on ABE for BSN which are the KP-ABE and ciphertext-policy attribute based encryption (CP-ABE) is carried out. Both the ABE are analysed and the suitable ABE is deployed in the BSN framework. Then, a BSN framework prototype is designed to protect patient's medical information by using KP-ABE encryption scheme. Finally, a secure connected healthcare system framework with international standards is proposed.

ACKNOWLEDGEMENT

The strength, love and wisdom from Lord, Jesus Christ has brought me to the completion of this dissertation. It was His calling and given courage that I took up the master degree course. It was a good three years of learning and experiencing God's faithfulness and fruitfulness in my life. It is He who gives me hope and brings me through all the tough times during the studies. I thank God for all His wonderful blessings in my life.

I would like to thank my supervisor Prof. Dr. Goi Bok Min and co-supervisor Prof. Dr. Ryoichi Komiya for giving me a chance to pursue my master degree. I am thankful and grateful for their guidance, patience, and advices throughout the whole master studies. Also, their motivations have helped me a lot to move forward and do better.

I would like to thank my family especially my parents and fiancé for their awesome support and encouragements. My late maternal grandfather Mr. Lim Book Seng has been a great provider to me all these years. I am thankful to him for providing me financially and supporting me until his passing away during the course of my studies.

Special thanks to Mr. Tan Syh Yuan and Mr. Chong Zan Kai for many helpful discussions during the course of this research work. Finally, I would also like to thank all my postgraduate friends for their help and encouragements.

APPROVAL SHEET

This dissertation entitled "**RESEARCH ON DESIGN AND IMPLEMENTATION OF SECURE ATTRIBUTE-BASED ENCRYPTION FRAMEWORK FOR BODY SENSOR NETWORKS"** was prepared by **TAN YAR LING** and submitted as partial fulfillment of the requirements for the degree of Master of Engineering and Science at Universiti Tunku Abdul Rahman.

Approved by:

_____

(Prof. Dr. Goi Bok Min) Date: 30 April 2014
Professor/Supervisor
Department of Electrical and Electronic Engineering
Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

_____

(Prof. Dr. Ryoichi Komiya) Date: 30 April 2014
Professor/Co-supervisor
Department of Mechatronics and Biomedical Engineering
Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

FACULTY OF ENGINEERING AND SCIENCE

UNIVERSITI TUNKU ABDUL RAHMAN

Date: 30 April 2014

SUBMISSION OF DISSERTATION

It is hereby certified that **Tan Yar Ling** (ID No: **10UEM07476**) has completed this dissertation entitled "**Research on Design and Implementation of Secure Attribute-Based Encryption Framework for Body Sensor Networks**" under the supervision of Prof. Dr. Goi Bok Min (Supervisor) from the Department of Electrical and Electronic Engineering, Faculty of Engineering and Science, and Prof. Dr. Ryoichi Komiya (Co-Supervisor) from the Department of Mechatronics and Biomedical Engineering, Faculty of Engineering and Science.

I understand that University will upload softcopy of my dissertation in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

_____

(Tan Yar Ling)

DECLARATION

I Tan Yar Ling hereby declare that the dissertation is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTAR or other institutions.

_____

(TAN YAR LING)

Date: 30/04/2014

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES

LIST OF TERMINOLOGY

Terminology	Definition
Attribute	Identities/characteristics of a person
Access Policy	Policy to define which ciphertext an authorized user is able to decrypt
Electronic Health Record (EHR)	Patient’s vital sign and personal information
Leaf node	Any node that does not have child nodes
Private Key Generator	A trusted third party who handles the issuance of private key
Vital sign	An indicator of a person's general physical condition

CHAPTER I

INTRODUCTION

The progress of today's computing technologies and the wireless sensor networks have brought remarkable impacts on the current electronic healthcare. Furthermore, the current information communication technologies have made possible the distributed healthcare monitoring of patients outside the hospital possible.

Electronic healthcare devices are essential for the sensing and monitoring early prevention of possible life threatening abnormalities. The abnormalities are such as heart diseases, diabetes, hypertension, chronic obstructive pulmonary disease (COPD), and other chronic diseases. Early detection of disease symptom by using electronic healthcare devices could ease the treatment by healthcare professional and could prevent the development and deterioration of the disease.

Body sensor network (BSN), one of the electronic healthcare devices is a small personal electronic healthcare network which has been studied and tested its availability all over the world. The BSN is composed of wearable computing device with a set of sensors attached to different parts of human body to collect vital sign. The vital signs collected are such as body temperature, blood pressure, pulse rate (or heart rate), and respiratory rate. Once the vital signs are

captured, they will be sent to the third party storage server to be stored. The third party storage server can be a healthcare server. In this way, healthcare professional could retrieve and diagnose patients' vital signs from the healthcare server. Thus, allowing patients to be monitored remotely from the hospital.

The captured vital sign together with patient's information will be stored and shared by any healthcare professional (e.g. doctors, nurses, pharmacies, patient and etc.) at healthcare server. Therefore, it is very important to ensure the security and privacy of the patients' electronic health record (EHR) including patient's vital signs and personal information. Therefore, the EHR needs to be encrypted before sending and storing at any healthcare server. Moreover, some patients might prefer to selectively share their EHR to specific hospital professionals who are an expert or specialist in that specific medical field. Therefore, by implementing the ABE scheme on the BSN, the security and privacy issues and sharing of encrypted EHR by medical experts could be worked out.

Thereafter, a BSN framework design with international standards is essential to provide a clearer picture of BSN in the telemedicine network. Besides that, the BSN framework helps to clearly justify the practicality and extensibility of BSN toward different users. With the possible extensibility, the BSN framework based on international standards could cater for the needs of users' connection to telemedicine network globally.

1.1 Justification of Study

Cryptography aims to enable users to communicate with one another securely over an insecure channel by constructing schemes or protocols. This is a way to ensure users' privacy and security during data transmission.

The aim of the research work is to encrypt the EHR for transmission and storage. Since the encrypted EHR is stored in the storage server, the storage server cannot be fully trusted with the encrypted EHR. An assumption is made where the storage server will not maliciously remove the encrypted EHR. However, any unauthorized personnel at the storage server may attempt to learn the contents of the stored encrypted EHR**.**

On another hand, sharing of encrypted data at fine-grained level should be feasible. Sharing encrypted data at fine-grained level means that only a certain authorized healthcare professional could have the access right to the encrypted data. For example, doctors of the cardiology department can only view the data of cardiology of the patient and not having the access right to any other data. Attribute-based encryption is one of the powerful approaches to secure EHR which at the same time allows sharing of encrypted data at a fine-grained level.

Also, in order to achieve the practical usage of a secured BSN among different users in different countries, a globally applicable BSN framework design is highly required.

1.2 Research Objectives

Research objectives of this study are summarized as below.

1. To study attribute-based encryption (ABE) and its application to BSN.
2. To build a BSN prototype with deployment of ABE.
3. To design a BSN framework in telemedicine network with international standards.

1.3 Research Methodologies

The research methodologies of this study are as below;

- Study and analysis of the ABE with its application to BSN by literature review and discussions,
- ABE scheme definition as a security model for BSN,
- An indoor BSN prototype with ABE design and experiments,
- BSN framework proposal in telemedicine using international standards.

1.4 Dissertation Structure

- Chapter 2 gives a comprehensive literature review of BSN system, ABE schemes and the application of security schemes in BSN.
- Chapter 3 presents the study of ABE in term of the comparisons between the two different models of ABE.
- Chapter 4 shows the prototype of the work and the experimental results.
- Chapter 5 discusses the BSN with ABE framework design proposal using international standards.
- Chapter 6 concludes this dissertation together with open problems and future works.

CHAPTER II

LITERATURE REVIEW

2.1 Telemedicine

Telemedicine (Perednia and Allen, 1999; Güler and Übeyli, 2002; Ekeland et al., 2010) enables patients to be remotely monitored or taken care of at a distance with the use of electronic information and communications technologies. In other words, it is referred to as a remote health care system. It allows the exchange of medical, imaging and health informatics data via the Internet. The purpose of telemedicine is for remote medical consulting and examinations. It helps in improving the access of patients especially those living in rural areas to medical services by eliminating the distance barrier.

Historically telemedicine started from simple telephone conversation between two health specialists about a case. Later on it has become more sophisticated system by using video-conferencing equipment and satellite technology.

There are two major methods of telemedicine; real-time and store-and-forward (Harnett 2006). The two methods are applied to different purposes depending on the patients' disease conditions. Real-time telemedicine allows simultaneous both way communications between patient and healthcare professionals. Patient sends medical information to healthcare professionals almost instantaneously. If patient's disease condition is unstable and urgent treatment

is sometimes necessary, then the real-time vital sign transmission to healthcare professionals is required.

Real-time telemedicine enable patients to benefit real time diagnosis at a distance by the healthcare professionals. Also, healthcare professionals can make immediate decisions and requests at the time of the diagnosis session with patients. Moreover, real-time telemedicine is more effective in terms of consultation and patient satisfaction than store-and-forward telemedicine (Hailey et al., 2004). However, the disadvantage of real-time telemedicine is that it would incur higher cost than store-and-forward telemedicine. It is due to the relatively expensive interactive videoconferencing involving audio, video, and data transmission technologies and applications (Marilyn, 1996). Besides that, timely scheduling is required for consultation between healthcare professionals and patient.

In contrast, store-and-forward allows non-simultaneous communications between patient and healthcare professionals. Patient encapsulates the medical information and then transmits to healthcare professionals at certain time of period. If patient's disease condition is stable and doctor's office visits can be made by doctor's suggestion, then store-and-forward telemedicine is appropriate for the transmission of stored vital sign. Vital sign and clinical query can be transmitted by the patient and then diagnosed and answered by healthcare professionals at a convenient time. Therefore, it is more effective in terms of cost, complexity and convenience than real-time telemedicine (High et al., 2000). However, store-and-forward telemedicine has the disadvantage of

lower diagnostic accuracy than real-time telemedicine due to the time different between symptoms occurrence and time of diagnosis.

Due to the widespread applicability in telemedicine applications as well as the improved sensor technology and miniaturization of transmission and processing devices, the concept of BSNs have received increased consideration.

2.2 Body Sensor Networks (BSNs)

BSNs (Istepanian et al., 2004; Lo et al., 2005; Otto et al., 2006; Ko et al., 2010) is emerging wireless wearable and implantable systems that promise to improve quality of life through improving healthcare, independent living for the elderly, and healthcare cost reduction. Several promising type of body sensors have emerged for managing and monitoring patients of different medical condition such as acute diabetes, epilepsy, neurological disorders and chronic cardiac diseases. BSN is composed of multiple sensor nodes which are interconnected on a human body. Each sensor node provides sensing, processing, and wireless communication capabilities.

2.2.1 Sensors

Sensors are generally divided into three categories; physiological, bio-kinetic and ambient. Physiological sensors are used for applications such as electrocardiography (ECG), electromyography (EMG), and electroencephalography (EEG),

Bio-kinetic sensors measure angular rate of rotation and acceleration derived from human movements. Ambient sensors measure environmental phenomena, such as temperature, sound pressure level, humidity, and light.

2.2.2 Communication

BSNs are unique because they attempt to restrict the communication radius to the body vicinity. Limiting transmission range reduces a node's power consumption, decreases interference among adjacent BSNs, and helps maintain privacy. BSNs typically can communicate over Zigbee (IEEE 802.15.4) radio (Timmons and Scanlon, 2004; Lo et al., 2005) and Bluetooth (IEEE 802.15.1). Zigbee is a specification of a very low-power wireless personal area network (WPAN) protocol. Bluetooth on another hand is a low-cost, low-power, robust, short-range wireless communication protocol. In year 2012, the IEEE 802.15.6 (Astrin et al., 2009; Martelli et al., 2011) started specifically for wireless networks on or in the body with low power. IEEE 802.15.6 standard is set up in order to meet the current demands on modern health. It is mainly to improve the performance such as shorter range communication, lower device complexity, higher transfer of data rate, lower power constraint, in-body environment, security, and quality of service.

2.2.3 Storage

One of the functionality of BSN is the availability of on-node storage. On-node storage is a reasonable solution for archiving data. On-node storage could incorporate extra memory resources and this allows the additional storage of data while the BSN is not maintaining data streaming during network outages.

Some applications might be chosen to cache data until the data is ready to transmit after network recovery. Consequently, conditional caching could prolong battery life, and decrease bit errors.

2.3 Technical Preliminaries

This section shows the definition of bilinear pairing and access tress structure.

2.3.1 Bilinear Pairings

Definition 2.1 *Let* $\mathbb{G}$ *and* $\mathbb{G}_T$ *be cyclic group of prime order p. Let g be a generator of* $\mathbb{G}$*. The bilinear map* $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ *is said to be an admissible map if it satisfies the following conditions:*

1. *(Non-degeneracy)* $e(P, P) \neq 1$.
2. *(Bilinearity)* $e(aP, bQ) = e(P, Q)^{ab}$ *for all* $a, b \in Z_q$.
3. *Efficiently Computable.*

2.3.2 Access Tree Structure

In KP-ABE, ciphertexts are associated with a set of descriptive attributes while private keys are embedded with a tree access structure which is also known as access policy. The leaves are associated with attributes and each interior node of the tree is a threshold gate. Meanwhile in CP-ABE, the ciphertexts are associated with the tree access structure while the private keys are embedded with a set of descriptive attributes. The access structure in this dissertation is a monotone access structure. Let $\mathcal{T}$ be denote as the access structure.

Definition 2.2 *Each non-leaf node is represented by a threshold gate which is described by its children and a threshold value. If* num_x *is the number of children of a node* x *and* k_x *is its threshold value, then* $0 < k_x \leq num_x$ *.* $k_x = 1$ *if the threshold gate is an OR gate and* $k_x = num_x$ *if it is an AND gate. Each leaf node x of the access tree* $\mathcal{T}$ *is described by an attribute and a threshold value* $k_x = 1$.

The parent of the node x in the tree is denoted by parent(x). The function att(x) is defined only if x is a leaf node and denotes the attribute associated with the leaf node x in the tree. Access tree $\mathcal{T}$ *defines an ordering for the children of every node, from 1 to num. The function index(x) returns the number associated with the node x. The function index(x) returns the ordering number associated with the node x where the index values are uniquely assigned to nodes in* $\mathcal{T}$ *for a given key in an arbitrary manner.*

Let $\mathcal{T}_x$*be the subtree of root access tree* $\mathcal{T}_r$ *at node x. If a set of attributes* γ *satisfies* $\mathcal{T}_x$*, it is denoted as* $\mathcal{T}_x(\gamma) = 1$*. If x is a non-leaf node,* $\mathcal{T}_x(\gamma)$ *is computed recursively by evaluating every* $\mathcal{T}_{x'}(\gamma)$ *for all children* x' *of node x.* $\mathcal{T}_x(\gamma)$ *returns 1 if and only if at least* k_x *children return 1. If x is a leaf node, then* $\mathcal{T}_x(\gamma)$ *returns 1 if and only if att(x)* ϵ γ.

2.4 Background

In 1985, Shamir introduced a type of public encryption scheme called Identity-Based Encryption scheme (IBE) (Shamir 1985), which enable users to securely communicate, verify and exchange each other's signatures without any

exchange of public or secret keys. Thus, eliminates the need to keep key directories. Instead of generating a random pair of public/secret key and made the public key known to everyone, the public key can be in a form of any arbitrary string. Such as, names, phone number, home address, e-mail address and etc. provided that they can uniquely identify the user whom he cannot later deny. For example, Alice can encrypt her message and sends to Bob at Bob's email address, bob@email.com where Bob's email address is Bob's identity. When Bob received Alice's message in his email address, he then will need to authenticate his identity to the private key generator (PKG), a third party, in order to retrieve his private key to decrypt Alice's message. With the use of identity-based encryption, Alice can send Bob message even if Bob has yet to own his public key certificate.

In year 2001, Boneh and Franklin came up the first secure and practical IBE from the Weil pairing on elliptic curves (Boneh and Franklin, 2001). The IBE scheme is composed of four algorithms:

1) Setup: Generates the global system parameters and a master-key,
2) Extract: Uses the master-key to compose the private key corresponding to an arbitrary public key string ID,
3) Encrypt: Encrypts messages by using the public key ID,
4) Decrypt: Decrypts messages by using the corresponding private key.

In 2005, Sahai and Waters introduced a scheme called Fuzzy Identity-Based Encryption (FIBE) (Sahai and Waters, 2005). In IBE, identities are viewed as arbitrary strings. While in FIBE, identities are being viewed as a set of descriptive attributes. In FIBE scheme, a user is allow to decrypt a ciphertext when his/her private key corresponding to a set of identity, *ID* overlap with the

ciphertext encrypted with the public key, *ID'* by some distance metric, *d*. Thus, FIBE scheme allows a certain amount of error-tolerance in the identities. In this paper, the authors mentioned on the application of FIBE termed as Attribute-Based Encryption (ABE). In an ABE system, a user's private key and ciphertext are associated with a set of attributes. A private key can decrypt a ciphertext if there is a match between the attributes of the user's private key and ciphertext.

2.4.1 Key-Policy Attribute Based Encryption (KP-ABE)

After ABE was first introduced in the work of Sahai and Waters, in year 2006, Goyal et al. proposed the key-policy attribute based encryption for fine-grained sharing of encrypted data (Goyal et al., 2006). Encryption of vital sign usually limits the ability of encrypted vital sign to be shared among different users. In other words, the encrypted vital sign can only be selectively shared at a coarse-grained level. For example, in order to perform vital sign decryption, patient needs to give his/her private key to another party. This somehow allows another party to have all the access of the patient's vital sign. Another alternative, patient can act as an intermediary to perform decryption on the relevant vital sign but can be arduous. Both approaches do not seem appealing as they are not practical and inefficient. Fine-grained sharing of encrypted data enables different authorized users to retrieve and decrypt ciphertext based on their access policy. The access policy embedded in the user's key specifies the type of ciphertext that the user's key is allowed to decrypt. In KP-ABE, each ciphertext is labeled with a set of descriptive attributes, while the access policy is embedded in the user's key. User is able to decrypt a ciphertext if the access

policy of user's key matches the descriptive attributes labeled at the ciphertext. KP-ABE scheme is able to grant different access rights to different users.

Construction of KP-ABE

Setup Define the universe of attributes $\mathcal{U} = \{1,2,\dots,n\}$. Associate each attribute $i \in \mathcal{U}$ with a number t_i choose uniformly at random from $\mathbb{Z}_p$. Choose y uniformly at random in $\mathbb{Z}_p$. The public key, PK is:

$$PK = (T_1 = g^{t_1}, \dots, T_{|\mathcal{U}|} = g^{t|\mathcal{U}|}, Y = e(g,g)^y)$$

The master key MK is:

$$MK = (t_1, \dots, t_{|\mathcal{U}|}, y)$$

Encryption(M, γ, PK) Choose a random value $s \in \mathbb{Z}_p$. Encrypt a secret message $M \in \mathbb{G}_2$ with a set of attributes γ. The ciphertext is:

$$E = \left(\gamma, E' = MY^s, \{E_i = T_i^s\}_{i\in\gamma}\right).$$

Key Generation $(\mathcal{T}, \mathrm{MK})$ This algorithm outputs a private key D embedded with an access structure. The private key D enable user to decrypt a message encrypted under a set of attributes γ if and only if $\mathcal{T}(\gamma) = 1$. The algorithm proceeds by choosing a polynomial q_x for each node x (including the leaves) in the access tree $\mathcal{T}$. These polynomials are chosen in the following way in a top-down manner, starting from the root node r.

For each node x, set the degree d_x of the polynomial q_x to the one less than the threshold value k_x of that node, that is, $d_x = k_x - 1$. For the root node r, set $q_r(0) = y$. Randomly choose d_r element in $\mathbb{Z}_p$ to completely define q_r. For any other non-leaf node x, set $q_x(0) = q_{\text{parent}(x)}(\text{index}(x))$ and randomly choose d_x element in $\mathbb{Z}_p$ to completely define q_x. For each leaf node x, the following secret value is assign to the user:

$$D_x = g^{\frac{q_x(0)}{t_i}} \text{ where } i = \text{att}(x).$$

The set of above secret values is the decryption key D.

Decryption (E, D) Define a recursive algorithm DecryptNode(E, D, x) that takes as input the ciphertext $E = \left(\gamma, E', \{E_i\}_{i\in\gamma}\right)$,the private key D (assume the access tree $\mathcal{T}$ is embedded in the private key), and a node x in the tree. It outputs a group element of $\mathbb{G}_2$ or $\perp$.

Let $i = \text{att}(x)$. If the node x is a leaf node then:

$$\text{DecryptNode}(E, D, x)$$

$$= \begin{cases} e(D_x, E_i) = e\left(g^{\frac{q_x(0)}{t_i}}, g^{s\cdot t_i}\right) = e(g,g)^{s\cdot q_x(0)} \text{ if } i \in \gamma \\ \perp \text{ otherwise} \end{cases}$$

For non-leaf node x, all nodes z that are children of x. Let S_x be an arbitrary k_x-sized set of child nodes z such that DecryptNode(E, D, z) = $F_z \neq \perp$. If no such set exists then the node was not satisfied and the function returns $\perp$.

Otherwise, compute:

$$F_x = \prod_{z \in S_x} F_z^{\Delta_{i,S'_x}(0)}, \text{where } \begin{matrix} i = \text{index}(z) \\ S'_x = \{\text{index}(z) : z \in S_x\} \end{matrix}$$

$$= \prod_{z \in S_x} \left(e(g,g)^{s \cdot q_z(0)}\right)^{\Delta_{i,S'_x}(0)}$$

$$= \prod_{z \in S_x} \left(e(g,g)^{s \cdot q_{\text{parent}(z)}(\text{index}(z))}\right)^{\Delta_{i,S'_x}(0)}$$

$$= \prod_{z \in S_x} e(g,g)^{s \cdot q_z(i) \Delta_{i,S'_x}(0)}$$

$$= e(g,g)^{s \cdot q_x(0)}$$

Now that function DecryptNode is defined, the decryption algorithm calls the function on the root of the tree. DecryptNode$(E, D, r) = e(g,g)^{ys} = Y^s$ if and only if the ciphertext satisfies the tree. Since, $E' = MY^s$ the decryption algorithm divides out Y^s and recovers the message M.

2.4.2 Ciphertext-Attribute Based Encryption

In year 2007, Bethencourt et al. provides the first construction of a ciphertext-policy attribute-based encryption (CP-ABE) scheme (Bethencourt et al., 2007). In CP-ABE scheme, private key is labeled with a set of descriptive attributes, while the access policy is associated with the ciphertext. A user is able to decrypt the ciphertext if his attributes satisfy the access policy associated to the ciphertext.

Construction of CP-ABE

Setup. Choose a bilinear group $\mathbb{G}_0$ of prime order p with generator g. Next it chooses two random exponents $\alpha, \beta \in \mathbb{Z}_p$. The public key is:

$$PK = (\mathbb{G}_0, g, h = g^{\beta}, f = g^{\frac{1}{\beta}}, e(g,g)^{\alpha})$$

The master key MK is:

$$MK = (\beta, g^{\alpha})$$

Encryption $(\mathrm{PK}, M, \mathcal{T})$ Choose a random value $s \in \mathbb{Z}_p$. Encrypt a message $M \in \mathbb{G}_2$ with a set of attributes γ, and the ciphertext is:

$$E = \left(\gamma, E' = MY^s, \{E_i = T_i^s\}_{i \in \gamma}\right).$$

Key Generation $(\mathcal{T}, \mathrm{MK})$ The encryption algorithm encrypts a message M under the tree access structure $\mathcal{T}$. The algorithm first chooses a polynomial q_x for each node x (including the leaves) in the tree $\mathcal{T}$. These polynomials are chosen in the following way in a top-down manner, starting from the root node R. For each node x in the tree, set the degree d_x of the polynomial q_x to the one less than the threshold value k_x of that node, that is, $d_x = k_x - 1$.

For root node R the algorithm chooses a random $s \in \mathbb{Z}_p$. Sets $q_R(0) = s$. Then, it randomly chooses d_R element $\mathbb{Z}_p$ to completely define q_r. For any other non-leaf node x, set $q_x(0) = q_{\mathrm{parent}(x)}(\mathrm{index}(x))$ and randomly choose d_x elements in $\mathbb{Z}_p$ to completely define q_x.

Let, Y be the set of leaf nodes in $\mathcal{T}$. The ciphertext is then constructed by giving the tree access structure $\mathcal{T}$ and computing

$$\mathrm{CT} = \Big(\mathcal{T},\ \bar{C} = Me(g,g)^{\alpha s}, c = h^{s}, \forall y \in Y: C_y = g^{q_y(0)}, C'_y = H\big(\mathrm{att}(y)\big)^{q_y(0)}\Big).$$

KeyGen (MK, S)**.** The key generation algorithm will take as input a set of attributes S and output a key that identifies with that set. The algorithm first chooses a random $r \in \mathbb{Z}_p$, and then random $r_j \in \mathbb{Z}_p$ for each attribute $j \in S$. Then it computes the key as

$$\mathrm{SK} = \big(D = g^{(\alpha+r)/\beta}, \forall j \in S: D_j = g^{r} \cdot H(j)^{r_j}, D'_j = g^{r_j}\big).$$

Decryption $(\mathrm{CT}, \mathrm{SK})$ Define a recursive algorithm $\mathrm{DecryptNode}(\mathrm{CT}, SK, x)$ that takes as input a ciphertext $\mathrm{CT} = \big(\mathcal{T}, \tilde{C}, C, \forall y \in Y: C_y, C'_y\big)$, a private key SK, which is associated with a set S of attributes, and a node x from $\mathcal{T}$.

For each leaf node x let $i = \mathrm{att}(x)$ and define as follows: If $i \in S$, then

$$\mathrm{DecryptNode}(\mathrm{CT}, \mathrm{SK}, x) = \frac{e(D_i, C_x)}{e(D'_i, C'_x)} = \frac{e\big(g^{r} \cdot H(i)^{r_i}, g^{q_x(0)}\big)}{e(g^{r_i}, H(i)^{q_x(0)})} = e(g,g)^{r q_x(0)}$$

If $i \notin S$, then define $\mathrm{DecryptNode}(\mathrm{CT}, \mathrm{SK}, x) = \perp$.

For each non-leaf node x, all nodes z that are children of x. Let S_x be an arbitrary k_x-sized set of child nodes z such that $\text{DecryptNode}(\text{CT}, \text{SK}, z) = F_z \neq \perp$. If no such set exists then the node was not satisfied and the function returns $\perp$.

Otherwise, compute:

$$F_x = \prod_{z \in S_x} F_z^{\Delta_{i,S'_x}(0)}, \text{where } \begin{matrix} i = \text{index}(z) \\ S'_x = \{\text{index}(z) : z \in S_x\} \end{matrix}$$

$$= \prod_{z \in S_x} \left(e(g,g)^{s \cdot q_z(0)}\right)^{\Delta_{i,S'_x}(0)}$$

$$= \prod_{z \in S_x} \left(e(g,g)^{s \cdot q_{\text{parent}(z)}(\text{index}(z))}\right)^{\Delta_{i,S'_x}(0)}$$

$$= \prod_{z \in S_x} e(g,g)^{s \cdot q_z(i) \Delta_{i,S'_x}(0)}$$

$$= e(g,g)^{s \cdot q_x(0)}$$

Now that function DecryptNode is defined, the decryption algorithm begins by calling the function on the root node R of the tree $\mathcal{T}$. If the tree is satisfied by S, set $A = \text{DecryptNode}(\text{CT}, \text{SK}, R) = e(g,g)^{r q_R(0)} = e(g,g)^{rs}$. The algorithm now decrypts by computing

$$\tilde{C} / (e(C,D)/A) = \tilde{C} / (e(h^s, g^{\frac{(\alpha + r)}{\beta}}) / (e(g,g)^{rs})) = M$$

2.5 Related Work

Several cryptographic schemes have been proposed to secure and preserve the privacy of EHR. (Bao et al., 2008; Sun and Fang, 2010; Zhang et al., 2012). Hu et al. (2009) proposed the public key infrastructure (PKI) to protect the privacy and security of health record. PKI scheme is deployed for authentication and distribution of EHR and symmetric cryptographic is used to preserve the confidentiality of the EHR. However, the proposed work is not practically implemented on the hardware system.

Benaloh et al. (2009) proposed the patient controlled encryption (PCE). PCE design proposes a hierarchical-based encryption scheme to protect the EHR which allows patients to delegate access rights to their medical record. The PCE provides the advantage of storing medical record over any third party storage server. However, PCE has the drawback where it needs to create and manage multiple keys by patients and healthcare professionals. For instance, if patients wish to share their EHR based on the sensitivity of data within a given category, then a separate decryption key is required for each sensitivity level in that category. Therefore, PCE has the limitation which prevents flexible access to patients' EHR.

Tan et al. (2008) proposed a lightweight identity based encryption (Lite-IBE) scheme for BSN sensors. The work of Tan et al. proposes scheme mainly deals with emergency care scenario where privacy of EHR and access right restrictions is concern. In Tan et al. scheme, sensor nodes compute public keys from each arbitrary string. The public keys are then stored on the flash memory

to be used for executing elliptic curve encryption/decryption. For each different arbitrary string, a public key needs to be generated. Thus, the proposed work has the drawbacks of higher execution time, greater energy consumption due to increased computational complexity and higher storage requirement as the results of public key storage.

Akinyele et al. (2010) implement a self-protecting electronic medical records (EMRs) using attribute-based encryption. In their system, each node is encrypted in the XML-based electronic medical record file with the access policy being generated automatically which is then exported to the cloud system. The attributes in the private key defined an EHR's user's access rights. Nonetheless, key revocation and key delegation is not solved in the system. Besides that, the implementation work is limited due to the malformed metadata of the encrypted XML file.

Ibraimi et al. (2009) present a variant of ciphertext-policy attribute-based encryption (CP-ABE) scheme which is used to enforce patient/organizational access control policies. In the proposed work, health records can be encrypted with an access policy which has attributes issued by two trusted authorities: the trusted authority (TA1) of the professional domain (PO) and the trusted authority (TA2) of the social domain (SO). However, no implementation work is carried out on the proposed work.

Table 2.1: Comparison Table

	Hu et al. (2009)	**Benaloh et al. (2009)**	**Tan et al. (2008)**	**Akinyele et al. (2010)**	**Ibraimi et al. (2009)**	**Dissertation**
Encryption method	PKI	PCE	Lite-IBE	KP-ABE/ CP-ABE	CP-ABE	KP-ABE/ CP-ABE
Hardware Implementation	No	No	Yes	Yes	No	Yes
Platform	-	-	N/A	Workstation/ Server & Mobile	-	Computing
Operating System	-	-	N/A	Mac OS	-	Ubuntu
Encryption Time (a) KP-ABE (b) CP-ABE *For number of leaves/attributes =40	-	-	-	(a) ≈0.8sec (b) ≈1.3sec	-	(a) ≈0.6sec (b) ≈0.8sec
Decryption Time (a) KP-ABE (b) CP-ABE *For number of leaves/attributes =40	-	-	-	(a) ≈1.0sec (b) ≈2.0sec	-	(a) ≈0.25sec (b) ≈0.4sec
Private Key Generation Time (a) KP-ABE (b) CP-ABE *For number of leaves/attributes =40	-	-	-	-	-	(a) ≈0.75sec (b) ≈0.96sec
Security Parameter	-	-	-	224-bit Elliptic Curve	-	160-bit Elliptic Curve
Security Strength	-	-	-	112-bit	-	80-bit
Proposed Design with International Standard	No	No	No	No	No	Yes

Table 2.1 shows the comparison table of the work in this dissertation with the related works. In this dissertation, attributes are used to encrypt the EHR helps to solve the issue of key management problem. As a result, every healthcare professional has only one private key corresponding to their access structure which is used to perform decryption on the encrypted EHR.

Key management issue is for example; patient may need to give his/her private key to healthcare professional in order to allow the healthcare professional to perform EHR decryption. However, by giving his/her private key to healthcare professional somehow allows the healthcare professional to have all the access of the patient's EHR. Another alternative, patient can act as an intermediary to perform decryption on the relevant encrypted EHR but this action can be arduous. Thus, both approaches do not seem appealing as they are not practical and inefficient.

Moreover, encryption of EHR using attributes also enables sharing of encrypted EHR at a fine-grained level. Fine-grained sharing of encrypted data enables different hospital professionals to retrieve and decrypt EHR based on their access structure embedded in their private keys which specify types of encrypted EHR which are allowed for decryption.

A BSN framework is designed and ABE encryption schemed is deployed in a real hardware system to create a prototype of ABE for BSN. Hence, the scalability and flexibility are highly preserved. Furthermore, BSN framework design using proposed international standards are proposed. This work uses a 160-bit elliptic curve group which provides 80-bit security strength which is minimum recommended security strength.

CHAPTER III

COMPARISON OF ENCRYPTION METHODS FOR BODY SENSOR NETWORK

This chapter discusses the study and analysis of the suitability of attribute-based encryption for both KP-ABE and CP-ABE in the BSN framework**.** In this chapter, comparisons between KP-ABE and CP-ABE are conducted in terms of the encryption time, assignment of attribute and access policy and hardware implementation.

Table 3.1 (Recommended Elliptic Curve Domain Parameters 2010) shows the information of the properties of recommended elliptic curve domain parameters over finite field. Both KP-ABE and CP-ABE in this work use a 160-bit A type elliptic curve group based on the supersingular curve $y^2 = x^3 + x$ over a 512-bit finite field without preprocessing. Therefore, as shown in Table 3.1, the work of this dissertation is proven to provide 80-bit security strength. Furthermore, 80-bit security strength is the minimum recommended security strength.

Table 3.1: Properties of Recommended Elliptic Curve Domain Parameters over F_p

Parameters	Strength	Size	RSA/DSA
p112	56	112	512
p128	64	128	704
p160	80	160	1024
p192	96	192	1536
p224	112	224	2048
p256	128	256	3072
p384	192	384	7680
p521	256	521	15360

3.1 Encryption and Decryption Time

In order to secure the privacy of the patients' EHR, the EHR has to be encrypted before sending to the remote server. The EHR in the encrypted form however, limits the sharing of information (i.e. vital signs) among different users (i.e. healthcare professionals). Therefore, it is essential to design a selective sharing of encrypted EHR at fine-grained level.

In KP-ABE, attributes are being encrypted in the EHR and access policy is embedded in the private key. Therefore, the Private Key Generator (PKG) plays an important role in private key issuing with embedded access policy to the authorized healthcare professionals. If the PKG itself is compromised by malicious people, the confidentiality of the patients together with their EHR

could be deprived. On the other hand, in CP-ABE, access policy is embedded in the EHR and attributes are embedded in the private key. In CP-ABE, the security and protection of the encrypted EHR is mainly dependent on the access policy. Private Key is issued based on a set of identity of the healthcare professionals. Table 3.2 indicates the attributes and access policy setting in each ABE scheme.

Table 3.2: Attributes and Access Policy Setting in ABE Scheme

ABE Scheme		Ciphertext	Private Key
KP-ABE	Attributes	✓	
	Access Policy		✓
CP-ABE	Attributes		✓
	Access Policy	✓	

Both KP-ABE and CP-ABE schemes are able to share encrypted data at fine-grained level. This also means that healthcare professionals are able to retrieve and decrypt selected pieces of the encrypted EHR according to the specified attributes and access policy. Therefore, healthcare professionals need to validate themselves to the third party Private Key Generator (PKG) before they request and retrieve their private keys.

Figure 3.1 shows the experimental results of encryption time for KP-ABE and CP-ABE. The number of attributes (for KP-ABE) and leaf-nodes (for CP-ABE) are being increased from 5 to 50. For each increment of attribute/leaf-node the

encryption process is performed and the encryption time is captured. Each encryption time is captured by repeating the encryption process for 30 times and then the average time of encryption is obtained by calculation.

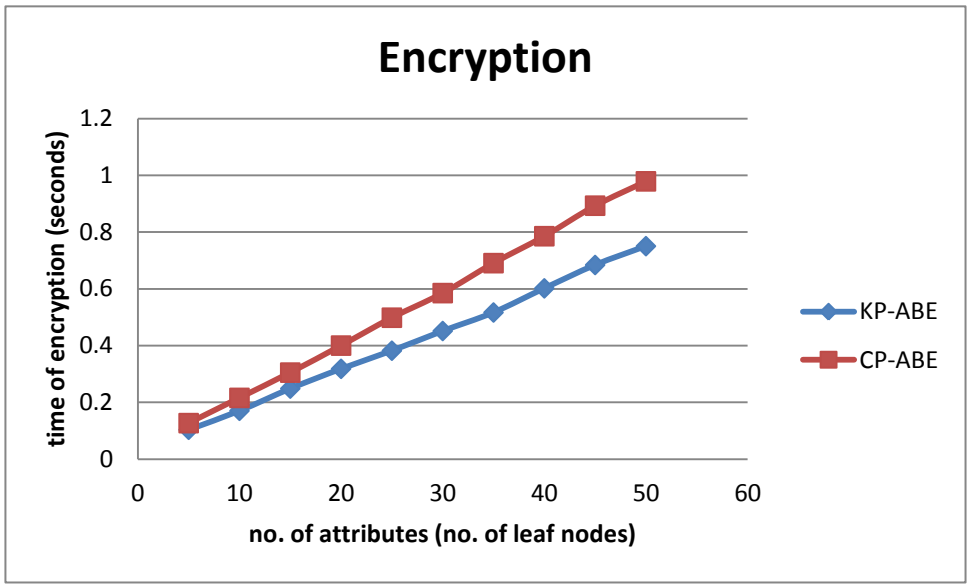


Figure 3.1: Encryption time of KP-ABE and CP-ABE

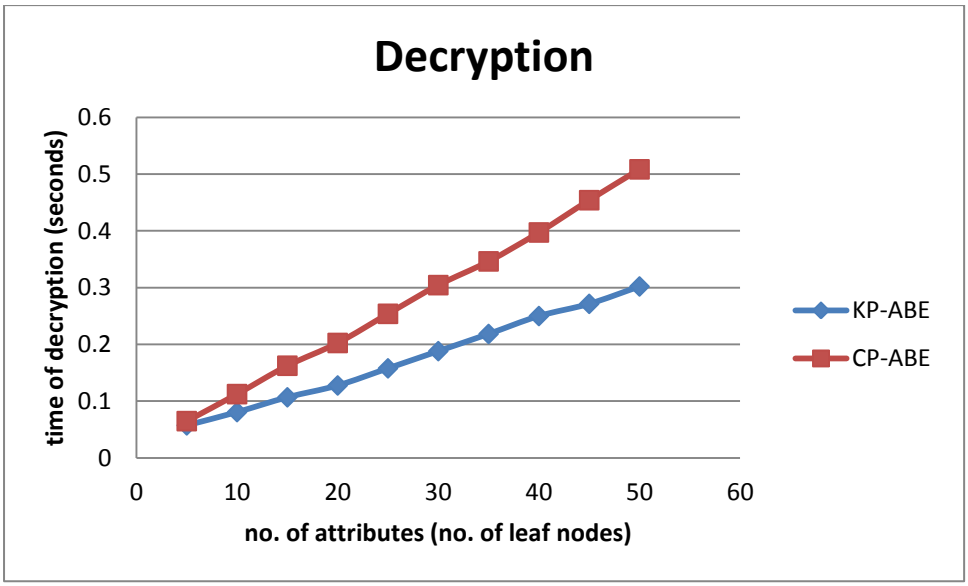


Figure 3.2: Decryption time of KP-ABE and CP-ABE

For KP-ABE encryption, the encryption time increases according to number of attributes. As for CP-ABE the encryption time increases according to number of leaf nodes. CP-ABE encryption algorithm takes longer encryption time compared to KP-ABE encryption algorithm. This is because KP-ABE encryption algorithm performs one exponentiation for each attribute while CP-ABE encryption algorithm performs two exponentiations for each leaf in the ciphertext's access tree. In Figure 3.1, in case of attribute number of 40, encryption time difference between KP-ABE and CP-ABE is 200 msec. By considering practical number of attributes or leaf nodes, the encryption time difference would be significant.

Figure 3.2 shows the experimental results of KP-ABE and CP-ABE decryption. After performing the encryption process by using different number of attribute/leaf nodes, the decryption process is carried out. Therefore, the number of attributes/leaf-nodes at decryption is measured also from 5 to 50. For each increment in attribute/leaf-node, the decryption process is performed and the decryption time is captured. Each decryption time is captured by repeating the decryption process for 30 times and then the average time of decryption is obtained by calculation.

As for decryption experimental results shown in Figure 3.2, the decryption time of KP-ABE is roughly twice faster than CP-ABE. This is due to the reason that KP-ABE only performs one bilinear mapping for each attribute while CP-ABE performs twice for each leaf node.

3.2 Assignment of Attribute and Access Policy

Attributes are the identities or characteristics of a person. For example, “General Doctor”, “Specialist”, “Kuala Lumpur”, “Cardiologist” and etc. Access policy on the other hand is the access structure. For example, {(“General Doctor” AND “Specialist”) AND (“Kuala Lumpur” OR “Penang”) OR “Medical Experience>20years” OR “Name: Dr. Hosanna”}.

All private keys are being issued and managed by the PKG. The PKG will have to manage the information of the registered healthcare professionals in order to issue the correct private keys embedded with access policy as shown in Figure 3.3. Private Key for all healthcare professionals are being issued once unless the healthcare professionals request for a new private key with attribute/access policy updates.

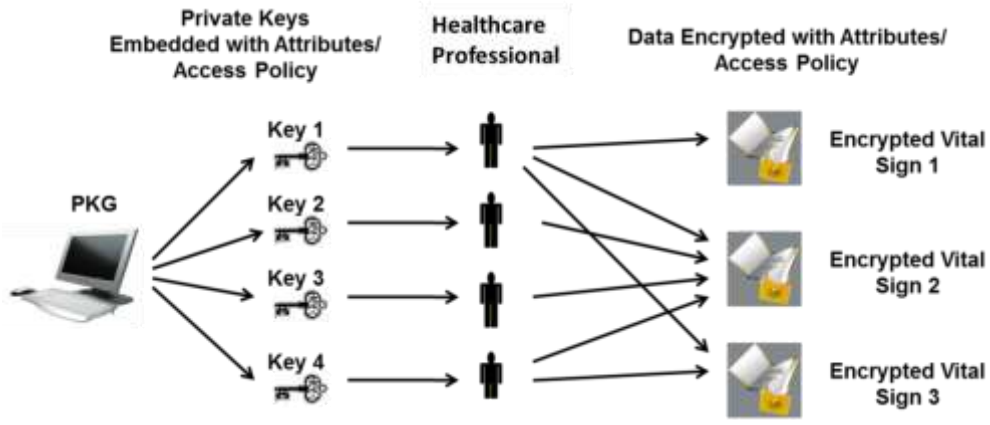


Figure 3.3: Key Issuance and Access to Encrypted Data

Therefore, PKG is responsible for the assignment of attributes and access policy which are embedded in the private key. However, the assignment of

attributes and access policy are to be embedded in the ciphertext (for both KP-ABE and CP-ABE), the patients should assign them with the assistance of the medical agents of the healthcare authority. Assignment of attributes by the patient with the assistance of medical agents is much simpler than assigning the access policy in the ciphertext by patients with the assistance of medical agents. Patient may also be able to alter the attributes accordingly in a more efficient and faster manner than making changes onto the access policy. This is due to the reason that by making a slight mistake of alteration of the access policy may cause a complication in the entire encryption and decryption system.

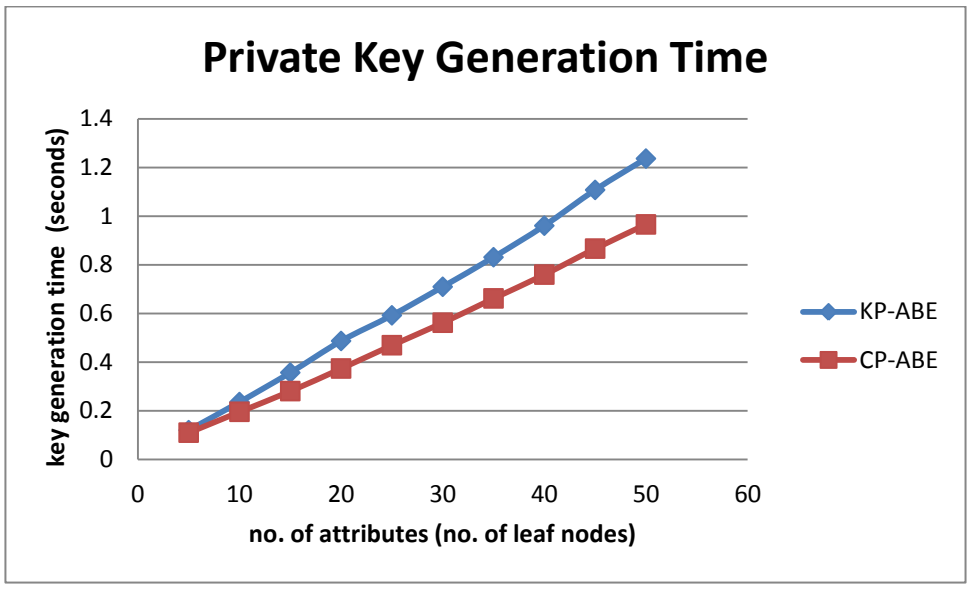


Figure 3.4: Private Key generation time of KP-ABE and CP-ABE

Figure 3.4 shows the experimental results of private key generation time for both KP-ABE and CP-ABE. As expected, private key generation time of ABE is linearly increasing according to the number of attributes in KP-ABE and the

number of leaf nodes in CP-ABE. KP-ABE private key generation takes longer time than CP-ABE. The private key generation time difference between KP-ABE and CP-ABE would be significant by considering the large number of hospital professionals' private keys required to be generated.

3.3 Hardware Implementation

From the view point of hardware implementation, lower computation power is prerequisite. In this section the memory power consumption is studied.

Table 3.3: Memory usage of KP-ABE and CP-ABE

Process	Memory (MB)	
	KP-ABE	CP-ABE
Encryption	19	21

Table 3.3 shows the estimated memory size usage of KP-ABE and CP-ABE encryption. The memory size usage is estimated during the running process of encryption in the personal computer with 2.53GHz processor. KP-ABE requires lower memory usage as compared to CP-ABE. It is essential that the encryption process could be fast and provide sufficient security for the EHR. Lower memory usage is to reduce the computing power, thus extending the battery life of the computing device. It is also important that the ciphertext size should not be too large which would need more storage size and longer transmission time which is applicable for both store-and-forward and real-time transmission.

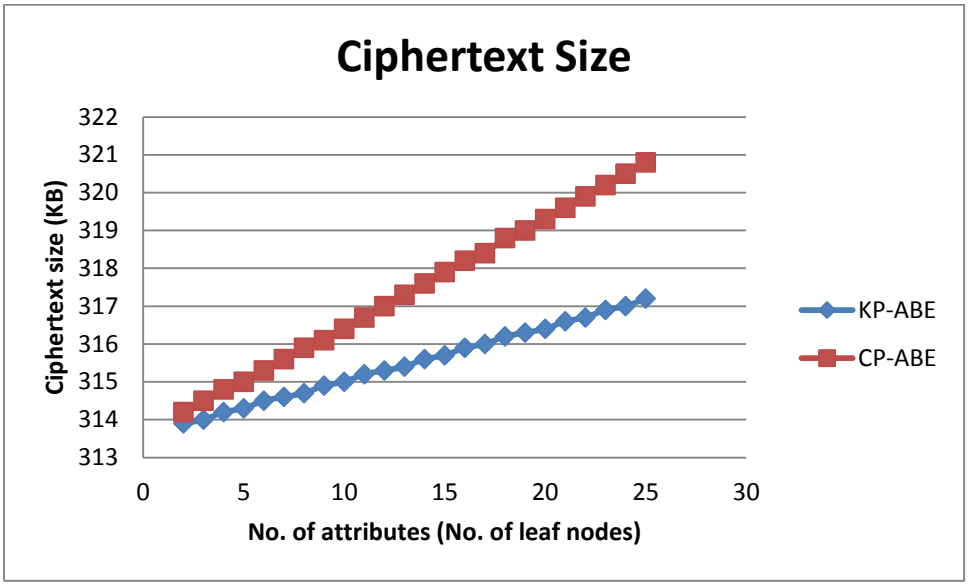


Figure 3.5: Ciphertext size of KP-ABE and CP-ABE

Figure 3.5 shows the ciphertext size of both KP-ABE and CP-ABE from the experiment carried out. Once each encryption process is completed by using different number of attribute/leaf nodes, the ciphertext size is captured. From the figure, as the KP-ABE encryption attributes increase, the ciphertext size will become larger. Also, for CP-ABE encryption, as the number of leaf nodes increase, the ciphertext size will also increase. However, from the comparison, CP-ABE ciphertext size is larger than KP-ABE ciphertext size. Therefore, KP-ABE scheme would be used as it would realize lightweight encryption and smaller ciphertext size which is suitable for resource constraint condition. For KP-ABE, the high complexity and processing work to embed the access policy in private keys will be done by the PKG. CP-ABE on the other hand, having the drawback of longer encryption computation time and larger ciphertext size. The encryption computation is heavier than KP-ABE because much processing

work of encryption is needed due to the embedded access policy in the ciphertext to be created in the patient's BSN.

3.4 Conclusions

Experiments have been carried out to estimate encryption time, decryption, private key generation time, ciphertext size and memory usage for encryption for KP-ABE and CP-ABE. From the experiment results, KP-ABE would be more suitable than CP-ABE to be deployed in a resource constraint device condition. However, encryption method should not be only limited to KP-ABE considering other conditions besides recourse constraint condition.

Table 3.4: Efficiency comparison between KP-ABE and CP-ABE

Experiments	**KP-ABE**	**CP-ABE**
Encryption time	✓	
Decryption time	✓	
Private Key generation time		✓
Memory usage for encryption process	✓	
Ciphertext size	✓	

Table 3.4 shows the summary of the experiment results comparing the efficiency between KP-ABE and CP-ABE. KP-ABE encryption time, decryption time is shorter, memory usage for encryption process is lower and ciphertext size is smaller than CP-ABE. CP-ABE on the other hand requires shorter private key generation time than KP-ABE. KP-ABE is selected as most suitable ABE in this research work.

CHAPTER IV

PROTOTYPE SYSTEM DESIGN AND ITS EXPERIMENTAL RESULTS

In this chapter, a prototype system design and its experimental results are discussed and the experimental results of the prototype are shown. The prototype handles only vital signs in order to confirm the basic performance of KP-ABE.

4.1 Prototype

A prototype is designed by attaching body sensor nodes to human body to record vital signs. Vital signs are then sent from the sensors to a personal computer (PC) via Bluetooth. These vital signs are encrypted using KP-ABE encryption algorithm and sent to the server. Authorized personnel (e.g. hospital professional and family members) are able to retrieve and decrypt the vital signs according to their access rights. Figure 4.1 shows the prototype system.

Figure 4.1: Prototype of BSN with KP-ABE on Indoor Mobile Healthcare System

4.1.1 Body Sensor Node

Body sensor node is a small, lightweight and wearable sensor platform. In the prototype, 2 types of sensors are used; electrocardiogram (ECG) sensor and accelerometer sensor. The function of ECG sensor is to record human's heart rate. The function of accelerometer sensor is to record the 3-dimensional motion of human body. The ECG and accelerometer sensors are manufactured by Realtime Technologies Ltd.

Figure 4.2 shows the conventional disposable electrodes. The ECG leads connect the sensor node to the conventional disposable electrodes as shown in Figure 4.3. Then, the disposable electrodes are attached to the human body as shown in Figure 4.4 to monitor the ECG. There are a few variants of ECG. The variants of ECG are 3-lead ECG, 5-lead ECG and 12-lead ECG [Cardogen M.]. The 3-lead ECG uses 3 or 4 ECG electrodes. The electrodes are LA (left arm), RA (right arm), LL (left leg) and RL (right leg), which is a neutral electrode. These basic electrodes yield enough information for heart rhythm-

monitoring. The 5-lead ECG uses 5 electrodes which are LA, RA, LL, LA and Chest. On another hand, 10 electrodes are required to produce 12-lead ECG. The electrodes are composed of electrodes on all 4 limbs (RA, LL, LA and RL) and electrodes on precordium (V1-V6). Precordium is the portion of the body over the heart and lower chest. 12-lead ECG enables interpretation of specific areas of the heart which are the inferior, lateral and anterior areas.

In the prototype, 3-lead ECG is implemented and the position of the electrodes are shown in Figure 4.4. However, the prototype does not restrict to only 3-lead ECG implementation. Figures 4.5 and 4.6 show a screenshot of motion data and ECG captured using the sensor node.

Figure 4.2: Disposable electrodes

Figure 4.3: ECG sensor node

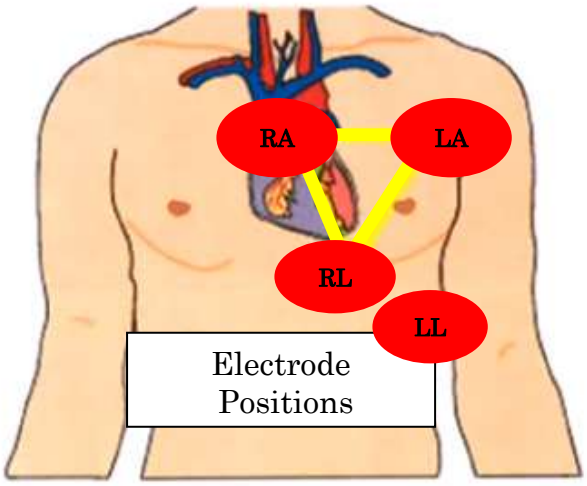


Figure 4.4: ECG leads placement on human body

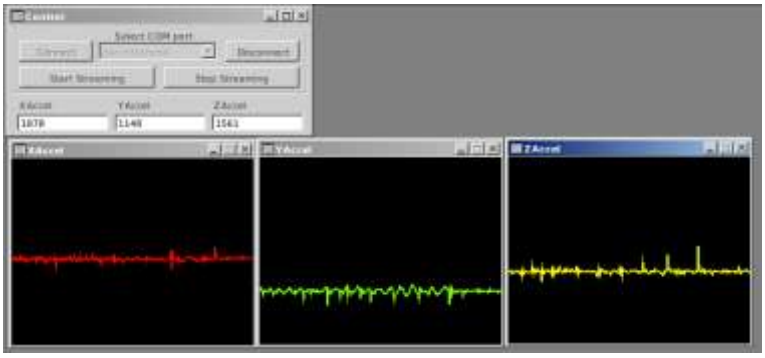


Figure 4.5: Screenshot of motion data

Figure 4.6: Screenshot of ECG data

4.1.2 Communication

The communication between sensor node and personal computer is conducted by Bluetooth. Covering radius of the Bluetooth in indoor is within 10m, which is under the class 2 Bluetooth device. The vital signs transmission from sensor node to the personal computer is protected by the security feature of Bluetooth called as Secure Simple Pairing (SSP). The SSP is a form of public key cryptography, where a public key and a private key are required. The communication between personal computer and cloud storage is via the Internet. The communication is protected by the transport layer security (TLS) and secure sockets layer (SSL) which are the cryptographic protocols that provide communication security over the Internet.

4.1.3 Personal Computer

Once the heart rate and 3D motions reading are recorded in the sensor node, the vital signs readings are sent to the patient's personal computer. The personal computer acts as a hub to collect all the vital signs and perform KP-ABE encryption. The scheme was implemented by using Charm framework

(Akinyele, J.A. et al., 2013). Charm is a framework for rapid cryptographic prototyping. The Charm framework helps to minimize development time and code complexity in the prototype development.

The KP-ABE scheme consists of four algorithms.

- Setup (1^k): The setup algorithm inputs a security parameter, 1^k and outputs the public parameters, *PK* and a master key, *msk* which is known only to the private key generator (PKG).
- Enc (*m, PK, γ*): The encryption algorithm inputs a message, *m*, a set of attributes, γ and the public parameters, *PK*. It outputs the ciphertext, *c*.
- KeyGen (*PK*, msk, *A*): The key generation algorithm inputs the public parameters, *PK*, the master key, *msk* and an access policy, *A*. It outputs the private key, D_A.
- Dec (*c*, *PK*, D_A): The decryption algorithm inputs the ciphertext, *c* which was encrypted under the set of attributes, *γ*, the public key parameters, *PK* and the private key, D_A for access control structure, *A*. It outputs the message *m* if $\gamma \in A$.

4.1.4 Cloud Storage Server

Cloud computing is a model for enabling ubiquitous and convenient access to a shared computing resources via internet. Cloud storage server is a model of networked enterprise storage where data is stored not only in the user's computer, but in virtualized pools of storage which are generally hosted by third parties as well. Medical data requires huge amount of data storage. Thus,

the cloud computing based healthcare service is able to provide economical, secure and global medical data sharing. Cloud storage services can be accessed through a web service application programming interface (API), a cloud storage gateway or through a Web-based user interface. Moreover, cloud storage services allow transfer, storing, access and sharing of files across different platforms and devices. Thus, allowing authorized personnel to have convenient access to the file at any time and at any locations with wired/wireless Internet connections.

As the EHR is encrypted before storing in the cloud storage server, they are protected from being accessed from any intruders including the cloud storage server administrator. On the other hand, the encrypted vital signs stored in the cloud storage are able to be flexibly shared among different authorized personnel (e.g. hospital professionals, patient, patient's and family members).

4.2 Vital sign transmission methods

There are two methods of transmission for vital signs. One is store-and-forward and other is real time.

Store-and-forward: Patients encrypt the vital signs and send them to the storage server at any time or any day as shown in Figure 4.7.

Store-and-forward transmission mechanism:

1. Vital signs are sent from BSN coordinator to PC.
2. PC assembles the vital signs and save them in a file.

3. PC encrypts the file and sends to server at certain time period. Encryption can be done either by hand-operated or self-starting.
4. Hospital personnel retrieve the encrypted vital signs and perform decryption to regenerate the original vital signs.

In the prototype system, store-and-forward medical data encryption can be performed in two ways.

- Hand-operated: Encryption is manually performed by patient in a direct manner.
- Self-starting: Encryption is performed automatically by the system at a certain time period (e.g. hourly basis, daily basis, weekly basis or certain time of the day in a week). Time for medical data transmission period can be flexibly changed accordingly.

Real-time: Patients' vital signs are encrypted and sent to storage server at a continuous basis as shown in Figure 4.8.

Real-time transmission mechanism:

1. Vital signs are sent from BSN coordinator to PC.
2. PC receives the vital signs packets and encrypts the vital signs.
3. Encrypted vital signs packets are sent to server packet by packet basis.
4. Hospital personnel retrieve the encrypted vital signs and perform decryption to regenerate the original vital signs.

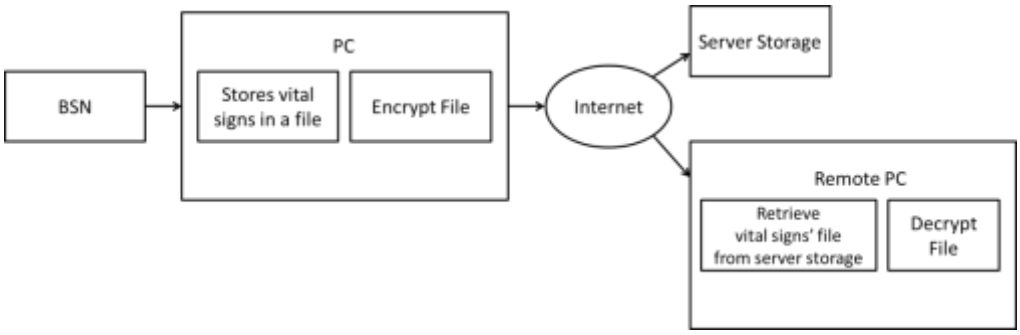


Figure 4.7: Store-and-forward encryption tansmission

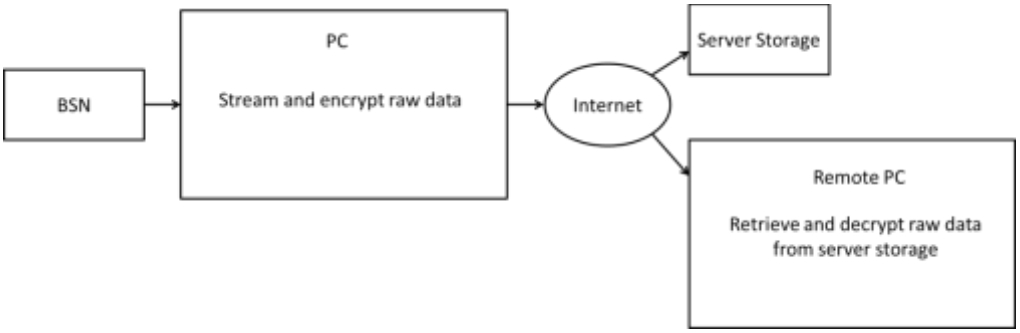


Figure 4.8: Real-time encryption transmission

Table 4.1: Store-and-forward vs. real-time encrypted data transmission

Features	**Store-and-forward**	**Real-time**
Data Type	File	Packet
Encryption Basis	Hourly, daily, weekly, monthly	Every few seconds according to the sample rate.

Table 4.1 shows the comparison of store-and-forward and real-time encryption of the prototype in terms of their data type and encryption basis. For store-and-forward encryption, vital signs are being collected for a period of time in a file and then encrypted in an hourly, daily, weekly or monthly basis. For real-time encryption, vital signs are sent packet by packet basis in every few seconds according to the sampling rate.

4.3 Results of Experiment

This section shows and discusses the experimental results of the BSN prototype. Following sub-sections show the conditions to carry out the experiment and results of the experiment. The results shown are correct encryption and decryption as well as the incorrect encryption and decryption.

4.3.1 Experimental conditions for KP-ABE and CP-ABE

The experiment is carried out under a set of conditions. The conditions considered are Bluetooth distance, movement of the subject, Bluetooth transmission condition and number of repetition to confirm the correct/incorrect encryption/decryption.

Experiment conditions are;

(1) Bluetooth distance: Within 10 meters

(2) Number of repetitions to confirm correct/incorrect encryption/decryption: 30 repetitions

(3) Movement of the subject : From one location to another within 10 meters inside a house

(4) Bluetooth transmission disturbance condition: Wall and door (interference) between BSN and PC.

(5) Sensor data rate (Throughput): 50Hz, 1.2kpbs

4.3.2 Attribute and Access Structure

Fine-grained sharing of vital signs experiment was being carried out by issuing a few set of private keys embedded with different set of access policy. Private

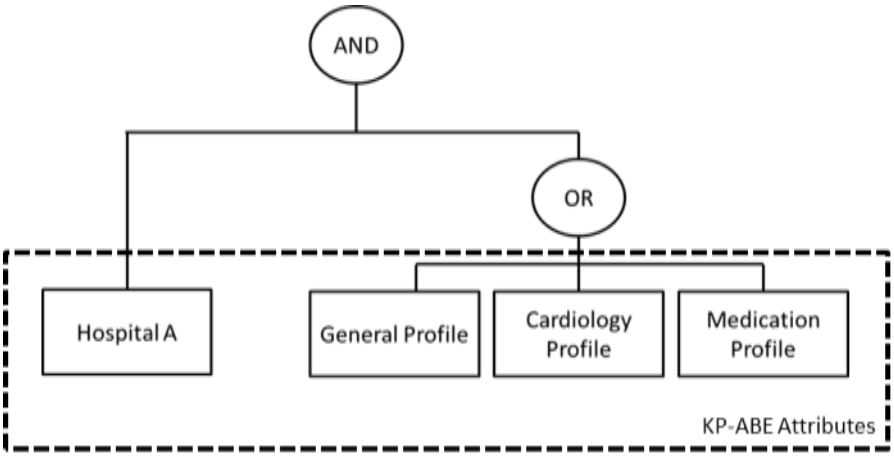
keys that hold the set of access policy that matched with the set of attributes of the encrypted vital signs perform successful decryption. Contrary, private keys which hold a set of access policy that mismatched with the set of attributes of encrypted vital signs are not able to decrypt the ciphertext. Hence, sharing of encrypted vital signs could be more efficiency among different healthcare professionals.

Defining a proper attributes set and access structure is essential to build an efficient ABE-based BSN system. This section presents the attributes set and access structure for both KP-ABE and CP-ABE.

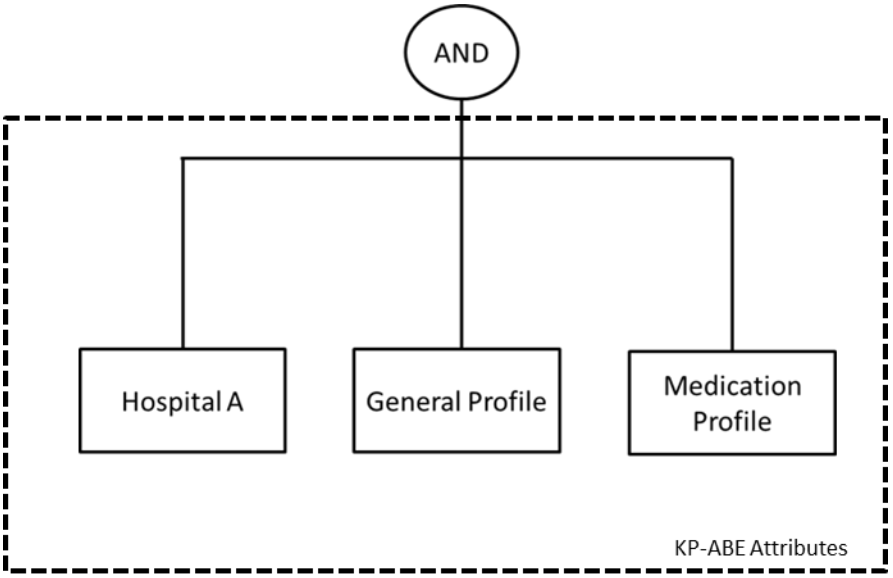
KP-ABE Attribute and Access Structure

In this dissertation, the attributes universe $\mathcal{U}$ is defined with a set of attributes. The attribute sets of KP-ABE are record based such as general profile, cardiology profile, and medication profile.

As for access structure, each access structure defines the authority of individual healthcare professionals. For example, cardiology doctor is granted access to medical record labelled as general, cardiology and medication profile. Nurse and pharmacist are granted the access to the medical record which is labelled as general and medication profile. Besides that, each medical professional is also restricted by location where the medical professionals can only access the medical records of the patients of the hospital they are working for. The access structures for medical professionals are shown in Figure 4.9.



(a) Access structure of cardiology doctor



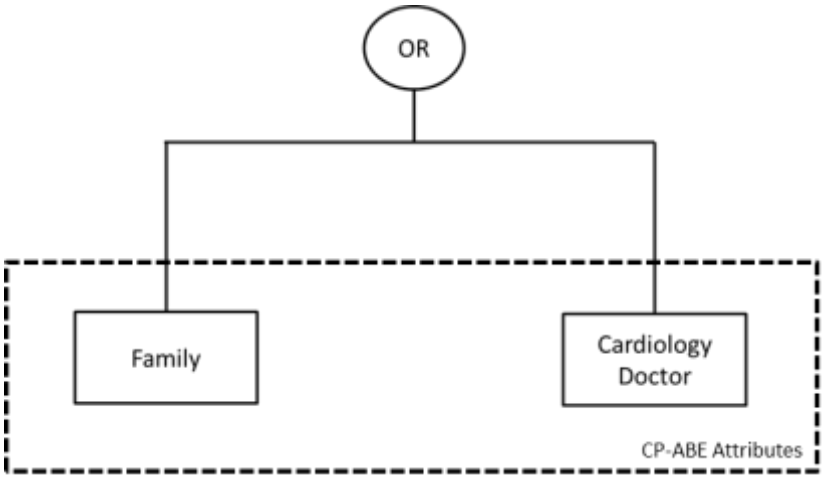
(b) Access Structure of Nurse and Pharmacist

Figure 4.9: KP-ABE Access Structures

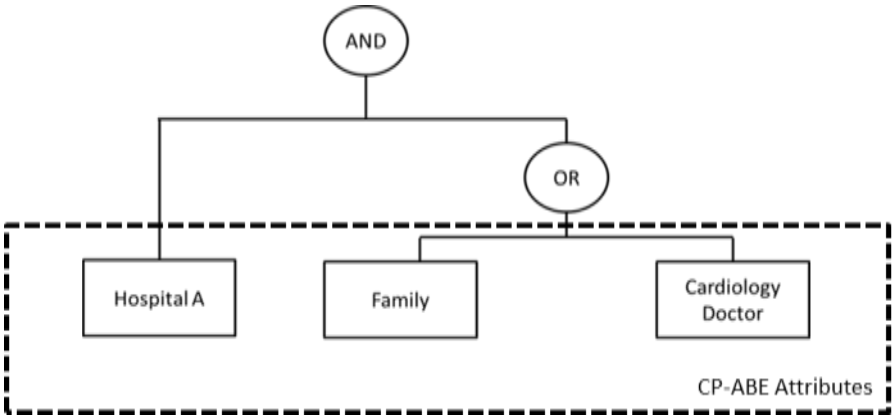
CP-ABE Attribute and Access Structure

The attributes set of CP-ABE is defined by role based with the used of the role information of each individual such as cardiology doctor, nurse, pharmacist and family.

For CP-ABE access structure, each access structure determines the authorized personnel who is able to access the medical records. For example, patient Joel may want to grant access of his cardiology record to his family and to his cardiology doctor only. Therefore, Joel's family and all cardiology doctors without restrictions at any stated hospital could access to Joel's cardiology record. However, if Joel would like to grant access right to cardiology doctor in Hospital A only, the access structure can be altered to restrict cardiology doctor from other hospital to access to Joel's cardiology record as shown in Figure 4.10.



(a) Access structure of cardiology record for any cardiology doctor



(b) Access structure of cardiology record for Hospital A's cardiology doctor

Figure 4.10: CP-ABE Access Structures

4.3.3 Correct Encryption and Decryption

Figure 4.11 shows the screenshot of the work. The vital signs are being encrypted with a set of attributes at the patient's site and then sent to remote server site. The decryption is successful where the access policy embedded in the private key matches the attributes encrypted in the vital signs.

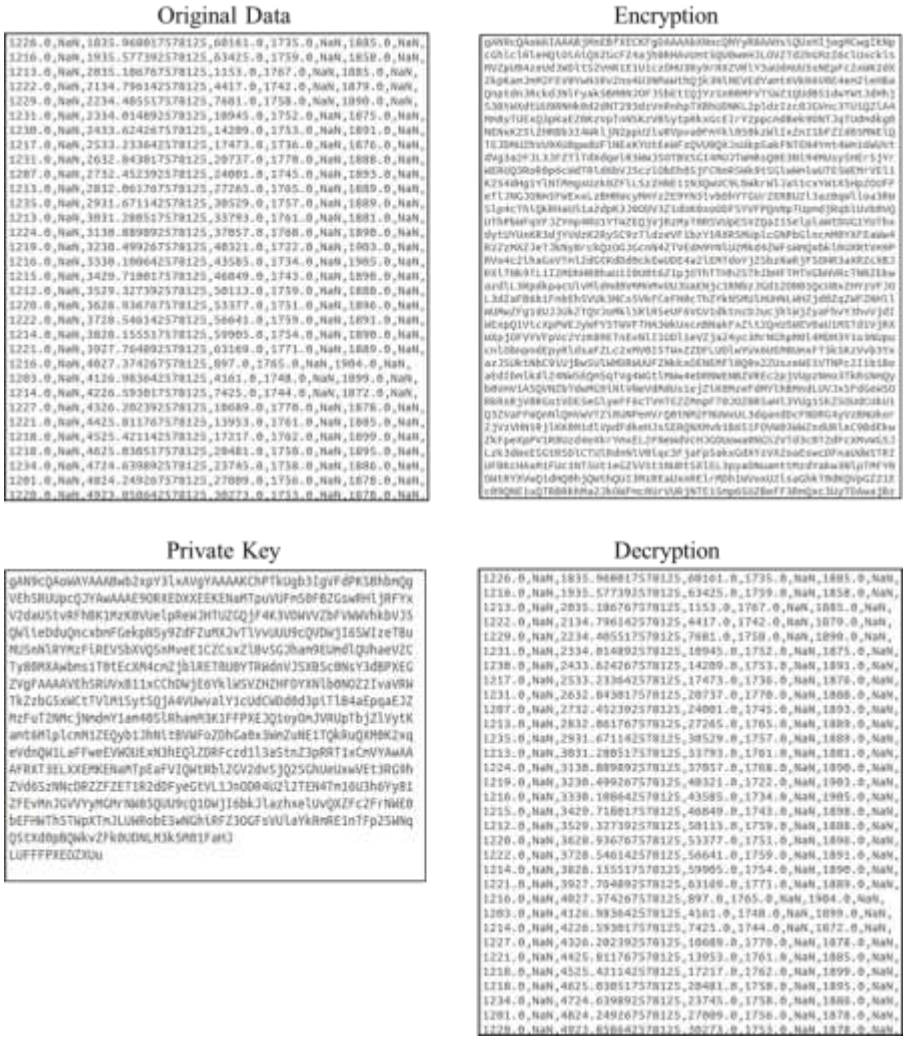


Figure 4.11: Screenshot of correct encryption and decryption

4.3.4 Decryption using Incorrect Private Key

From the screenshot shown in Figure 4.12, the encrypted vital signs are being decrypted with an incorrect private key. The original vital signs cannot be reconstructed as the embedded access policy in the private key does not satisfy the attributes encrypted in the vital signs.

Figure 4.12: Screenshot of encrypted data and decrypted data using incorrect private key

4.4 Conclusions

Experiment is carried out under a set of conditions to confirm working condition of the BSN prototype. The confirmed performances by the BSN prototypes are;

(1) Vital sign transmission by store-and-forward and real-time.

(2) Validity of KP-ABE to ensure patient's security and privacy.

(3) Sharing encrypted data only by certain authorized healthcare professionals.

CHAPTER V

BSN FRAMEWORK IN TELEMEDICINE NETWORK AND ITS PROPOSED DESIGN WITH INTERNATIONAL STANDARDS

This chapter discusses the BSN framework in telemedicine network and its proposed design with international standards. The placement of BSN framework in telemedicine network is necessary to clarify the BSN in telemedicine network. Besides that, it is also indispensable to realize extensibility of the BSN which guarantees changes of various BSN parameters due to the conveniences of patients, healthcare providers, and other telemedicine relevant network nodes. For these purposes, it is required to define BSN functional blocks, functional interface reference points between BSN functional blocks and finally to apply the existing international standards to relevant BSN framework interface reference points.

5.1 BSN Framework in Telemedicine Network

BSN framework is composed of four main nodes which are the sensor node, healthcare professional node, storage server node and healthcare authority node (or private key generator node). The BSN framework is defined by these four main nodes. The nodes are interconnected by the Internet. The entire network configuration composed of the above nodes is referred to as telemedicine network. The attribute based encryption is designed and developed at the application layer of the Internet protocol. Figure 5.1 shows the BSN framework in telemedicine network.

5.2 Details of the Proposed BSN Framework Defined in Telemedicine Network

The BSN framework in Figure 5.1 is composed of BSN node, storage server node, healthcare provider node and healthcare authority node. Other nodes can be connected to the telemedicine network according to the requirements of telemedicine. However, in the proposed BSN framework, discussion is confined to the EHR encryption and access, private key distribution, attribute/access policy updates and healthcare professional addition and revocation.

5.2.1 EHR Encryption and Access

Vital signs are picked up by patient's body sensors. Patient's EHR is to be encrypted under a set of attributes for the hospital professionals to access under a certain access policy. Patient then uploads the attribute-based encrypted EHR to the storage server node. Only the authorized hospital professionals at healthcare provider node are allowed to access and decrypt encrypted EHR.

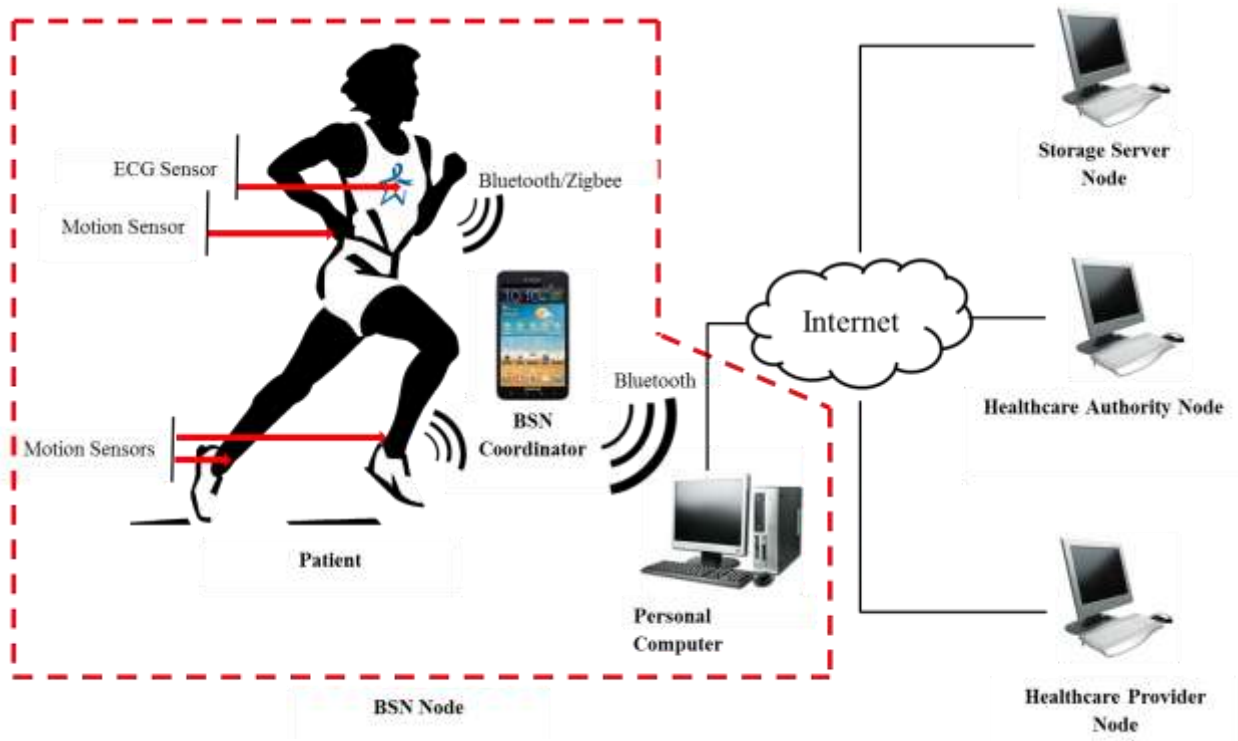


Figure 5.1: BSN framework in telemedicine network

5.2.2 Private Key Distribution

The BSN framework defines universal attributes for every patient. Healthcare authority node generates a set of corresponding public and master keys for each patient. The public keys can be published via telemedicine network. On the other hand, private key of the healthcare professionals can be obtained from the healthcare authority node. The healthcare authority node determines the access policy then generates the private key to the healthcare professional based on the identities/role of healthcare professionals. For example, a healthcare professional would receive {("General Doctor" AND "Specialist") AND ("Kuala Lumpur" OR "Penang") OR "Medical Experience>20years" OR "Name: Dr.Hosanna"} as his or her access policy embedded in the private key.

5.2.3 Attribute/Access Policy Updates

Patients can update the sharing of the existing EHR by updating the attribute in the ciphertext. The operations which may include modification, deletion or addition of attribute can be done by the healthcare authority node on behalf of the patient. For example, if a patient does not allow nurse to have access to his or her encrypted EHR, the patient can remove/delete the attribute "nurse" from his or her ciphertext attributes.

5.2.4 Healthcare Professional Addition and Revocation

The addition of a healthcare professional is possible when the healthcare professional obtains his/her private key from the healthcare authority node. The revocation here considers the revocation of healthcare professionals' private key. Lewko, Sahai and Waters's revocation system (Lewko, Sahai & Waters,

2010) is adapted in the user revocation of ABE. The idea of revocation is as follows. The encryption algorithm creates an encryption with a revocation set $S = ID_1, \dots, ID_r$ of r identities. Then it creates an exponent $s \in \mathbb{Z}_p$ and split r random shares $s_1, \dots, s_r$ such that $\sum s_i = s$. Ciphertext is then created such that any user key with $ID = ID_i$ will not be able to decrypt the ciphertext. ID is embedded in the private key during the private key generation.

5.3 Functional Blocks Definition with Relevant Interface Reference Points in BSN Framework

Figure 5.2 shows the functional blocks associated with their interface reference points at the BSN node. Figure 5.3 summarizes BSN framework diagram with relevant functional nodes and their interfaces reference points between functional nodes in the telemedicine network. The functional nodes are interconnected to each other by the Internet. The information exchanges between the blocks are shown in Table 5.1. Table 5.1 creation is necessary to apply international standards at functional interface points.

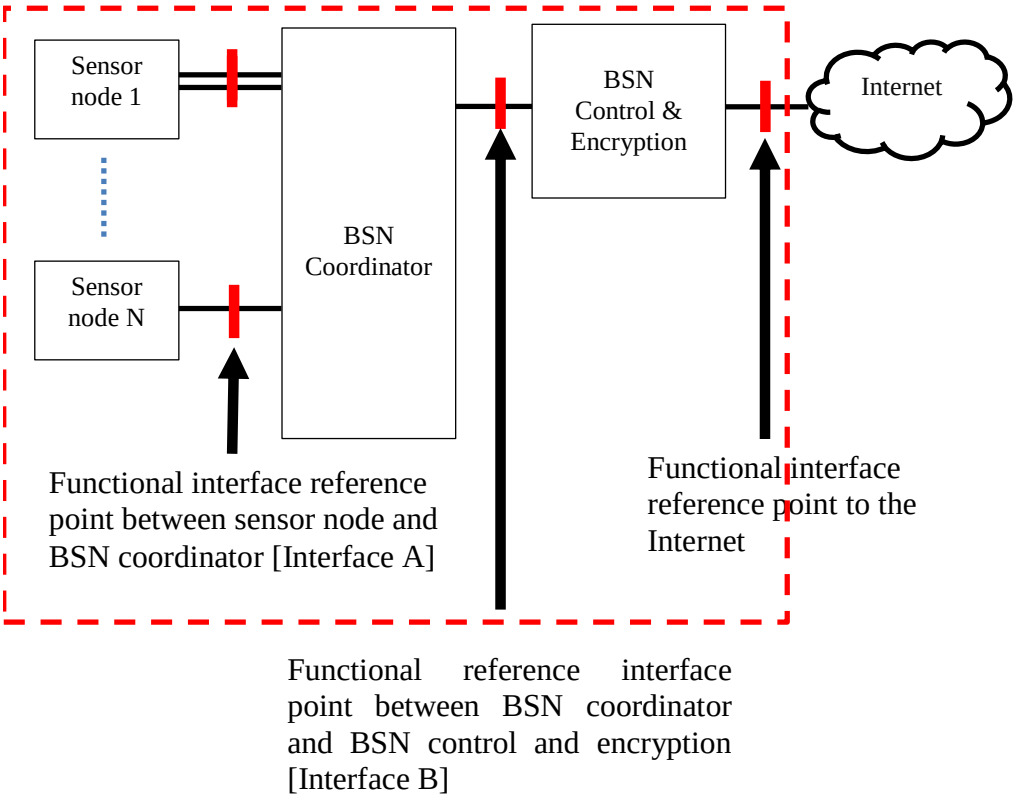


Figure 5.2: Functional block diagram and relevant interface reference points at BSN node

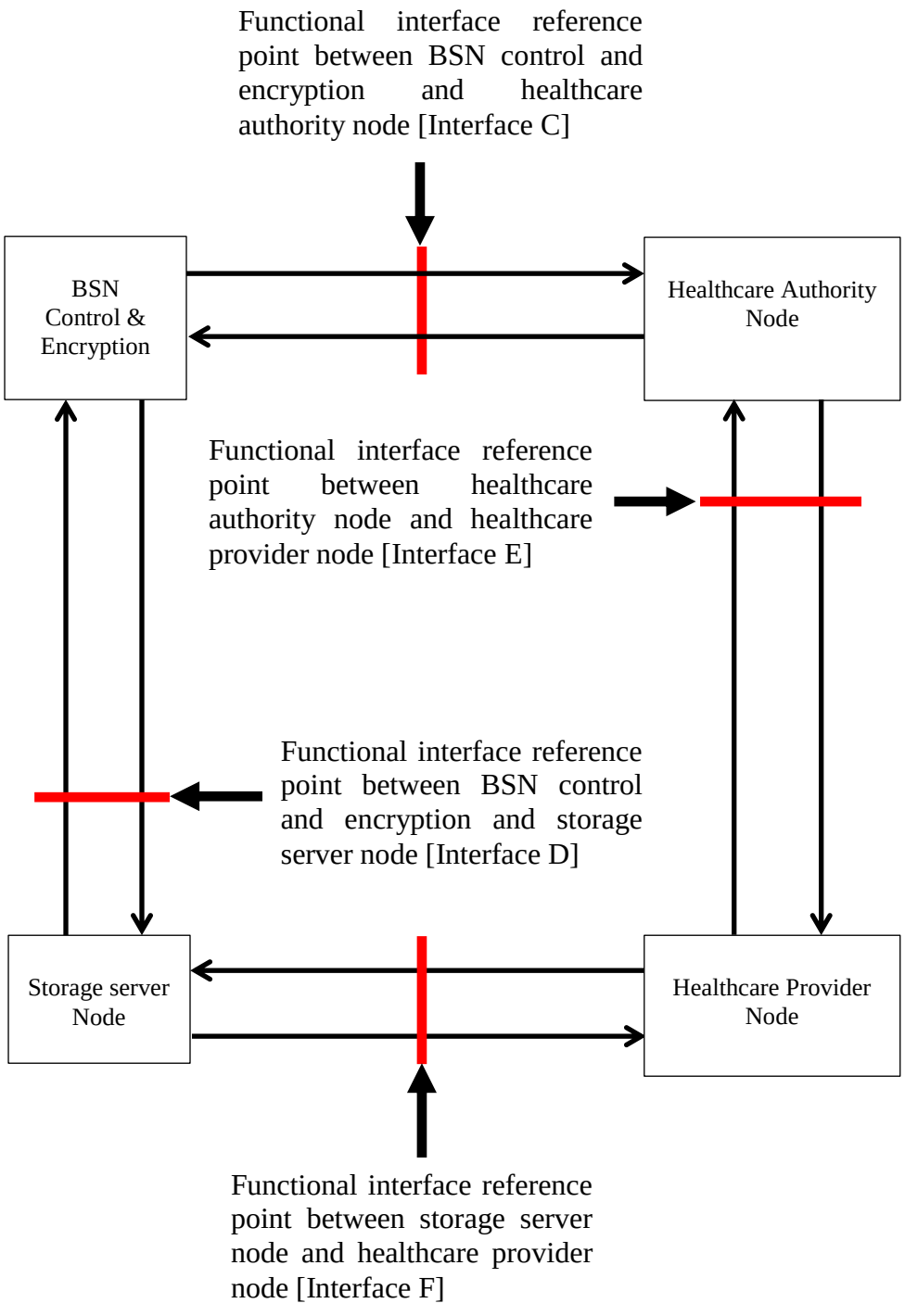


Figure 5.3: Functional block diagram BSN framework with relevant interface reference points in the telemedicine network

Table 5.1: Information exchange across the functional interface reference points

Interface name	Information exchange across the interface reference point	Information direction
Interface A	Sensor node activation	From BSN coordination to sensor node
	Sensor node activation confirmation	From sensor node to BSN coordination
	Sensor node deactivation	From BSN coordination to sensor node
	Sensor node deactivation confirmation	From sensor node to BSN coordination
Interface B	BSN coordination activation	From BSN control and encryption to BSN coordination
	BSN coordination activation confirmation	From BSN coordination to BSN control and encryption
	Sensor node deactivation	From BSN control and encryption to BSN coordination
	Sensor node deactivation confirmation	From BSN coordination to BSN control and encryption
	Raw vital sign and patient data transmission	From BSN coordination to BSN control and encryption
Interface C	Request for modification or updates on attributes or access policy	From BSN control and encryption to healthcare authority node
	Change or update the attributes or access policy for EHR encryption	From BSN coordination to BSN control and encryption
Interface D	Transmission of encrypted EHR	From BSN control and encryption to storage server node
	Retrieval of encrypted EHR	From storage server node to BSN control and encryption
Interface E	Private key retrieval request by using healthcare professional identity	From healthcare provider node to healthcare authority node
	Healthcare professional identity confirmation and issuance of private key	From healthcare authority node to healthcare provider node
Interface F	EHR retrieval request	From healthcare provider node to storage server node
	Transmission of EHR	From storage server node to healthcare provider node

5.4 International Standard Interface Examples to be Applied at Functional Interface Reference Points

This section shows the international standards to be applied at BSN framework functional interface reference points. Table 5.2 illustrates international standards to be applied to functional interface reference points at BSN node.

Table 5.2: International standards to be applied at BSN node functional interface reference points

<table>
<tr><th>Functional block</th><th>Physical entity example</th><th>International standard interface</th></tr>
<tr><td>Sensor node</td><td>ECG, Motion sensor</td><td rowspan="2">Between sensor node and BSN coordinator

- Zigbee, Bluetooth, IEEE802.15.6</td></tr>
<tr><td rowspan="2">BSN coordinator</td><td rowspan="2">Smartphone</td></tr>
<tr><td rowspan="2">BSN control and encryption</td><td rowspan="2">Personal computer</td><td>Between BSN coordinator and BSN control and encryption

- Bluetooth, Wireless LAN [IEEE802.11]</td></tr>
<tr><td rowspan="2">Internet</td><td rowspan="2">Wired/wireless LAN card</td><td rowspan="2">Between BSN control and encryption to the Internet

- Wired/Wireless LAN [IEEE802.11]</td></tr>
</table>

5.5 Variable Parameters in BSN Framework

The variable parameters in BSN for each functional block/interfaces are shown in Table 5.3. The parameters could be changed by healthcare authority accordingly at each functional block.

Table 5.3: Variable parameters in BSN framework

Functional block	Variable parameter
BSN coordinator	- Type of sensors - Number of sensors - Addition/deletion of sensors
BSN control & encryption	- Encryption methods
Healthcare authority node	- Attribute assignments/updates
Storage server node	- Storage size assigned to patients
Healthcare provider node	- Role/position (e.g. nurse, pharmacist, specialist) - Addition/revocation of healthcare provider

5.6 Data Transmission Frame Format

Various international standards are used in the transmission of data from one functional block to another. IEEE 802.15.1, Bluetooth (Madhavapeddy, A., and Tse, A., 2005) standard is used for the transmission of data from sensor node to BSN coordinator node and from BSN coordinator node to BSN control and encryption node.

Figure 5.4: Bluetooth transmission data frame

Figure 5.4 shows a Bluetooth transmission data frame format. Each data frame supports one sensor data. Therefore, the data frame is being sent continuously for every vital sign collected. This data frame format supports various types of sensor data and it provides enhanced reliability to the data transmission through packet sequence numbers and a cyclic redundancy check.

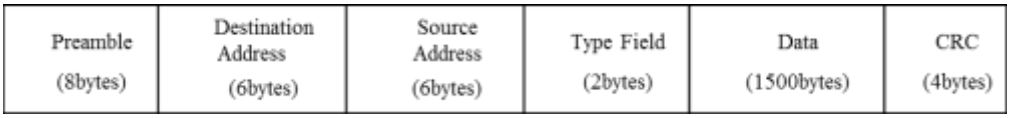


Figure 5.5: IEEE 802.3 Ethernet frame

The BSN control and encryption node then put together the sensor nodes data and encrypt the data. Then, the Bluetooth frame format is mapped on IEEE 802.3 Ethernet frame (Postel, J., and Reynolds, J. K., 1988; Christensen, K. et al., 2010) shown in Figure 5.5. Destination address of the Ethernet frame is the address of the healthcare provider node whereas the source address is the address of BSN node. The data in the Ethernet frame is then mapped on the IP frame format which then is transported using the standard Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) protocols. TCP is used for the transmission of patient's healthcare record. UDP on the other hand is for the transmission of vital sign waveform such as the ECG waveform.

5.7 Extensibility of the BSN framework

Extensibility of the BSN framework is necessary to meet the requirements for larger number of people using the system. With the growing number of users, room for expansion would be required to maintain the efficiency of the system.

Moreover, the BSN framework should allow addition of more functional nodes to cater for different sectors beside the healthcare provider. Table 5.4 shows the prospective extensibility of the BSN framework according to the functional block. Figure 5.6 shows the generic functional block diagram of the BSN framework with additional functional blocks.

Table 5.4: Prospective extensibility of the BSN framework

Functional block	Prospective BSN extensibility
BSN node	- Addition and reduction of number of sensors on a patient - More than one patient's vital signs can be captured and encrypted at home
Healthcare Provider node	- Addition and reduction of number of experts or specialities
Healthcare Authority node	- Addition of healthcare authority
Storage server node	- Storage size of the server. - Server site
Other nodes	- Different sectors (e.g. Insurance sector)

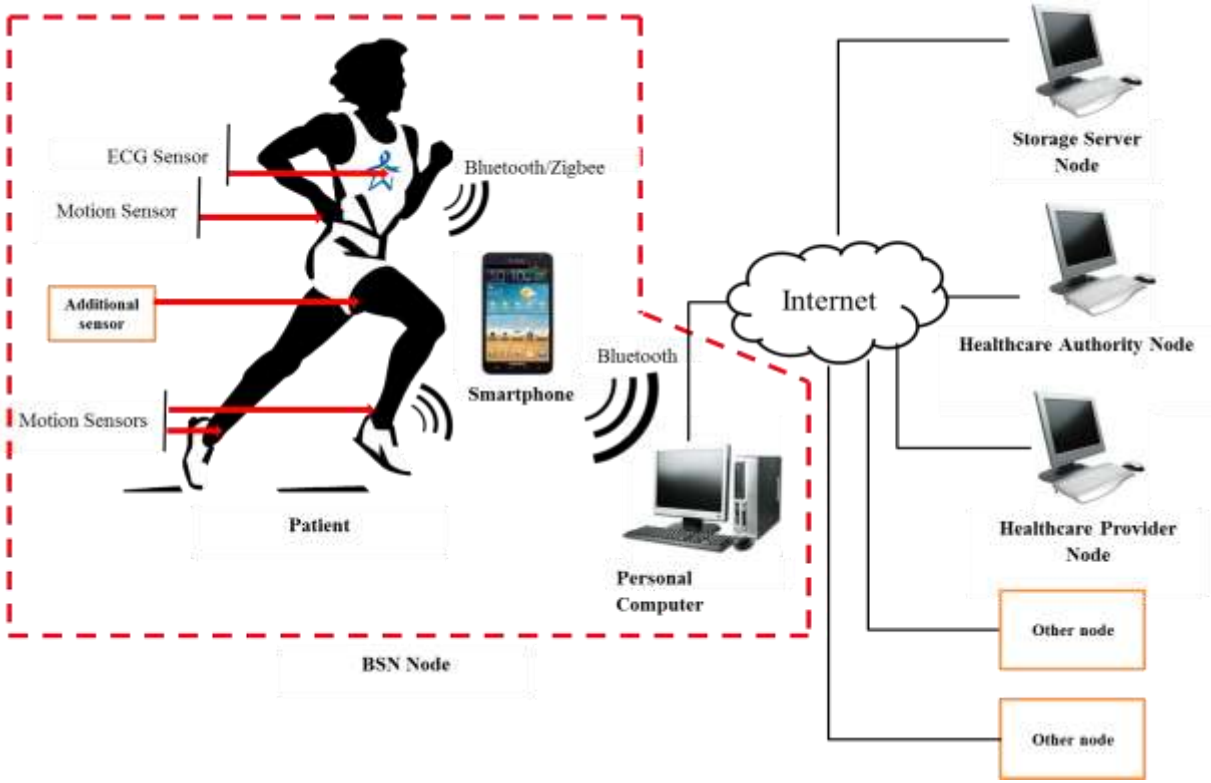


Figure 5.6: Generic BSN framework in telemedicine network with additional nodes

5.8 BSN Framework Design using Proposed International Standards

The proposed international standard in the BSN framework design are IEEE 802.15.1 Bluetooth, IEE802.11 WLAN, Health Level 7 (HL7) (Quinn, J., 1999; Tracy, W. R., and Dougherty, M., 2002.), and Medical waveform Format Encoding Rules (MFER) (Kimura, E., Norihiko, T., and Ishihara, K., 2006) as shown in Figure 5.7. Bluetooth (IEEE 802.15.1) standard is used in the transmission from one device to another within the BSN node.

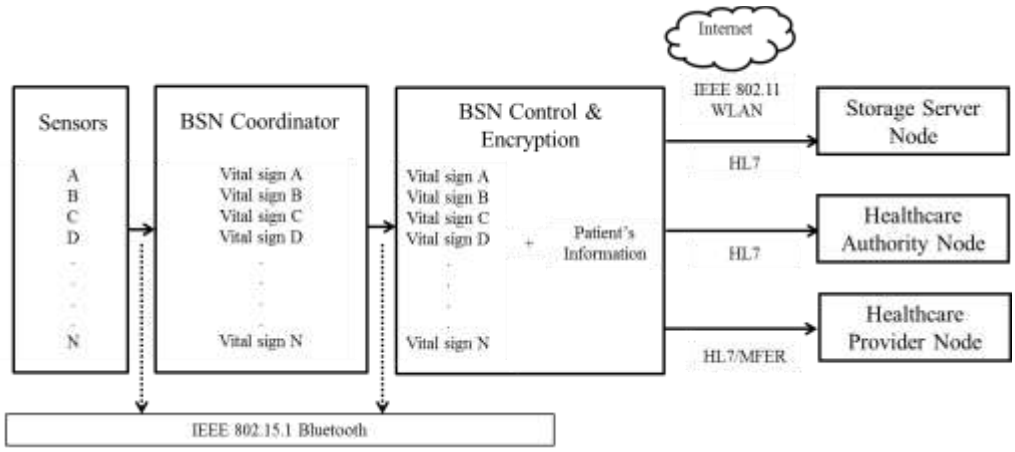


Figure 5.7: Proposed international standards for BSN framework design

HL7 is an international healthcare standard for the sharing, exchange, integration, and retrieval of patient's health record. HL7 standard can be deployed in server storage node in the BSN framework where patients keep records of their EHR. Healthcare provider node typically has many different computer systems used. All of these systems should communicate/interface with each other when new information is receive/updated. Thus, HL7 specifies some standards, methodologies, and guidelines where various healthcare systems can communicate with each other. Such guidelines or data standards enable information to be shared and processed in a consistent manner. These

data standards are set to bring convenience for healthcare organizations to easily share EHR.

MFER is specialized in the encoding and transmission of medical waveforms which includes the encoding and transmission of ECG. Besides ECG, MFER also supports waveforms such as EEG, and respiratory waveforms. MFER standard can be deployed in the transmission of waveform from BSN node to healthcare provider node.

5.9 Conclusions

A BSN framework is designed together with proposed international standards. Change of variable parameters and the extensibility of the BSN framework by adding relevant new nodes enable the BSN framework to evolve according to the requirements of users based on international standards. Furthermore, today's global penetration of medical tourism has accelerates its necessity. This is because the medical tourist might need continuous monitoring after returning to their mother lands.

CHAPTER VI

CONCLUSIONS AND FUTURE WORKS

This research work is carried out with the intention to protect the privacy and confidentiality of the vital signs captured by the body sensor nodes before sending it to a remote server for patients' EHR storage. In order to keep the vital signs protected, encryption is one of the potent ways. On the other hand, availability of sharing encrypted vital signs to different healthcare professionals at a fine-grained level is also essential and practical. Hence, the deployment of attribute-based encryption scheme has been studied in this dissertation. The BSN prototype is designed and built to confirm the above mentioned feasibility. Subsequently, a BSN framework with international standard is proposed.

6.1 Conclusions

1. Adoption of ABE encryption scheme for its high security performance and fine-grained sharing of EHR. Comparisons between KP-ABE and CP-ABE have been performed exhaustively and KP-ABE is selected for the most appropriate encryption and fine-grained sharing for the BSN data.

2. Design and deployment of a BSN prototype. The BSN prototype is successfully built for the working confirmation of patient's vital signs transmission using KP-ABE scheme by experiment.

3. BSN framework design proposal using international standards. In the proposed framework design, the extensibility of the BSN is taken into consideration. Besides that, with the proposed international standard, BSN framework can be evolved according to the needs of users and global evolution of the medical tourism.

6.2 Future works.

1. Security analysis for the combination of the security scheme and algorithms used on the BSN framework in the current work. The ABE schemes and algorithms used in the framework are proven to be secure theoretically. Thus, the ABE schemes and algorithms are assumed to be secured. Therefore, security analysis could be carried out to prove the framework security practically.

2. Encryption of EHR using smartphone. The current BSN prototype uses the personal computer to perform encryption of EHR. For future work, the EHR encryption could be done directly in the smartphone instead of using the personal computer.

3. Implementation of EHR in the smartphone. To implement EHR composed of HL7 and MFER in the smartphone technology would be necessary.

4. Data archiving of EHR. This includes matters of; ownership of EHR, legal issues and openness of the archive.

REFERENCES

Perednia, D.A. and Allen, A., 1995. Telemedicine technology and clinical applications. *JAMA: the journal of the American Medical Association*, 273(6), pp. 483-488.

Güler, N.F. and Übeyli, E.D., 2002. Theory and applications of telemedicine. *Journal of Medical Systems*, 26(3), pp. 199-220.

Ekeland, A.G., Bowes, A. and Flottorp, S., 2010. Effectiveness of telemedicine: a systematic review of reviews. *International journal of medical informatics*, 79(11), pp. 736-771.

Harnett, B., 2006. Telemedicine systems and telecommunications. *Journal of telemedicine and telecare*, 12(1), pp. 4-15.

Hailey, D., Ohinmaa, A., Roine, R., 2004. Study quality and evidence of benefit in recent assessments of telemedicine. *Journal of telemedicine and telecare*, 10(6), pp. 318-324.

Marilyn, J.F., 1996. *Telemedicine: A Guide to Assessing Telecommunications for Health Care*, 1st edn. National Academies Press, Washington, D.C.

High, W.A. et al., 2000. Assessment of the accuracy of low-cost store-and-forward teledermatology consultation. *Journal of the American Academy of Dermatology*, 42(5), pp. 776-783.

Istepanian, R.S., Jovanov, E. and Zhang, Y.T., 2004. Guest editorial introduction to the special section on m-health: Beyond seamless mobility and global wireless health-care connectivity. *Information Technology in Biomedicine, IEEE Transactions*, 8(4), pp. 405-414.

Lo, B., Thiemjarus, S., King, R. and Yang, G.Z., 2005. Body sensor network-a wireless sensor platform for pervasive healthcare monitoring. *The 3rd International Conference on Pervasive Computing*, 13, pp. 77-80.

Otto, C. et al., 2006. System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia*, 1(4), pp. 307-326.

Ko, J. et al., 2010. Wireless sensor networks for healthcare. *Proceedings of the IEEE*, 98(11), pp. 1947-1960.

Timmons, N.F. and Scanlon, W.G., 2004. Analysis of the performance of IEEE 802.15. 4 for medical sensor body area networking. *Sensor and ad hoc communications and networks, IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference*, pp. 16-24.

Lo, B., Thiemjarus, S., King, R. and Yang, G.Z., 2005. Body sensor network-a wireless sensor platform for pervasive healthcare monitoring. *The 3rd International Conference on Pervasive Computing*, 13, pp. 77-80.

Astrin, A.W., Huan-Bang, L.I. and Kohno, R., 2009. Standardization for body area networks. *IEICE transactions on communications*, 92(2), pp. 366-372.

Martelli, F., Buratti, C. and Verdone, R., 2011. On the performance of an IEEE 802.15. 6 wireless body area network. *Wireless Conference 2011-Sustainable Wireless Technologies (European Wireless), 11th European*, pp. 1-6.

Shamir, A., 1985. Identity-based cryptosystems and signature schemes. *Advances in cryptology*, pp. 47-53.

Boneh, D. and Franklin, M., 2001. Identity-based encryption from the Weil pairing. *Advances in Cryptology—CRYPTO 2001*, pp. 213-229.

Sahai, A. and Waters, B., 2005. Fuzzy identity-based encryption. *Advances in Cryptology–EUROCRYPT 2005*, pp. 457-473.

Goyal, V., Pandey, O., Sahai, A. and Waters, B., 2006. Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89-98.

Bethencourt, J., Sahai, A. and Waters, B., 2007. Ciphertext-policy attribute-based encryption. *Security and Privacy, 2007. SP'07. IEEE Symposium*, pp. 321-334.

Bao, S.D., Poon, C.C., Zhang, Y.T. and Shen, L.F., 2008. Using the timing information of heartbeats as an entity identifier to secure body sensor network. *Information Technology in Biomedicine, IEEE Transactions*, 12(6), pp. 772-779.

Sun, J. and Fang, Y., 2010. Cross-domain data sharing in distributed electronic health record systems. *Parallel and Distributed Systems, IEEE Transactions*, 21(6), pp. 754-764.

Zhang, G.H., Poon, C.C. and Zhang, Y.T., 2012. Analysis of Using Interpulse Intervals to Generate 128-Bit Biometric Random Binary Sequences for Securing Wireless Body Sensor Networks. *Information Technology in Biomedicine, IEEE Transactions*, 16(1), pp. 176-182.

Benaloh, J., Chase, M., Horvitz, E. and Lauter, K., 2009. Patient controlled encryption: ensuring privacy of electronic medical records. *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 103-114.

Tan, C.C., Wang, H., Zhong, S. and Li, Q., 2008. Body sensor network security: an identity-based cryptography approach. *Proceedings of the first ACM conference on Wireless network security*, pp. 148-153.

Akinyele, J.A. et al., 2013. Charm: A framework for rapidly prototyping cryptosystems. *Journal of Cryptographic Engineering*, 3(2), pp. 111-128.

Lewko, A., Sahai, A., and Waters, B., 2010. Revocation systems with very small private keys. *IEEE Symposium on Security and Privacy*, pp. 273-285.

Madhavapeddy, A., and Tse, A., 2005. A study of bluetooth propagation using accurate indoor location mapping. *UbiComp 2005: Ubiquitous Computing*, pp. 105-122.

Postel, J., and Reynolds, J. K., 1988. Standard for the transmission of IP datagrams over IEEE 802 networks.

Christensen, K. et al., 2010. IEEE 802.3 az: the road to energy efficient ethernet. *Communications Magazine, IEEE*, 48(11), pp. 50-56.

Quinn, J., 1999. An HL7 (Health Level Seven) overview. *Journal of AHIMA/American Health Information Management Association*, 70(7), pp. 32-34.

Tracy, W. R., and Dougherty, M., 2002. HL7 standard shapes content, exchange of patient information. *Journal of AHIMA/American Health Information Management Association*, 73(8), pp. 48-51.

Kimura, E., Norihiko, T., and Ishihara, K., 2006. Development MFER (medical waveform format encoding rules) parser. *Proceedings of American Medical Informatics Association Annual Symposium*, pp. 985.

Akinyele, J.A. et al., 2010. Securing electronic medical records using attribute-based encryption on mobile devices. *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, pp. 75-86.

Ibraimi, L., Asim, M., and Petkovic, M., 2009. Secure management of personal health records by applying attribute-based encryption. *Wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop*, pp. 71-74.

Hu, J., Chen, H. H., and Hou, T. W., 2010. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. *Computer Standards & Interfaces*, 32(5), pp. 274-280.

Sec 2: Recommended Elliptic Curve Domain Parameters, 2010. Available from: < http://www.secg.org >. [January 2010].