Privacy-Preserving Access Control Model for IoT On Healthcare System

September 2016

MSc Cyber Security

Abstract

A rocketing number of the applications on Internet of Things (IoT) attracts a focus on security issue between the devices. The information privacy and the secure transaction are one of the considered aspect of the IoT researching area, owing to the highly confidential and personnel of the collected data by the IoT devices. The public especially pay attention on the IoT system relative to medical side. The health condition data recording in medical systems gain a great concern from mass since it is considered the most private personal information in the western world. The access control system on general system can manage the users' accessibility to the data, and it can also rule the devices gain the assets owned by each device; hence, to enhance the access control system is one of the method to preserve the data privacy. To improve the access control system, OCBE protocols is considered as one of the appropriate approaches. The protocols provide the feature of ABAC and CBAC which can simply give the privilege to individual users and also the confusion and diffusion for the transaction data. Moreover, a modification on protocols that can do the reverse verification for accord with the certain situation have been done; since the original protocols can only allow the sender to verify the receiver. The report applied the OCBE protocol onto the healthcare IoT system, and approve that the OCBE protocols enhance the privacy protection on devices and the secure transaction.

Table of Contents

List of Tables

Chapter 1 : Introduction

1.1 Background

Internet of Things (IoT) is progressively used on countless systems. The phenomena gratefully changed our lifestyles such as the resident area and the physical condition surveillance. The wearable devices and the smart furniture help people to methodically and scientifically manage our behaviours and habits in order to improve the quality of life and the health condition. However, the security and the privacy is the big issue on the IoT system. The IoT devices are always collecting the trivial data of the users which can analysis the personal customs by collecting these data. It leads that the security performance on the IoT system is frequently discussed. The worry on the health record is especially focused on. The health condition data are considered as the strictly confidential information; hence, the data preserving pressure form mass pressing on hospitals is surging ahead. Once the record leaked, not only the consequence personal information might be embezzlement but also the hospital might have to face financial loss such as the compensation of insurance and mortgage refusing [1]. Therefore, an access control system is needed IoT system to limit the privileges of the users [1][2].

1.2 Aims and Objectives

The data privacy issue in the healthcare IoT system is usually concerned with the confidentiality. The private information would only be reveal to the certain purpose and responsibility [1], [3], [4]. Moreover, the privacy and the security of the receivers' proof are also worried. Whilst the the subject request the object, the subject need to provide their certificates to the request the permission; however, it is possible to be eavesdropped the proof and be counterfeited. The research endeavours on solving the data-security and the privacy problem on the healthcare IoT system. For finding out the solution, I will identify why the ABAC model and CBAC model are both needed in the IoT system and why the OCBE protocols is appropriate for the this system according to their characteristics. Then, I will designed an new healthcare scenario to applied the IoT system and the protocols on. Following, the policies and conditions will be made for identify working process and how the protocols works in the scenario. Finally, evaluate the policies and analysis the risk of the protocols.

1.3 Outline

There are 6 chapter in the report including introduction, project plan, literature review, evaluation and the conclusion.

Chapter 1: Introduction

In this section, a short introduction of the security issue and privacy concern on access control on healthcare IoT system will be given. Also, the aim and the object of the report would be clarified.

Chapter 2: Project Plan

The schedule of the project will be shown in the chapter. In addition, I will talk about the risk of the project and the personal reflection on the project.

Chapter 3: Literature Review

In this chapter, I will present several access control system model including Role-Based Access Control model, Attribute-Based Access Control model, and Cryptography-Based Access Control model. In addition, I compared the model to figure out what the benefit of each model. Moreover, I mention the recently published access control models which combined with two of the mentioned access control model.

Chapter 4: IoT Health-Care System Scenario

I will explain the protocols applied on the healthcare scenario and illustrate how I twisted the method. Moreover, the detail of the healthcare scenario will be given. In addition, I have listed the defined the policies and condition in the chapter, and alos the commitment exchange processes will be examplified in the section.

Chapter 5: Evaluation

A table will be given where the table is regarding to the results that the condition filtered the different situations and the request from different users. Through the presumed situations, the evaluation to the designed policies and conditions can be done; moreover, it can test the effectiveness and efficiency of the protocols on the healthcare IoT scenario.

Chapter 6: Conclusion

A brief summary and the achievements of the programme will be reviewed. Moreover, I will explain the limitation of the project and the suggest several points where might able to be extended for the future research.

Chapter 2 : Project management

2.1 Gent chart

The following table is the planned schedule of the project which arranged the process of the project. It outlined the order and the trivial procedure, which have to be done in these 13 weeks.

		Week (13 weeks)												
#	Task	1	2	3	4	5	6	7	8	9	10	11	12	13
Investigate and Study														
1	Investigate Access Control													
2	Study OCBE													
3	Analyse a IoT scenario in hospital													
Design, Implement and Evaluation														
4	Create a scenario													
5	Define the rules													
6	Make the Condition													
7	Evaluate and testing the applications													
Document														
8	Write a report													

2.2 Reflection

The purpose of the project is improving the security of the access control which is an aspect that I really want to enhance the knowledge on. It is pretty exiting to work with the professor who is sophisticated in this aspect. The most challenging task of the project is

understating the OCBE protocols. The contained cryptography processes in the protocols makes the protocols inaccessible; moreover, this is my very first time to deeply research the cryptography protocols and understanding the process of proving the crypto-equations. Although I have started reading the protocols before the project formally embarked, it still took me 3 weeks to understand the equations of the encryption and decryption process. The another tough task is to decide the methodology of evaluation. Since the time of the last term of the master degree is short which merely has three months, I am not able to complete the implementation, and it leads me cannot physically test the system. Thus, the evaluating method become a great quandary for me. Thanks the advices from my supervisor and second examiner, which let me have the idea to complete the evaluation. The other difficulty is the whilst outline the scenario, it is hard to image how large the IoT system can be. Because I have never attended a giant IoT system, it is hard to jump out the cube and see the whole picture of a system having handers of or thousands of devices work together. It made me confuse whilst designing the conditions and making the scenario. It is fabulous to do the project and research the solution of enhance the security on IoT system. I acquired a great amount of knowledge of the access control aspect.

Chapter 3 : Literature Review

In this section, we identify the security issues on IoT and also introduces several access control modules and their further extension. Additionally, the motivation of address the access control problem is acclaimed in this section.

3.1 Access Control to IoT

The number of application on Internet of Things (IoT) is proliferating over recent years [5]. According to the predicate from IBM, the number of connected objects will shortly rise up to billions[6]. The data from connected objects can help the computer calculates to find a much accurate predication or improve it. The Internet of Things is a concept that an interaction and collaboration between the things or objects including the sensors, smart phones, RFID (Radio-Frequency Identification), etc [7]. The concept has been applied on numerous areas such as smart-house, automation, transportation and healthcare [8]. IoT helps people to monitor their behaviours and habit to predicate and summarize their life habits and enhance it [8], [9]. Here is an example about the IoT system been applied on the residential area. The electric, water and gas consuming number are been recovered by the power grill system and the other flux monitoring devices. Also, the lamp switch can be control via a phone or an website; meanwhile, the lamp will record the time that users switch it on and off to analysis the lifestyle of users. Through the data collecting, users are able to acquire the statistical data which help to improve the life. The applications have been extended to the house healthcare. The devices help the doctors and patients collect and gather the data which assist both of them to understand the condition of the health [10]. The concept of IoT has been implemented at innumerable fields that the topics relative to the IoT system have been frequently discussed.

The security problems on IoT is one of the common discussion. The security issues have been indicated by the Open Web Application Security Project (OWASP). The organisation has categorised top ten security concerned: Insecure Web Interface, Insufficient Authentication/authorisation, Insecure Network Service, Lack of Transport Encryption, Privacy Concerns, Insecure Cloud Interface, Insufficient Security Configurability, Insecure Software/Firmware, and Poor Physical Security [11]. One of the crucial problem is the authentication and authorisation issue. In certain situation, the collected data from the devices

in IoT systems are highly relative to the behaviour of users, which can only be reveal by the particular devices or users. Hence, a robust access control system to all the devices are necessary. A weak access control mechanism might be review by the hackers; moreover, the privilege can be escalated unconsciously. The another problem is the transport encryption. The transport over the local networks are lack of encryption mechanism to protect the data; hence, the data in transporting in the local network is simply read through reviewing the network traffic [11]. The users are under the threat of data exposing and data losing. The other issue is the privacy concern. Alike the authentication and authorisation problem, the collected data should only be read by the certain users; however, in certain situation, the information can be accessed by numerous users and users but with accessing limitations. The certain part of collected data should only be reveal to a particular group of users and devices. Automated tools can inspect the raw data and acquire the collection of the sensitive personal information, which causes the data leaking [11]. Another worried issued on privacy is the attribute leaking. Whilst the devices submit their attributes to the senders and asking for the data, the attribute might been collected and abused by the senders or been middle-attacked. In certain situation, the attributes refer to the users' private information such as their ID or drive license number, and the explosion on those personal data might threat the users. The security issues are still doubted and remain in discussing though the the IoT have been rapidly and highly developed. Hence, it is necessary to built a robust access control module and system to ensure the data security on IoT system.

3.2 Access Control Models

In this section, a review of several access control will be given include the Role-Based Access Control Model (RBAC), the Attribute-Based Access Control Model (ABAC), and the Cryptography-Based Access Control Model (CBAC). There are two types of Access control which are Mandatory Access Control and Discretionary Access Control[12]. The characteristics of MAC are that there is always a central system classifies messages to levels of secrete and groups the system visitors. All of the objects and subjects are holding a flag which shows their security levels and the access permissions. In the DAC, the permission can be decided by the object providers. The concept of the DAC is that allowing the named users share, control, or modify the named object, such as documents. In other words, in DAC, the

permission is discretionarily decided by the users on to all the object[13]. The RBAC and ABAC models are classified as MAC models and the CBAC is the one of DAC models. The following paragraphs illustrates the models and compares these three modules.

3.2.1 Role-Based Access Control (RBAC)

The Role Based Access Control (RBAC) is one of the access control approaches which is categorised to mandatory access control (MAC). However, the RBAC are not underlying the multilevel control system [14][15]. The approach is that the system will permit the accessing request according to the users' role. In the system, a role represents the permitted functions that users have. The administer will defined a set of permission rules to determined the privilege of each role and the users will be assigned a role that the role turns out the accessibility of the users. The users are assigned a role by the administers and the roles represents the permission the users have and their permission limitations in the systems. In the other words, the users' transaction requests will be permitted depending on the role they belonging and the permissions of the roles have [16][17].

For example, the staffs at front desk in the hospital can append new patients and insert their basic information. In addition, the doctors are allowed to insert the diagnosis and medication the doctors suggested, and treatments performance record. The pharmacist can only read the suggested medications and basic information of the patients. Meanwhile, the staffs at front desk and the pharmacists are not allowed to modified the record of diagnosis and any other data relative to the treatments and only the staff at the front desk can correct the basic information. In these process, all the transactions have to be verified by the systems under the permissions of the roles before the transactions are acted. It will ensure the objects or the actions will not be maliciously executed and peeked. However, there are some limitation of the RBAC model, a user cannot be assigned as two roles at the same time. Moreover, whilst a special user in the group of the role need the extra permission, an extra role is necessary to be created for catering the requests.

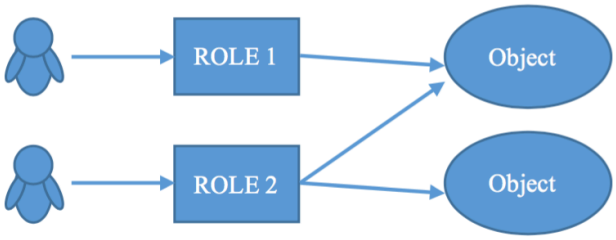

Figure 1 In The Role-Based Access Control, The Rules Are According To The Role Which Users Belonging to

3.2.2 Attribute-Based Access Control (ABAC)

An access control system which permit the user accessibility according to the attribute held by the users is named as Attribute-Based Access Control (ABAC). In ABAC, the programmers and the system administers can authorise the users to execute the certain functions or the certain data. For example, in the same webpage, the user Alice might only be allowed to see the data; meanwhile, Bob can not only read the data but also have the permission of data modify function. [18][19][20]

There is always a control centre to commit the accessibility permission of each function. The control centre will authorise the access requests according to the policy which administers or the documents owners determined. Whilst the users attempt to obtain the objects, the users have to hand their attributes to the control centre. Then the control centre will decide whether the users can approach the objects or not. Whilst the attributes that users submitted accord with the policies regulated by the administers, the users can acquire the data or execute the certain function. Here is an instance, the administers make a policy that in the certain page, function 'ADD' can only be executed if only if the users hold the attribute greater then '5'. The users submit their attribute to the control centre for function execution permission. If the attribute that users owned is larger than '5', such as '10', then the server will accept the added new data.

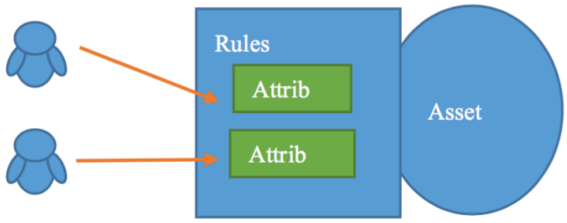

Figure 2 In The Attribute-Based Access Control, The Rules Are According To The Attribute Which Users Have

Compare with the Role-Base Access Control model, the ABAC model can rule the users' accessibility much more flexible. In the Role-Based Access Control model, the permission is depending on the role that user belonging to; on the counterpart, the ABAC model only cross reference the attribute which owned by users. Hence, through the ABAC model, the administers allow to give the users different privilege even they are as the same role.[20] For example, there are two nurses Alice and Bob, and both of them are able to access the page which shows the patients' detail and are able to read the basic information of patients. However, Alice are in charge of the job of front desk where need to receive new patients; hence, she needs the permission to insert the information for new patients. In the RBAC model, the administers have to create a new role such as "front-desk nurse" to distinguish who have the permission to attach a new data. On the contrary, through the ABAC, whilst designing the information showing pages, the designers can regulate that the basic information showing function can be executed if the Attr ≥10; meanwhile, the "ADD" function can be acted whilst the Attr ≥ 30. We defined the all of the nurses can read the data and the Attr of all of them are 10. Then, the administers can permit Alice by change the Alice's attribute of the information showing page from 10 to 30, and then Alice is able to attach the new data to the database. In the case, through the ABAC, the administer only need to alter the attribute instead of drawing a new role to achieve the extra permission change. Through the ABAC model, the position would not be changed whilst the extra permissions are given. Extend the previous example to illustrate the reason. Whoever the nurses working at the front-desk or the nurses who take the responsibility of general document work, their working position still are nurses, whilst the extra permissions have to be given, the real position is not change. Hence, in contrast to the

RBAC, the flexibility of the ABAC model is much higher and much simpler to alter the accessibility for users.

3.2.3 Cryptography-Based Access Control (CBAC)

An access control mechanism which underlying cryptographic methodologies is Cryptography-Based Access Control (CBAC). CBAC underlies on the symmetric cryptography or asymmetric cryptography. [21] In the asymmetric cryptography model, the private key was also named as encryption key and the public key was known as decryption key. In the CBAC, all the actions are restricted by keys. Certain subjects need a paired key to approach the objects. For instance, the data provider would public an encrypted text by the encryption key and if only if the users who own a decryption key have the permission to read the text [22] [23].

In the model, the permission of the documents and other objects are assigned by the owners, which is much more flexible for the owners to decide who can be the certain subject. Moreover, CBAC provides a much secure file storage mechanism on untrusted servers and supply a safer remote control environment. During the period of flourishing cloud service, the users cannot be aware of which trusted services providers would not penetrate or leak the users' data. Over the model, users encrypt the data stored on the cloud; thus, even the encrypted data are accidently exposed, hackers will not be able to peak the objects. The benefits of using CBAC model are that the model provides a much safer mechanism to storage the files on the untrusted servers and a much secure remote control environment. In recent year the cloud-storage and relative services are flourishing; however, the customers cannot know which services providers are much trustable which will not be not simply to penetrated and leak the data. Over the model, the data stored on the cloud are encrypted; hence, even though the objects are accidently approached, the hackers still cannot easily peak the objects. Additionally, it is also much safer to transmit the objects on the internet; in a same reason, even the objects are stolen or monitored during the data transport to the end-side users, the hackers still cannot simply understand the objects. Moreover, the key can be managed without the internet which means the key might be possible to not transmit on the internet under the risk of the key stolen.

3.2.4 Contrasts and Comparison

The difference between RBAC model and ABAC model are that the permission verification process is depending on the users' role or the attributes which users obtaining. In certain situations, the ABAC model is much flexible, since the model ameliorate the process to determined the permissions for individuals. On the other hand, the RBAC provides a well-establish role structure and concerns the structure of real company. Both of the RBAC model and ABAC model require a trusted central operating systems to permit the access requests and manage users' privileges. There is a hazard to apply these models whilst the the operating systems are trustless and the operating system can be hacked. Here is the benefit of the CBAC model that the CBAC model do not require a robust and reliable operating system. The transaction permission and the accessibilities are depending the key the users' have. Hence, whilst the access control systems are implemented on the sceptical operating system, the CBAC is an option should be concerned.

It is possible to take the benefits from two of the models and merge the them. Aftab et al. (2015) had combined two models which import the "Role" into the ABAC model. It eases the process of alter the permission of individual users for RBAC and still remains the features of RBAC which grouping the users and standardizing the policy. A research mentions another model-combined approach which gathering the CBAC model and RBAC model [8][24]. The model owns the features from both of the models which can be imported on an unreliable operating system and butch process the user management.[17] However, the model is not as flexible as the ABAC model, Li and Li combined the CBAC and ABAC which conquer the limitation, which is the protocols are applied in our monitoring model, the OCBE protocols. Through the OCBE protocols, the owners of the assists can appoint the users who own the certain attributes to access the objects; meanwhile, the assists are unreadable confusion and diffusion documents.

3.3 Summary

The Internet of Thigns (IoT) have been imported into countless areas. The technologies regarding to the IoT system have been highly developed and been frequently discussed. The security issue on IoT system is one of the repeatedly mentioned issues in a considerable number of researches. Authentication and authorization, transport encryption, and policy issue are three of the mainly concerning threats. A sturdy and robust access control systems have to employed

into the IoT system to protect the collected data. In addition, the access control systems should provide a data encrypting mechanism to ensure the data transportation. There are three access control models have been considered where are Role-Based Access Control model (RBAC), Attribute-Based Access Control model (ABAC), and Cryptography-Based Access Control (CBAC). Over the RBAC model, administers can efficiently setup the privilege of group of users and through the ABAC model, the managers are able to alter the permissions of individual uses. Meanwhile, the CBAC model gives a safe mechanism to transit the data through the unreliable network tunnels. There are researches combined the models together and take both of their benefits. For instance, a new model has been innovated by combining the RBAC model and CBAC model which simultaneously provides a simple approach to manage the users by groups and the secure data transaction. The further integrated model bonded the ABAC and CBAC model which serving the flexible permission control system and also the encrypted transacting tunnel.

In the IoT system, the things, devices, and sensors cooperate together automatically. In the certain scenario, owing to the mess number of devices, the senders cannot identify the receivers whilst transacting the obtained data [25], [26]. Over the traditional encryption mechanism, the senders have to identified receivers and exchange the decryption key to ensure the data secure, which have the difficulty on policy supply. The attribute-based encryption system can solve the problem. The devices can merely access the data and obtain the key by showing their attribute. It efficiently solved the access control problem in the mess IoT system such as Smart Home or Smart City [27]. However, there is a hazard to show the receivers' attribute to senders whilst the attribute might contain certain personal information. To solve the problem, I employed the OCBE protocols into the IoT system and applied on the hospital monitoring scenario to realize the access control system.

Chapter 4 : A privacy-preserving access control model for IoT

The chapter is regarding to the monitoring scenarios and the approaches to relieve the worried of security hazard to access control on IoT. First of all, an introduction of monitoring scenario will be given and the following are the policies to built up the access control model, the detail of OCBE protocols and how I applied the protocols to the healthcare to IoT system scenario and addressed the security issues.

4.1 Monitoring Scenario

The monitoring devices for physical condition surveillance are widely applied on IoT systems [28]. The monitoring devices can continuously watch the health condition and collected data for the users. The collected data will be submitted to a server or a service provider for machine learning and health problem prediction to help the users improve their health. In the healthcare IoT systems, there are three components compose are crucial: the monitoring devices, medium processors, and the service providers. Since the limitation of computing efficiency and the battery on monitoring devices, they are not an appropriate computer for processing complicated data and doing the long-distance wireless data transaction. Therefore, a medium, a processor, is needed to establish the communication between monitoring devices and the service providers. A processor might be a smart phone or the smart home central controllers which can do the data transaction stably. After the processor catch the data, it might do certain process or merely combine the other data and send them to the servers.

Due to the worth of the health record, the data can be a dangerous asset, and it turns the access control to a pressing problem [29]. One of the possible approach to conquer the problem is to build an access control system over the OCBE protocols. Therefore, I apply the protocols on the health condition monitoring system and will introduce in following paragraphs.

To certify the application on Healthcare IoT system through the OCBE protocols, we selected an health-care scenario which is altered from the glucose monitoring system proposed by Josh Holmes[30]. We assume that, in the scenario, there is a trusted and robust authentication system which has identified all of the servers and devices. Additionally, the processors are required to install a specific purpose-made application for identification and the data processing.

The monitoring device using in the selected scenario is an all-in-one tele-health device made by Medilync, called Insulync. The Insulync combined the glucose surveillance and insulin inject functions, which allow doctors to monitor the health condition of the patients, analyse the data near real-time and be able to do the emergent treatment or injection whilst the certain situation happened. The collected data will be sent to a processor and the processor will simultaneously combine the other data received from the other health-care devices or the data that patients inserted. The server of the appointed hospitals will be feed those collected data for machine learning. The machine learning procedure will train the data and attempt to observe the potential disease and help doctors or patients understand the patients' health condition then identity the best treatment and health care for the patients.

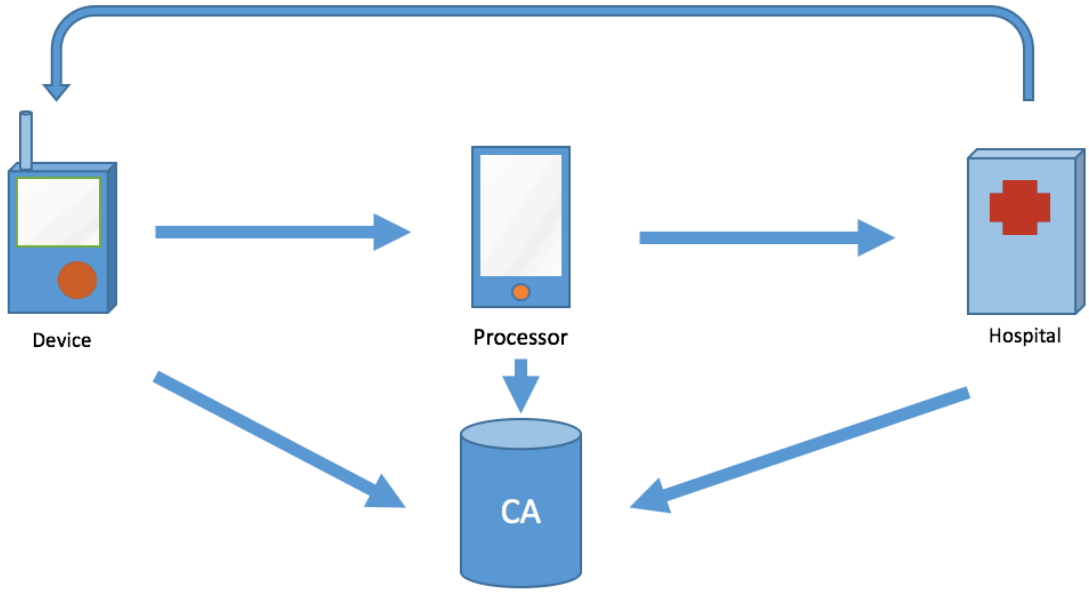

Figure 3 Basic Structure of the Scenario

We defined four components in the structure of the scenario, including a patients-owned monitoring device, a processor, a server of the appointed hospital, and the hospital personnel. We also determined four paths, which is hazard, to apply the OCBE protocols on for ensuring the secure transaction. The data transaction between the monitoring device and the processor via Bluetooth is the first path. The second path is the processor sends collected and combined

data through the Wi-Fi or Mobile Data to the server of the hospital and to do the machine learning. The third path is the treatment command from the hospital sent to the monitoring devices. The last path is the personnel access the database to look up the stored data or the analysed outcome. All of the data should only be read by the authorized users, also the command should be given and be acted by the authorized users; hence, we applied the OCBE protocols into those four paths to achieve the secure transaction. In each path, we selected an appropriate condition and policy to ensure the data can be transmitted via a secure way. The conditions will be introduced at section 3-2 and the introduction of the protocols is the following section. Then, the 3-4 are the details of each four paths.

4.2 Background

4.2.1 Access Control Policy Specification

In the policies, there are two pre-requisites of the policy which all of the devices are supposed have been authenticated by the service provider, and all the devices are equipped a corresponding to customised application. There are two primitives in the access control policy. To formulate the expression to represent the policy, I twisted the policy format from IBM evaluating access control polices[31] which be presents as <Subject Group, Resource Group>.

(1) *Subject:* The actors receiving the messages are the subjects in the model. The subject will hand out their attributes to request the permission to the resource. In the monitoring model, whether monitoring devices, processors or servers, can be a subject to request the resource.

(2) *Resource:* The sent data are the assets which the subjects aim to receives. Meanwhile, the resource is the object that aiming to protect. In the model, the collected data from the monitoring devices and the data storages on the cloud are the resources which is necessarily to be concerned to be received by the certain subjects.

Policy 1: <Data Collecting Processors, Collected Data>

This is the policy for the situation that the central data collector gathering the data from numerous peripheral devices. The are expected to receive the collected data from the monitoring devices. The processors have to be the receiver that senders named; meanwhile, they are expected that the subjects belong to the same medical system as the monitoring devices.

Policy 2: <Servers, Merged Data from Processors>

For the the servers of the service providers, the rule of the data accessing would have to accord with the following conditions: the servers are belonging to the same service system as the senders, the servers should be permitted to collect the merged data from the processors. In the monitoring module, the hospital might employ numerous servers, and only the permitted servers can obtain and process the data.

Policy 3: <Personnel, Data stored on server>

The data stored on the server should be accessed merely by certain users depending on their accessibility. To acquire the data, the personnel have to submit their attributes for asking the permission. In the health monitoring scenario, the attributes are the id of the personnel or their position in the hospital.

Policy 4: <Monitoring Devices, returned command>

For the returned data, the monitoring devices have to verified the command is from the specialist doctors in the contracted hospitals. Hence, the doctors have to hand in their attributes to verified whether they have the permission. After then, an issued commitment will be transmitted to the Monitoring Devices, and the devices will verify weather the return commands are from the particular users.

4.2.2 OCBE Protocols

The Oblivious Commitment-Based Envelope (OCBE) scheme are protocols for protecting the receivers' attributes. The OCBE protocols applied in the IoT monitoring module is following the OCBE protocols defined by Jiangtao Li and Ninghui Li [32]. In the defined OCBE protocols, a Pederson commitment Scheme is applied in, which will be introduced in the first part of the section. The followings are the introduction of OCBE protocols.

4.2.2.1 Pedersen Commitment Scheme

The initialisation of the OCBE Protocols employed the Pedersen Commitment Scheme to setup the CA. There are three steps including setup, commit, and open. Through the scheme,

the CA can produce the numbers ***p, q, g, h***, which represented as **Params** = **<*p, q, g, h*>**. The following paragraph is going to give a review of scheme.

Setup: Assume there is a trusted third party, and the party selected great prime numbers ***p, q*** whilst ***p-1*** can be divided by ***q***. Then the g is assign as the generator of G_q which is the one of the unique subgroup of $\mathbb{Z}_q$ which in order-***q***. I follow the expressing method $x \leftarrow \mathbb{Z}_q$ to represent the x which is chosen randomly from the set $\mathbb{Z}_q$. A secrete integer $x \leftarrow \mathbb{Z}_q$ is selected by the third party, then the third party take x the to calculate $h = (g^x \bmod p)$. The numbers ***p, q, g, h*** will be published and the secret ***x*** will be confidentially preserved by the trust third party.

Commit: A party *Amy* commit a value $a \in \mathbb{Z}_q$ to the three party, where $\mathbb{Z}_q$ is the domain of committed value. After then, the third party calculates the $c = (g^a h^r \bmod p)$.

Open: The verifiers open the commitment verify ***c*** by compute $c = (g^a h^r \bmod p)$.

The scheme introduced in the Li's OCBE protocols, which is also employed in our module, have somewhat differences from the original Pedersen commitment scheme. In this scheme, A and setup programme is run and zero-knowledge proof is done by the verifiers for persuading A that the parameters are constructed properly.

4.2.2.2 OCBE Protocols

The protocols are involving a receiver, a sender, and a trusted Certificate Authority(CA). The OCBE protocols have five step: CA-Setup, CA-commit, Initialization, Interaction, and Open.

CA-Setup: The setup step is a preparation before the transaction begin which will be run by the CA. First of all, CA takes a security parameters ***t*** and publish ***Params*** for commit. Also CA publics a set of possible value V, a set of Predicates ***P***. Every predicate in ***P*** will be mapped an element in V to ***TRUE*** or ***FALSE***.

CA-Commit: The Receiver submits their attribute and the identity of the Sender to the ***CA*** and the ***CA*** will randomly choose a number ***r*** and output the commitment ***c*** = $commit_{Params}(a,r)$. A Certificate which contains ***r*** and ***c*** will be issued to Receiver by CA. Then the commitment ***c*** will be send to the Sender

Initialization: Sender decides a sending message ***M*** in binary and Receiver agree a predicate ***Pred*** from ***P***.

Interaction: Sender and Receiver interactive through the protocol by using an envelope which contain the encrypted message and sent from the sender to the receiver.

Open: If the attribute that receiver hold is accord with the predicate, the ***Pred(a)=True***, then the Receiver can decrypt the message ***M***. If the ***Pred(a)=False***, then Receiver cannot learn anything about the message.

4.2.2.3 EQ-OCBE

The EQ-OCBE is one of the OCBE protocols which only allow the users whose attribute is exactly equal to the predicate which sender decided. The EQ-OCBE protocols we applied to the scenario is based on the methods proposed by Jiangtao Li and Ninghui Li ((Paper)). The method adopted the Diffie-Hellman key-agreement protocol; however, whilst the attributes of receiver is equal to the selected predicate then the shared key can be calculated by the receiver. The following are the detail of the steps of the EQ-OCBE.

Assume $\boldsymbol{\varepsilon}$ is a semantically secure symmetric encryption scheme with keyspace $\{0,1\}^s$. $H \longrightarrow G_q\{0,1\}^s$ is a cryptographic hash function that extract a key for $\boldsymbol{\varepsilon}$ from an element in the group Gq. The order-q subgroup of $\mathbb{Z}_p$ *.

CA-Setup: A security parameter ***t*** would be select by CA and runs Pedersen Commitment Scheme Setup Algorithm. Then the CA generates **Params** = **<*p, q, g, h*>** and also the $V = \mathbb{Z}_p$ *and* $\boldsymbol{P} = \{ \mathbf{EQ_{ao}} \mid \boldsymbol{a_0} \in V \}$, where $\mathbf{EQ_{ao}}$: $V \longrightarrow \{ \boldsymbol{True}, \boldsymbol{False} \}$. $\mathbf{EQ_{ao}(a)}$ is a set of predicate where $\mathbf{EQ_{ao}(a)}$ would be true if $\boldsymbol{a} = \boldsymbol{a_0}$; on the other hand, if $\mathbf{a \neq a0}$, then $\mathbf{EQ_{ao}(a)}$ would be false

CA-Commit: The attribute that Receiver held is an integer and will be submit to the CA. CA randomly chooses a number $r \leftarrow \mathbb{Z}_q$ and generates the commitment $\boldsymbol{c = g^a h^r}$. Consequently, ***c*** and ***r*** will be packed as a Certificate and be sent to the Receiver; meanwhile the ***c*** will be submitted to the Sender.

Initialization: A message would be decided by sender. Then the sender and receiver will agree a predicate $\mathbf{EQ_{ao}} \in \boldsymbol{P}$.

Interaction: Sender will select an integer $y \leftarrow \mathbb{Z}_q$, then compute $\sigma = (cg^{-a0})^y$ and send the $< \eta = h^y, C = \varepsilon_{H(\sigma)}[M] >$ to the receiver.

Open: Receiver obtains the $< \eta, C >$ and calculate $\sigma' = \eta^y$ to decrypt C by $H(\sigma')$. If $\mathbf{EQ_{ao}}(a)$ = **TRUE** which means the a_0 = a, the Receiver can successfully decrypt the message by $\sigma = (cg\text{-}a0)^y = (gahrg\text{-}a0)^y = (ga\text{-}a0hr)^y = (hr)^y = (hy)^r = \eta r = \sigma'$ ***(Equation 1***; meanwhile, the Receiver obtains the same symmetric key to encrypt the return message. If $\mathbf{EQ_{ao}}(a)$ = FALSE, receiver cannot decode and acquire any contain of the message.

$$\sigma = (cg^{-a0})^y = (g^a h^r g^{-a0})^y = (g^{a-a0} h^r)^y = (h^r)^y = (h^y)^r = \eta^r = \sigma' \text{ (Equation 1)}$$

4.2.2.4 GE-OCBE

The GE-OCBE twist the EQ-OBCE protocol by using greater-than-or-equal-to operation. The following is the details of the GE-OCBE.

Assume ε is a semantically secure symmetric encryption scheme with keyspace $\{0,1\}^s$, and two cryptographic hash functions , $H \rightarrow Gq\{0,1\}^s$ and $H':\{0,1\}^{s\ell} \rightarrow \{0,1\}^s$.

CA-Setup: A security parameter t and a parameter ℓ will be selected by CA, which define the range of the attribute value. Then the setup algorithm of the Pedersen commitment scheme will be run and generate the **Params =** $<p, q, g, h>$ whilst $2^\ell < q/2$. In addition, the CA will generate the $V = \mathbb{Z}_p$ and $P = \{\mathbf{GE_{a0}}|\mathbf{a_0} \in V\}$, where $\mathbf{GE_{a0}}$**: V→{TRUE, FALSE}**.

CA-Commit: The attribute $a \in V$ which receiver has will be send to the CA. and the commitment $c = g^a h^r$ will be computed by the CA. Meanwhile, c and r will be sent to the receiver and the c will be send to the sender.

Initialization: A message will be designed by the sender. Then, the sender and receiver would agree a predicate $\mathbf{GE_{a0}} \in P$.

Interaction: We assumed $d = ((a\text{-}a_0) \bmod q)$, and if $\mathbf{d} \in [0 \ldots 2^\ell\text{-}1]$ then $\mathbf{GE_{a0}(a)}$ = **TRUE**. Receiver decides $r_1, \ldots, r_{\ell\text{-}1} \leftarrow \mathbb{Z}_q$ and sets $r_0 = r - \sum^{\ell-1}_{i=1} 2^i r_i \bmod q$. Whilst $\mathbf{GE_{a0}(a)}$ = **TRUE**, d can be represented as a set binary digit $d_{\ell-1}, \ldots d_1, d_0$, which means $d = d_0 2^0 + d_1 2^1 + \ldots. d_{\ell-1} 2^{\ell-1}$. However, whilst $\mathbf{GE_{a0}(a) = FALSE}$, the binary set $\mathbf{d_{\ell-1}, \ldots d_1, d_0} \leftarrow \mathbf{\{0,1\}}$ would be randomly selected by the receiver and set $\mathbf{d_0} = \sum^{\ell-1}_{i=1} \mathbf{2^i d_i}$. Then, the receiver commits $\mathbf{C_i} = \mathbf{commit(d_i, r_i)} = g^{di} h^{ri}$, $(0 \le i \ge \ell\text{-}1)$ and submit the commitment $C_0 \ldots C_{\ell-1}$ to Sender. Sender

verifies $cg^{-a0} = \prod^{\ell-1}_{i=0} (Ci)^{2i}$ and randomly pick **K** sets of keys $\mathbf{K_0}.....\mathbf{K_{\ell-1}} \in \{0,1\}^t$. Then, Sender selects a random parameter $y \leftarrow \mathbb{Z}_q^*$ to calculate $\eta = h^y$ and $C = \mathcal{E}_k[M]$. Moreover, Sender counts $\sigma^0_i = (C_i)^y$ $\sigma^1_i = (C_i g^{-1})^y$ **and** $C^0_i = H(\sigma^0_i) \oplus K_i$ and $C^1_i = H(\sigma^1_i) \oplus K_i$. Sender transfers $<\eta, C^0_0, C^1_0, C^0_1, C^1_1, \ldots. C^0_{\ell-1}, C^1_{\ell-1}, C>$ to Receiver.

Open: Receiver receives the $< \eta, C^0_0, C^1_0, C^0_1, C^1_1, \ldots. C^0_{\ell-1}, C^1_{\ell-1}, C>$. If $\mathbf{GE_{a_0}(a)} =$ **TRUE** where the $a > a_0$, then $d = \sum^{\ell-1}_{i=1} d_i 2^i$, which means the Receiver can know $\sigma'_i = \eta^{ri}$ and $K_i' = H(\sigma'_i) \oplus C^{di}_i$ $(0 \le i \ge \ell\text{-}1)$. Then, receiver can found $K' = H'(K'_0 || \ldots.. || K'_{\ell-1})$ and decrypt the C by K'.

4.2.2.5 OCBE Protocols for Other Predicates

In the OCBE protocols, the predicates are able to be logically combined. It extends the OCBE protocols to numerous new protocols include ∧AND-OCBE, ∨OR-OCBE, > GT-OCBE, ≤ LE-OCBE, < LE-OCBE, ≠ NE-OCBE, and RANGE-OCBE. Jiangtao Li provides a formal representing regulation which is *OCBE(Pred, a, M)* where the Pred is the predicate, a means the committed value, the message M which is the output message whilst the Pred(a) = TRUE [32], [33]. The following will briefly introduce the protocols.

1. **AND-OCBE:** The protocol can build a new predicate by logically combining two predicates. For accessing, the two attributes of users have to accord with two predicates, which been represented as $\mathbf{Pred = Pred_1 \wedge Pred_2}$. Whilst the sender and receiver interactive with $OCBE\ (Pred_1 \wedge Pred_2, a, M)$, the sender selects tow keys randomly which are k1 and k2. The key k will be set through a cryptographic hash function H as $k = H(k_1 \| k_2)$. The sender and receiver run the phases $OCBE\ (Pred_1, a, M)$ and $OCBE\ (Pred_2, a, M)$ together. A $\varepsilon_{H(\sigma)}[M]$ based on will be send to receiver and the M can be accessed if only if $Pred_1\ (a) = TRUE$ and $Pred_2\ (a) = TRUE$.

2. **OR-OCBE:** To construct the $OCBE\ (Pred_1 \vee Pred_2, a, M)$, the sender takes a key k randomly and runs the $OCBE\ (Pred_1, a, M)$ and $OCBE\ (Pred_2, a, M)$ at the same time with the receivers. Sender will send a $\varepsilon_{H(\sigma)}[M]$ to receiver and whilst $Pred_1\ (a) = TRUE$ and $Pred_2\ (a) = TRUE$, the receiver can obtain the M

3. **GT-OCBE:** Whilst the attribute a and the predicate number a_0 are integers, $a > a_0$ equals to $a \geq a0 + 1$. Hence, ***OCBE ($>a_0$, a, M)*** is same as ***OCBE ($\geq a_0 +1$, a, M)***.

4. **LE-OCBE:** The process of ***OCBE ($\leq a_0$, a, M)*** is as follow: found that $a \leq a_0$ if only if $d = ((a_0 - a) \bmod q) \in [0 \ldots 2^{\ell}-1]$. Assume the commitment for attribute a is $c = g^a h^r$. The commitment of d is $g^{a0} c^{-1} = g^{(a0-a) \bmod q} h^{-r \bmod q}$ which can be opened by the receiver. Then, the interaction and open process for LE-OCBE are the same as the GE-OCBE.

5. **LT-OCBE:** As the idea of GT-OCBE, the $a < a_0$ equals to $a \leq a0 - 1$, whilst in integer space. Hence, the ***OCBE ($<a_0$, a, M)*** can be represented as ***OCBE ($\leq a_0$-1, a, M)***.

6. **NE-OCBE:** $a \neq a_0$ is as same as $(a > a_0) \vee (a < a_0)$. Hence, we can use ***OCBE ($> a_0 \vee < a_0$), a, M)*** to represent ***OCBE ($a \neq a_0$, a, M)***.

7. **RANGE-OCBE:** Whilst in integer space, a can be limited in a range and be represent as $a_0 \leq a \leq a_1$ and it is equal to $(a \geq a_0) \wedge (a \leq a_1)$. Therefore, as the previous approach, wec an do ***OCBE ($a_0 \leq a \leq a_1$, a, M)*** as ***OCBE ($\geq a_0 \wedge \leq a_1$, a, M).***

4.2.2.6 MOCBE: Multi-attribute OCBE

OCBE protocols ensure that the receivers who can open the message are always satisfy with the senders' policies. However, in certain cases, it is necessary to use more than one attribute to identify the users. Such as the situation in monitoring scenario, the monitoring device will verify the commands are from the contract hospitals and the specialist doctors. The MOCBE protocols can verify multi-attribute and compare the predicates. The symbol $\diamondsuit$ represent the operations including $\geq$, $>$, $\leq$, $<$, $\neq$, and $=$. There are two means to practice the MOCBE protocols which are Linear Relation Predicates and General Comparison Predicates. The following will only introduce the linear relation predication which will be used in the Healthcare system scenario[33].

The Linear Relation Predicate can combine two predicate together which represent as ***Pred(a1,…,an)*** taking the equation of $a_1 b_1 + \ldots + a_n b_n \diamondsuit e$, where e and $b1, \ldots, bn$ are integers from $V = \mathbb{Z}_p$. ***Pred(a1,…,an) = TRUE,*** whislt the $a_1 b_1 + \ldots + a_n b_n \diamondsuit e$ is true. Base

on the Pederson commitment scheme, the commitment $x = a_1b_1 + \ldots + a_nb_n$ can be turn out from calculating the $C = C^{b1}{}_1, C^{b2}{}_2, \ldots C^{bn}{}_n$, by bothe of the senders and receivers. The receiver can decrypted the message whilst the $x \diamondsuit e = TRUE$.

4.3 IoT Health-Care System Scenario

To specificly illustrate the security issue and the policies realizing, in this section, I will demonstrate the security concern and how the OCBE protocols are applied on the IoT scenario. The scenario is regarding the IoT application on healthcare system which interacting between devices that patients or the hospital possessed. There are five roles in the scenario: Monitoring Device, Processor, Server of Hospital, CA (Certificate Authority), and Hospital Personnel. Additionally, there are four transaction paths including the interaction between Monitoring Device and Processors, Processor to Server of Hospital, the Personnel hand treatment command to Monitoring Device, and between the personnel of Hospital and the server of Hospital. The following paragraph will meticulously explain the scenario and the application.

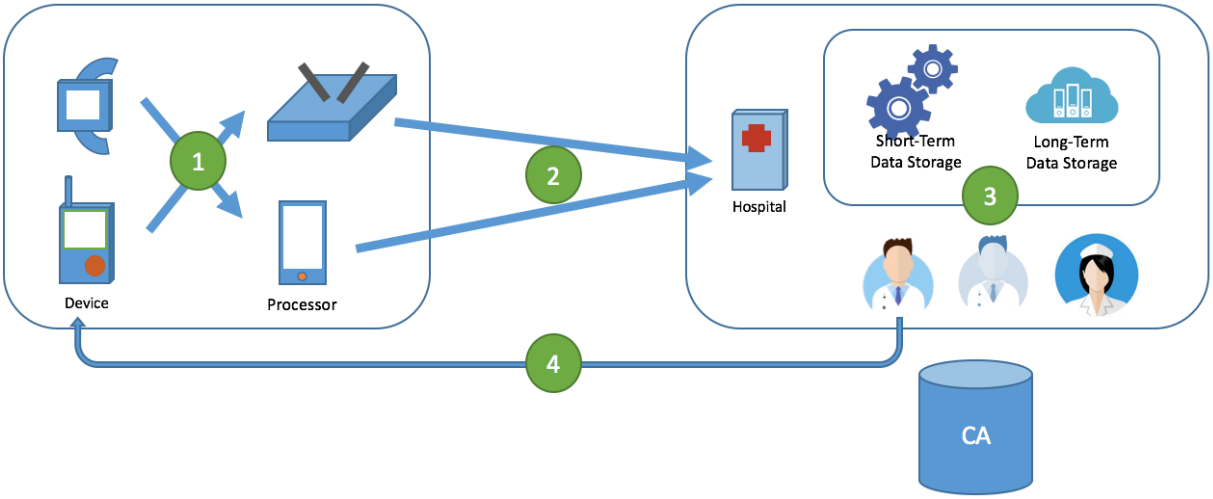

Figure 4 The Structure Of The Scenario

4.3.1 Conditions

The attributes for each role are assigned to clarify the scenario, and all of the attributes are belonging to the integer space. Principally, each device has an identical integer number named Patient ID (Pid) which shows who owns the device; moreover, they have a Device

Categories (DC) number which is the attribute regarding to the type of the devices. The servers of the hospitals hold an integer serial number Hospital Identify Number (Hid) which represent the belonging which hospital. There are two attributes are only for the hospital personnel. One of the two is "Role" which defined their working positions in the hospital where 10 represents Nurse, 20 means the general doctor, and 30 refer to the diabetes specialist doctors. The other is WE which represent how many years the personnel have working in emergency call.

The assists in the scenarios have been identified in the previous section about the policies. To protect the objects, the following conditions are designed for verified devices which are aiming on accessing them. There are three conditions, and each of the them are ruling the certain policies, where the condition 1 is for the policy 1 and 2, the policy 3 refers to the condition 2, and condition 3 corresponds to policy 4

Condition 1: Pid or Hid == certain personnel or hospital && DC == certain category

Policy 1: <Data Collecting Processors, Collected Data>

Policy 2: <Servers, Merged Data from Processors>

In a health condition monitoring system, there are more than one data processor near the patients. To authorise a processor having an access permission, the control mechanism merely need to verify who their owners are, underlying the premise that all the devices are authenticated. The objects to open the subject have to accord with the condition, no matter the correspondence between collecting data and the processors or the merged data and the hospitals' servers. To verify the Pid or the Uid is for preventing the data are read by the other devices owned by other patients'. Moreover, since only the processors are able to opened the collected data and combine with the data from other monitoring devices. Under the same reason, only the server in the certain hospital can obtain the data from health-care devices rather than exposing the information to other hospital or other devices.

Condition 2: Short-term → Role ≥ Nurse; Long-term → Role ≥ Doctor

Policy 3: <Personnel, Data stored on server>

The health condition data is always worthy; hence, the access control system should only allow certain personnel to obtain the data. Different data stored on the server have different value, for instance the long-term data can state the complete personal physical

condition; however, the short-term information can only refer to the problem happened currently. Since several personnel are not going to do the diagnosis such as nurses and front-table staffs; thus the control system should ban them to obtain the long-term data. Thus, I defined the personnel can access the short-term data should be a person a nurse or the working position is higher than nurse. Meanwhile, the long-term data should be access if only if the users are doctors.

Condition 3: Role ≥ Doctor && WE ≥ 3

Policy 4: <Monitoring Devices, returned command>

In some healthcare IoT system, the monitoring devices or processors might receive an advice from a doctor. In the situation, the receivers have to verify that the feedback is from a doctor, hence an access control is needed. There is a special thing that there is a special machine, Insulync, is using in our scenario. The devices can inject the insulin whilst the emergent situation underlying the command from doctors. Moreover, we assume that the diagnoses are expected from a doctor who acquired emergency call working experience for numbers of years. Therefore, the condition is defined that the attributes have to accord that the role are greater or equal to a doctor.

4.3.2 Each Paths in the Scenario

The following paragraphs will meticulously illustrate the processing progress of each path through the OCBE protocols. To effectively and efficiently explain the scenario, I assigned the attributes an integer numbers shown in the following tables. The first table presents the attributes which possessing by each device and the second table shows the personnel's attributes.

Table 1 Attributes of Devices

Devices	Pid	DC
Insulync	12345678	504 (Insulync)
Smart Watch	12345678	303 (Watches)
Mobile Phone	12345678	600 (Processor)
Smart Home Data Centre	12345678	600 (Processor)
	Hid	DC

Servers in Hospital A	23456789	800 (Server)

Table 2 Attributes of Personnel

Personnel	Role	WE
Nurse	10 (Nurse)	5
General Doctor A	20 (General Doctor)	2
General Doctor B	20 (General Doctor)	5
Diabetes Specialist Doctor	30 (Diabetes Specialist Doctor)	5

4.3.2.1 Patient monitoring device to Processor

In the scenario, the monitoring devices and processors are identified by the Hospital and be possessed by the users. The task of the devices is collecting the data of the patients' health, such as blood sugar, to surveillance the health condition. Then the collected data will be submitted to processors for caching and re-arrange, then be transferred to the servers of hospitals. The first policy, <Data Collecting Processors, Collected Data> has identified that the raw data from the Monitoring Device is one of the asset which means only the curtain Processor can decrypt the data. Through the Condition 1, which corresponding to the Policy 1 should be applied for securing the data.

First of all, the CA will run the CA-setup and publish the public parameters and the set of possible predicates. In the OCBE protocols, the $\mathbf{a_{Pid}}$ and $\mathbf{a_{DC}}$ are the attributes, Pid and DC, of processors and the **M** is the message. Whilst the communicate between the monitoring devices and processors are beginning, the processors will hand their attributes to the CA. Then the CA will distribute the commitment to both of the monitoring devices and processors; in additionally, post a secret parameter ***r*** to the processors. After then, the monitoring devices agree the $\mathbf{Pred} = \mathbf{Pred_1(Pid=12345678)} \wedge \mathbf{Pred_2(DC=600)}$ with he processors. The attributes of processors have to let $\mathbf{EQ_{Pid}(a_{Pid})} = \mathbf{TRUE}$ and $\mathbf{EQ_{DC}(a_{DC})} = \mathbf{TRUE}$. Through the **AND-OCBE** and over the MOCBE, the function can be $\mathbf{OCBE(Pred_1 \wedge Pred_2, (a_{Pid}, a_{DC}), M)}$ that if $\mathbf{EQ_{Pid}(a_{Pid})} = \mathbf{TRUE} \wedge \mathbf{EQ_{DC}(a_{DC})} = \mathbf{TRUE}$ then the processors can decrypt the message and get the **M**. For example, whilst the mobile phone and the Insulync are going to construct

the communication, the mobile phone will pass its Pid and DC to the CA and ask for the commitment. Then the Insulync would send the encrypted collected data to the monitoring devices. Since the Pid (12345678) and DC (600) which the attribute that mobile phone obtain are accord to both of the predicates, the mobile device can decrypt the sent message and the obtain the **M**. On the other hand, if the smart watch also requires the collected data from the Insulync, the watch cannot open the encrypt message because of $\mathbf{Pred_2(303 \neq 600) = FALSE}$. The condition can block the unauthorised devices to learn the collected data.

4.3.3 Processor to Hospital

The collected data will be merged with other data and transmit to the hospitals' servers. As the defined policy 2, <Servers, Merged Data from Processors>, the asset in this path is the merged data and the objects aiming on accessing it are the servers of the hospitals. To prevent the data leakage, the access control is need for the path. Similarly, I assumed that the identification jobs have done for the processers by the Hospital. For this path, the condition 1 are also applied on, and the following is the detail about the access control realisation on this path over OCBE Protocols.

As the previous path, before the transaction started, the CA will have done the preliminary work. The servers have the attributes Hid ($\mathbf{a_{Hid}}$) and DC ($\mathbf{a_{DC}}$) which will be sent to the CA for committing whilst communicate is establishing. We take the Hospital A as the target server that the processors send the data to. The CA will give the commitment and a secret parameter ***r*** to the servers and the commitment. Next, to accord the condition 2, the processors and the servers agree the predicates $\mathbf{Pred = Pred_1(Hid=23456789) \wedge Pred_2(DC=800)}$. Then, according to the AND-OCBE and MOCBE, the protocols can be represented as $\mathbf{OCBE(Pred_1 \wedge Pred_2,(a_{Hid}, a_{DC}), M)}$. Whilst the $\mathbf{EQ_{Hid}(a_{Hid}) = TRUE \wedge EQ_{DC}(a_{DC}) = TRUE}$, the servers can open the messages.

4.3.4 Personnel access health condition record

The personnel who work for the healthcare services in the hospital always require to read the patients' medical record. The collected data from the monitoring devices will be train and store as part of medical records of patients, and can be access by the certain personnel. Or,

the system can give an alert to a doctor whilst detected the abnormal signal from the users, which can let the doctors remotely do the emergent aid for patients such as insulin injection. The policy 3 identified that the subjects are the personnel and aiming on accessing the objects, the long-term and short-term data.

In the condition 2, which is for policy 3, are made for coping the situation. The personnel who request for short-term data, their Role should be greater than and equal to 10; meanwhile, the merely the personnel whose Role is greater than and equal to 20 can access the long-term data. Hence, over OCBE protocols, the servers will agree two predicate $\mathbf{Pred_1(Role \geq 10)}$ and $\mathbf{Pred_2(Role \geq 20)}$, after the CA has done the initialisation step and the personnel have handed their attribute $\mathbf{a_{Role}}$ to the CA, also receive the commitment and secrete parameter $\boldsymbol{r}$. Over the GE-OCBE, the equations of the predicates are $\mathbf{OCBE(\geq 10\ , a_{Role}\ , M)}$ and $\mathbf{OCBE(\geq 20\ , a_{Role}\ , M)}$. If only if the $\mathbf{EQ_{Role}(a_{Role}) = TRUE}$ can decrypt the message of long-term or shor-term data from the servers. For example, the the Doctor A whose Role is 20 can access both of the record because of $\mathbf{Pred_1(20 \geq 10) = TRUE}$ and $\mathbf{Pred_2(20 \geq 10) = TRUE}$. However, a nurse can only access the short-term where the $\mathbf{Pred_1(10 \geq 10) = TRUE}$ but $\mathbf{Pred_2(10 \geq 20) = FALSE}$.

4.3.5 Personnel to Monitoring Devices

An emergent remote treatment can be given due to the certain situations. Whilst the servers or the processors detected abnormal signals, an alert would send to the doctors and ask for doing the diagnose. The emergent disposal or injection might be needed whilst the patients' conditions are rapidly deteriorating or have certain problems. In this situation, the monitoring devices verify the treatment commands are from personnel who have the permission to inject. Hence, for the situation, I twisted the process of the OCBE protocols. The personnel have to submit their attribute to the CA for produce commitment. After that, the CA will send the commitment to the monitoring devices, then the monitoring devices construct the communication and exchange the shared-key with the personnel of the Hospital. The shared-key can encrypt the treatment command and the cipher will be send to the monitoring devices. Whilst the encrypted command can be decrypted by the monitoring device, then it means that the personnel who do the treatment is permitted and the command is trusted. Within the policy

4 and the condition 3, we have defined only the doctor who have over 3 years' experience in emergency call team.

Here is an example. As the general process, the CA has done the setup and all the devices and people are identified. The personnel send their attribute $\boldsymbol{a_{Role}}$ and $\boldsymbol{a_{WE}}$ to the CA. The CA distribute the commitment to personnel and the monitoring devices, and also transmit the secrete parameter $\boldsymbol{r}$ to the personnel. The monitoring devices and personnel agree the predicate $\mathbf{Pred} = \mathbf{Pred_1(Role \geq 20)} \wedge \mathbf{Pred_2(WE \geq 3)}$, where the formal equation is $\mathbf{OCBE(Pred_1 \wedge Pred_2, (a_{Role}, a_{WE}), M)}$ The monitoring device would send a hand-shake message to the personnel and then sharing the key $\boldsymbol{k}$, if the personnel's attribute can let $\mathbf{EQ_{role}(a_{Role}) = TRUE} \wedge \mathbf{EQ_{WE}(a_{WE}) = TRUE}$. Such as the Doctor A whose Role is a doctor however his working experience is merely two years where $\mathbf{EQ_{Role}(20) = TRUE}$ but $\mathbf{EQ_{WE}(2) = FALSE}$, then the Doctor A cannot commute the share-key. On the opposite side, the Doctor B can have the shared key since his working experience is over 3 years. Obviously, the nurse doesn't have the permission since the Role level is lower than 20. After shared the key, the monitoring devices would wait for the treatment command and do the command according to the doctors' advice.

Chapter 5 : Evaluation

The following paragraph will list the possible situations and test the policies and evaluate the conditions which have been applied on the OCBE protocols for the designed healthcare scenario.

Path 1:

The following is the set of possible situations to evaluate weather the policy 1 on path 1 can effectively filter the unauthorised access request. Table 3 shows several situations. In the table, it listed the attributes of the devices which attempting to ask the collected data. I suppose that in the structure, there are more than one monitoring device, processor, and patient. Also there are numbers of hospitals with numerous servers. Presuming that the user Alice and user Bob are the legal users in the system and all of their devices have been identified and verified by the authentication system. Similarly, the servers in the hospital also have been verified. The cell phone and the smart home control centre are classified as a processor, and the watches and Insulync are labelled as monitoring devices.

Table 3 The Request Result of Different Devices in Path 1

	User	Device	Device Category	Pid	DC	Result
Target	Alice	Any Processor	Processor	123456	300	
1	Alice	Cell Phone	Processor	123456	300	Open
2	Alice	Smart Home Control Centre	Processor	123456	300	Open
3	Alice	Watches	Monitoring Devices	123456	303	Deny
4	Bob	Insulync	Monitoring Devices	654321	504	Deny
5	Bob	Cell Phone	Processor	654321	300	Deny
6	Bob	Smart Home Control Centre	Processor	654321	300	Deny
7	Bob	Watches	Monitoring Devices	654321	303	Deny
	Hospital	Device	Device Category	Hid	DC	Result
1	Hospital A	Server A in the Hospital A	Server	234567	800	Permit

2	Hospital B	Server A in the Hospital B	Server	765432	800	Permit

Assume that the Alice's Insulync is sending the collected data, and the target receivers are the processors which own by Alice. The condition applied on the path 1 is **Pred** = $\mathbf{Pred_1}$(**Pid**) $\wedge$ $\mathbf{Pred_2}$(**DC**). For the first two situations, the devices are the cell-phone and the smart home control centre possessed by the patient Alice. These two devices can successfully decrypt the message because that both of their Pid and the DC are equal to the agreed predicates. In the third situation, the watch is owned by Alice; however, the device is not a processor which means the value of device category is not equal to 300, a processor; hence, cannot decrypt the message. The situation turns to focus on other users in the last four situations. Even the same devices, Insulync, it is also not able to decrypt the message from Alice's Insulync, whilst it owns by Bob (Pid $\neq$ 123456). In the same reason, the device category of the devices in the situation 5 and 6 are the same as the target devices; however, they are hold by Bob (Pid $\neq$ 123456); therefore, the message cannot be opened via these two devices. Bob's watch is not only not accord with the aimed devices category but also not hold by Alice; thus, it is impossible to open the encrypted message. The server of the hospitals cannot acquire the collected data directly, because of lacking the required attribute Pid.

Path 2:

An evaluation to path 2 will be test in this section. The following table presents the possible situations of the path 2, which contains the attributes that a hospital sever should have. Assume that there are numerous hospitals and each hospital has multiple servers; and there are two hospitals in the testing scenario, Hospital A and Hospital B, additionally, I added to the reverse direction which the other penitents' devices. The sending target is the servers in the Hospital A.

	Hospital	Device	Device Category	Hid	DC	Result
Target	Hospital A	Servers of the Hospital A	Server	234567	800	

1	Hospital A	Server A in the Hospital A	Server	234567	800	Permit
2	Hospital A	Server B in the Hospital A	Server	234567	800	Permit
3	Hospital B	Server A in the Hospital B	Server	765432	800s	Deny
4	Hospital B	Server B in the Hospital B	Server	765432	800	Deny
5	Hospital A	Nurse A's computer in the Hospital A	Processor	234567	148	Permit
6	Hospital B	Nurse B's computer in the Hospital B	Monitoring Devices	765432	225	Permit
	User	Device	Device Category	Pid	DC	Result
7	A	Cell Phone	Processor	123456	300	Deny
8	A	Smart Home Control Centre	Processor	123456	300	Deny
9	A	Watches	Monitoring Devices	123456	303	Deny

The conditions to accord with the policy 2 is as the same as the path 1 but replace Pid to Hid as the factor in path 2, which is **Pred** = $\mathbf{Pred_1(Hid)} \wedge \mathbf{Pred_2(DC)}$. As the supposed target, the attributes of servers should be Hid = 234567 and DC = 800, such as the servers in the first two situations. The Server A and the Server B in the Hospital A are obviously belonging to the Hospital A, which the attributes Hid and DC should be 234567 and 800; thus the servers can decrypt the message. As the third and fourth situations, though the machine type is completely equal to 800; however, they are belonging to the Hospital B that the Hid are 765432 which are not as the same as the target. The devices used in the fifth and the next situation are not server, whose DC are not equal to 800. Although in the situation 5, which the Hid is 23456, it would be filtered by the condition due to the unequal device category. The devices will be filtered since the two uncoordinated attributes (Hid $\neq$ 234567 and DC $\neq$ 800). The condition can check the last three situations as wall, because that the devices only have the Pid and lacking of the correct attribute Hid, then the devices cannot obtain the plain message. Through the situations in the Path 1 and Path 2, it is known that the condition 1 works most of the cases.

Path 3

There are two types of data accessing requests in the path 3 which are short-term and long-term data requesting. The policy for the path 3 have two conditions due to the situations which are $Pred_1$(Role≥10) and $Pred_2$(Role≥20). The Table 4 and Table 5 show the result of the short-term and long-term data requests from each personnel. I assume there are four personnel in the hospital, who are staff, nurse, general doctor, and specialist doctor. Each of them has been identified and verified by the hospital authentication system, and be able to submit the data queries.

Table 4 The Short-Term Data Request Result Form the Different Personnel in Path 3

Short-Term Data				
	User	Role	Role Number	Result
1	Front Desk A	General Staff	0	Deny
2	Nurse A	Nurse	10	Permit
3	General Doctor A	General Doctor	20	Permit
4	Diabetes Specialist Doctor	Diabetes Specialist Doctor	30	Permit

To request the short-term data, the receiver have to submit their attribute “Role” for obtain the permission, and the attribute should be grater and equal to 10 which is nurse. Such as the second situations, the Nurse A can hand out his/her “Role” which is equal to the asked number, 10; hence, he/she can acquire the privilege to read the short-term data. Same as the third and fourth condition, the general doctor and diabetes are the personnel whose role number is 20 and 30, the permission would be distributed and let them able to read the short-term data. However, Front Desk A who is a general staff, cannot decrypt the message since their attribute cannot accord with the predicate (Role≱10); therefore, the commitment is not helpful for the message decryption.

Table 5 The Long-Term Data Request Result Form the Different Personnel in Path 3

Short-Term Data				
	User	Role	Role Number	Result

1	Staff A	Staff	0	Deny
2	Nurse A	Nurse	10	Deny
3	General Doctor A	General Doctor	20	Permit
4	Diabetes Specialist Doctor A	Diabetes Specialist Doctor	30	Permit

The attribute requirement of the long-term data request is much strict than the querying the short-term data, where the Role has at least to be as a doctor ($Pred_2$(Role≥20)). As the situation that Front Desk A asked the long-term data, the message cannot be decoded due to the lower Role number ($Pred_2$(0≥20) = FALSE). As the same the same reason, Nurse A has been denied to decrypt the long-term data owing to the uncooperative attribute. As a general doctors or a diabetes specialist doctor, General Doctor A and the Diabetes Specialist Doctor A can accomplishedly acquired the long-term data ($Pred_2$(20≥20) = TRUE or $Pred_2$(30≥20) = TRUE).

Trough the cases listed for path 3, it can prove the condition can filter the general situations and achieve the data protection for short-term data and the long-term data.

Path 4

For the fourth path, the verifiers are swapped from senders to receivers. The verification would through the OCPE protocols which senders have to submit their attribute to CA, and then share the symmetric encryption key. Following the policy 4, I assume that the target receivers are the Insulync owned by the Alice. As the condition 3, the sender should be a doctor and have been experienced and worked in emergency call team, where the predicates are $Pred_1$(Role≥20) ∧ $Pred_2$(WE≥3). The Table 6 demonstrate the verification result by the Insulync that test whether the treatment command from the each personnel is permitted or not.

Table 6 The Verification Result of Treatment Command Form Different Personnel in Path 4

	User	Device	Role	WE	Result
1	Front Desk A	Staff	0	2	Deny

2	Front Desk B	Staff	0	10	Deny
3	Nurse A	Nurse	10	1	Deny
4	Nurse B	Nurse	10	8	Deny
5	General Doctor A	General Doctor	20	2	Deny
6	General Doctor B	General Doctor	20	4	Permit
7	Diabetes Specialist Doctor A	Diabetes Specialist Doctor	30	2	Deny
8	Diabetes Specialist Doctor B	Diabetes Specialist Doctor	30	5	Permit

The personnel in the first and third situation are not able to do the command since the working position of them and the acquired working experience are both under the minimum of the request. Though the crew of second and the forth situations have worked in the emergency call team for over 3 years, the position of them do not match the required Role. ($Pred_1(0 \geq 20)$ = FALSE or $Pred_1(10 \geq 20)$ = FALSE). In the situation 5, though the general doctors have the permission to command an emergent treatment; however, General Doctor A has merely worked for 2 years where his WE under 3, thus the key cannot be shared ($Pred_2(2 \geq 3)$ = FALSE). Same as the situation 7, the Specialist Doctor A cannot decrypt the has only attended the emergency call team for two years ($Pred_2(2 \geq 3)$ = FALSE). The only personnel who can do the command are the General Doctor B and Specialist Doctor B whose working position are both greater or equal than 20 and the obtain over 3 years working experience in the emergency call team. The above analysis of the listed situations shows the effectiveness of the policies and the conditions for the path 4, and proved that the conditions preserves the treatment command.

Chapter 6 : Conclusion

6.1 Project review

There is a pressing needed of privacy protecting on Internet of Thing (IoT) and the project aimed on improving the security problem. An introduction of several access control models and the analysis of the pros and cons of models have been given. Then the project takes the OCBE protocols which is the method mixed the Attribute-Based Access Control (ABAC) model and the Cryptography-Based Access Control (CBAC) model as the applied methodology. The project takes one of the category of IoT, healthcare system, as the scenario and employs the OCBE protocols to demonstrate how the protocols enhance the security on IoT system. In the report, we have assumed that all of the devices using in the scenario have been verified and identified by the hospital. The protocols would merely verify the privilege that users have instead of recognising the users. In the scenario, there is a reverse path that the receivers have to verify weather the senders have the privilege to give the treatment command; hence, we twisted the protocols and let the communication can be established by the share-key. After the scenario, a test report reviewing the conditions and paths has been given. Several situations have been arranged to several tables and shows weather the condition is effective.

6.2 Limitations and Future Work

The mainly limitation of the project is shortage of the realizing the system. Since the time limitation, the practical implementation cannot be done, the testing situations are merely gone through the logic thinking and artificially applied on the conditions and equations instead of running on a real system. It leads the evaluation cannot be comprehensive. Also, due to lack of the implementation, the scope of the scenario is not broad enough, because it would increase the difficulty of the artificial evaluation. Moreover, the efficiency and the effectively cannot be test by running the programme, and it spread a problem of evaluating the value of the project.

For the future of the project, implementing the programme can be one of the task for the further researchers. Also, the scope of the project can be broadened and the policies and the conditions can be extended. Moreover, the further research can employ the OCBE protocols to the other aspects of the IoT system such as the smart home or the smart city.

Chapter 7 : Reference

[1] P. C. K. Hung, J. Andrade, Y. Chen, R. Huang, M. V. Martin, Y. Zheng, P. Hung, M. Vargas-martin, J. Andrade, Y. Chen, and H. Huang, 'Research Issues of Privacy Access Control Model for Mobile Ad Hoc Healthcare Applications with XACML', *Adv. Inf. Netw. Appl. Work.*, 2007.

[2] J. Tan, *E-Health Care Information Systems: An Introduction for Students and Professionals*. 2005.

[3] S. Fischer-Hübner, *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms*. 2003.

[4] H. Leino-Kilpi, M. V. Ki, T. Dassen, M. Gasull, C. Lemonidou, A. Scott, and M. Arndt, 'Privacy : a review of the literature', *Int. J. Nurs. Stud.*, vol. 38, pp. 663–671, 2001.

[5] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, and N. Kheir, 'Internet of Things: a definition & taxonomy', in *International Conference on Next Generation Mobile Applications, Services and Technologies*, 2015.

[6] P.Brody and V.Pureswaran, 'Devicedemocracy–savingthefuture of the internet of things.', *IBM Inst. Bus. Value*, 2014.

[7] L. Atzoria, A. Ierab, and G. Morabitoc, 'The Internet of Things: A survey', *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[8] A. Witkovski, A. Santin, V. Abreu, and J. Marynowski, 'An IdM and Key-based Authentication Method for providing Single Sign-On in IoT', vol. 15, no. IEEE, 2015.

[9] S. Babar, P. Mahalle, A. Stango, and N. Prasad, 'Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)', 2010.

[10] S. Mathieson, 'NHS and internet of things: "The future of care is about the patient taking control"', *thegraduation*, 2015. [Online]. Available: https://www.theguardian.com/public-leaders-network/2015/jun/08/nhs-internet-of-things-future-care-patient-control. [Accessed: 18-Aug-2016].

[11] OWASP, 'Internet of Things Top Ten', 2014. [Online]. Available: https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf. [Accessed: 18-Aug-2016].

[12] H. Skogsrud, B. Benatallah, and F. Casati, 'Model-Driven Trust Negotiation for Web ServicesNo Title', *Identity Manag.*, vol. 03, 2003.

[13] E. Ferrari, *Access Control in Data Management Systems*. Morgan & Claypool Publishers, 2010.

[14] D. F. Ferraiolo and D. R. Kuhn, 'Role-Based Access Controls', pp. 554–563, 1992.

[15] S.-K. Chin and B. Older, *Access Control, Security, and Trust: A Logical Approach*. 2011.

[16] Z. Asaf, M. Asad, S. Ahmed, W. Rasheed, and T. Bashir, 'Role based Access Control Architectural Design Issues in Large Organizations', *Int. Conf. Open Sours Syst. Techonologies*, 2014.

[17] L. Zhou, V. Varadharajan, and M. Hitchens, 'Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage', vol. 10, no. 11, pp. 2381–2395, 2015.

[18] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, 'Attribute-Based Access Control', no. February, pp. 85–88, 2015.

[19] M. U. Aftab, M. H. Asif, and M. Irfan, 'Attributed Role Based Access Control Model 1', pp. 83–89, 2015.

[20] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, 'Guide to Attribute Based Access Control (ABAC) Definition and Considerations', *NIST Spec. Publ.*, vol. 800, no. 162, 2014.

[21] N. P. Smart, 'Access Control Using Pairing Based Cryptography', *Top. Cryptol. — CT-RSA 2003*, pp. 111–121, 2003.

[22] A. L. Ferrara, G. Fuchsbauer, and B. Liu, 'Policy Privacy in Cryptographic Access Control', 2015.

[23] A. Harrington and C. D. Jensen, 'Cryptographic Access Control in a Distributed File System'.

[24] Y. Zhu, G. A. Hongxin, and H. Huaixi, 'Cryptographic Role-based Security Mechanisms Based on Role-Key Hierarchy', *ACM ASIACCS*, pp. 314–319, 2010.

[25] J. Zhang, Q. Li, and E. M. Schooler, 'iHEMS: An Information-Centric Approach to Secure Home Energy Management', *Proc. IEEE SmartGridComm*, 2012.

[26] M. Ion, J. Hang, and E. M. Schooler, 'Toward content-centric privacy in icn: Attribute-based encryption and routing', *ACM SIGCOMM Work. ICN*, vol. 3, pp. 39–40, 2013.

[27] X. Wang and E. M. Schooler, 'Performance Evaluation of Attribute-Based Encryption : Toward Data Privacy in the IoT', in *Communication and Information Systems Security Symposium*, 2014, pp. 725–730.

[28] M. Maksimović, V. Vujovi, and B. Perišić, 'A Custom Internet of Things Healthcare System', University of East Sarajevo, 2015.

[29] D. Salvi, E. V. Mora, M. Teresa, and A. Waldmeyer, 'An architecture for secure e-Health systems', Universidad Politecnica de Madrid, 2010.

[30] Josh Holmes, 'Using IoT for Enhanced Glucose Monitoring', 2015. [Online]. Available: https://blogs.msdn.microsoft.com/partnercatalystteam/2015/06/01/using-iot-for-enhanced-glucose-monitoring/. [Accessed: 27-Jul-2016].

[31] IBM, 'Evaluating access control policies Version 8.0.0'. [Online]. Available: https://www.ibm.com/support/knowledgecenter/SSZLC2_8.0.0/com.ibm.commerce.admin.doc/concepts/caxevaluate.htm.

[32] J. Li and N. Li, 'OACerts: Oblivious Attribute Certificates', *IEEE Trans. Dependable Secur. Comput.*, vol. 3, no. 4, pp. 340 – 352, 2006.

[33] J. Li, 'Privacy Enhanced Automated Trust Negotiation', Purdue University, 2006.