HANDLING MALICIOUS INSIDERS IN AN IOT BASED ON CLOUD E-HEALTHCARE ENVIRONMENT

By

Afsheen Ahmed

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

Dec 2017

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by MS **NS Afsheen Ahmed,** Registration No. **NUST2014-63791-MMCS25214F**, of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: _____

Name of Supervisor Dr. Rabia Latif, PhD

Date: _____

Signature (HoD): _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

DECLARATION

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Afsheen Ahmed

ABSTRACT

The emergence of Internet of Things (IoTs) is introducing smart objects as the fundamental building blocks in order to develop a cyber-physical smart universal environment. The IoTs have innumerable daily life applications including healthcare industry: that has been improved to a much greater extent due to the provision of ubiquitous health monitoring along with the emergency response services and electronic medical billing. But due to the limited resources possessed by IoTs like storage and processing power, these intelligent objects are unable to efficiently provide the e-Health facilities as they are not able to process and store the enormous amount of collected data. To overcome these limitations, IoTs are merged with Cloud Computing technology. These two biggest hits in IT industry are transforming the healthcare world to a great level. Although the frameworks based on the integration of IoTs and Cloud Computing are contributing towards better patient care yet, on the contrary, they are challenging the privacy and reliability of the patients' information.

In this research work a framework, for e-Healthcare environment has been proposed in which IoTs are merged with Cloud Computing technology. This framework is operationally efficient as it deploys middleware layer on cloud. Furthermore, this framework has been made secure against Malicious Insiders attack inside Cloud by implementing the proposed Context Based Access Control System (CBACS).

The suggested CBACS protects the patients' information stored in cloud storage. This system counters the major threat of Malicious Insiders posed to the confidentiality and integrity of healthcare information by managing the access of insiders to the stored data inside cloud.

.

ACKNOWLEDGMENTS

First of all, I would like to thank Allah Almighty for His countless blessings. After that I want to express my appreciation to my family, my friends; Mohsin Tanveer and Maryam Khalid, colleagues and the faculty for providing their enormous support to help me to do this research. Without their relentless support, assistance and prayers, I would not have reached culmination point in a peaceful state of mind.

I am very grateful to my supervisor, Asst Prof Dr. Rabia Latif and Dr Haider Abbas who provided me a platform and gave me the liberty to work in the area of my interest and continuously supported me during the course of this research. Their technical guidance, encouragement, ideas and perspective were vital for completion of this tedious task. Their support gave me confidence and helped me to understand the subject matters deeply and inspired me towards my goals.

I would also like to thank Lec Waleed bin Shahid and Lec Narmeen Shafqat for being an important part of my Research Supervisory Committee. Their scholarly guidance, assistance and knowledge have been meaningful for successful completion of my research.

Finally, I am grateful and thankful to Military College of Signals and National University of Sciences and Technology for providing me a chance to help achieve excellence by being associated with the prestigious institutions.

Afsheen Ahmed,

Dec, 2017.

Table of Contents

LIST OF FIGURES

FIGURE # CAPTION……...……PAGE

LIST OF TABLES

ACRONYMS

IoT	Internet of Things
CSP	Cloud Service Provider
CBACS	Context Based Access Control System
PEP	Policy Enforcement Point
PDP	Policy Decision Point
PXP	Policy Execution Point
PIP	Policy Information Point
XACML	Extensible Access Control Markup Language
WSO2 AS	WSO2 Application Server
WSO2 IS	WSO2 Identity Server
WSO2 DSS	WSO2 Data Services Server
IDE	Integrated Development Environment
APIs	Application Programming Interfaces
PoC	Proof of Concept

Chapter 1

INTRODUCTION

1.1 Introduction

With the advancement in technology, everything is being shifted to the digital world. In today's environment of automation, daily life has become greatly dependent on the electronic devices that are there; to assist the individuals with performing their routine tasks, to help them in getting connected to the global world, to store their data and to transfer it from one end to the other. Thus nowadays it has become nearly impossible to live a good life without these amenities.

1.1.1 Internet of Things (IoTs)

In this era every entity aims to get connected by one means or another. Internet has played a vital role to do this job. Today even the devices are able to communicate to each other through internet. These devices are known as "Internet of Things (IoTs)". IoTs are designed to gather the data of their surroundings and then to transfer this collected data to the other concerned end by means of internet. Therefore they are playing an important part as sensors, cameras, RFID devices, etc. in different fields such as agriculture, traffic handling, healthcare, smart grids, smart homes and others as well.

IoTs are serving as the backbone for e-Healthcare industry as they are used to manage the patients both inside hospital and remotely. Because of the emergence of IoTs it has become possible to provide 24-hours care to patients in a better and convenient manner. In order to achieve this, IoTs transfer information on real time basis. Thus these devices have to handle large amount of generated data. But due to the limited resources of IoTs like computing power, storage and energy, they are unable to provide their services efficiently for healthcare organizations. So it is required to merge IoTs with another technology that could overcome the above mentioned limitations of IoTs to implement its concept for e-Healthcare.

1.1.2 Cloud Computing

Cloud Computing is another emerging technology that is being used by many individuals and organizations for the management of their assets and businesses. It is a shared pool of resources such as servers, storage, network and applications. Cloud Computing eliminates the need for deploying physical resources for the provision of aforementioned services. These resources are provided to the clients on pay-as-you-go basis. Based on the advantages of Cloud Computing, it can be successfully integrated with IoTs to present an efficient framework for e-Healthcare industry.

1.1.3 Security Issues in IoTs and Cloud Computing

Although IoTs and Cloud Computing are transforming the world to a great extent yet they have a number of open issues that need to be rectified before deploying the integrated framework of IoTs and Cloud Computing in a sensitive environment like e-Healthcare. Among these open issues, ensuring the confidentiality and integrity of patients' data is most challenging.

Besides other attacks that could threaten the confidentiality and integrity of healthcare information, the attack of Malicious Insiders is the most challenging one in terms of detection and prevention. It is the threat that has been rarely focused in field of IoT based Cloud e-Healthcare atmosphere. So the main aim of this research is to identify and control this threat in IoT based on Cloud e-Healthcare. In order to accomplish the aforementioned aim, an access control system is suggested in this research. This system limits the Malicious Insiders' threat inside Cloud by managing and controlling the access of Insiders to Cloud data storage.

1.2 Research Significance

This research focuses on the threat of Malicious Insiders and provides an open research area for future researchers. Along with it a solution to control this attack in an effective manner is also be presented.

1.2.1 Relevance to National Needs

This research is very useful in nature and it proposes secure framework that can be deployed in healthcare organizations in Pakistan, based on IoT and Cloud e-Health services. The proposed framework not only assists the healthcare organizations in managing the threats posed by Malicious Insiders but it will also provide a guideline to Military Organizations to tackle the risk of Malicious Insiders that could otherwise adversely affect an organization's mission.

1.3 Motivation and Problem Statement

Besides other security issues present in IoT and Cloud based frameworks that have been commonly addressed, the threat of Malicious Insiders within the cloud is the rarely focused. Malicious Insiders pose a major threat to any organization including e-Healthcare. According to 2016 cyber security intelligence index [14], 60% of all the attacks are caused by the insiders. Among this 60%, the part constituted by the malicious insiders is 44.5% which is indeed a great contribution. Malicious Insiders can adversely affect an organization's mission and reputation, and thus can cause a great harm to any business. If the malicious insiders are residing inside e-Healthcare environment then they can become the threat to the organization in the following ways:

- If a malicious insider lies inside the cloud environment, then he can easily access the patients' real-time information coming from the IoT objects and can therefore tamper this data or make it public in order to destroy the market image of a Cloud Service Provider (CSP) or the healthcare organization that is acquiring the cloud services.
- Similarly if a malicious insider is a current or former employee of the healthcare organization then he/she can modify the patient's data leading to wrong treatment of the patient thus putting a life at stake. Similarly he/she can release the health information of a patient to unauthorized entities thus violating the law of privacy.

1.3.1 Research Aims

The aims of this research include

- Proposing an efficient Framework for IoT based Cloud e-Healthcare environment.
- To identify the security issues and critically analyze the already existing techniques to handle the threat of Malicious Insiders in IoT based Cloud environment.
- To propose a framework to handle the threat of Malicious Insiders challenging the Integrity and Confidentiality of patients' health information stored in the cloud.

1.4 Contributions and Outcomes

During this research work, the contributions that have been made are shown in Table 1.1.

Table 1.1 Research Contributions and Outcomes

Contribution	Outcome
Contribution 1	An efficient framework introducing the concept of deploying middleware in cloud for IoT based Cloud e-Healthcare environment has been proposed.
Contribution 2	This research has critically analysed the threat of Malicious Insiders in IoT based Cloud e-Healthcare atmosphere which was not previously attended as a major issue by the researchers.
Contribution 3	Proposed and implemented a flexible and a scalable framework to control the threat of Malicious Insiders inside e-Health cloud.
Contribution 4	During this research work a Journal Paper about systematic literature review of Malicious Insiders threat in IoT based on Multi-Cloud e-Healthcare Environment is written.

1.5 Thesis Organization

This thesis comprises of five chapters and is organized as shown in Table 1.2.

Table 1.2 Thesis Organization

Chapter 1	It introduces the problem, motivation for research and its contribution
Chapter 2	This chapter is about the Literature Review conducted during this research. This chapter focuses on already suggested solutions to handle the threat of Malicious Insiders targeting the confidentiality and integrity of data, and the weaknesses and strengths of each proposed solution.
Chapter 3	It discusses the proposed frameworks for IoT based on Cloud e-Healthcare framework.
Chapter 4	It presents the implementation details and results of the framework that has been proposed to handle the threat of Malicious Insiders.
Chapter 5	This chapter gives the Future Directions after concluding the research.

Chapter 2

HANDLING MALICIOUS INSIDERS IN AN IOT BASED ON CLOUD E-HEALTHCARE ENVIRONMENT: A REVIEW

2.1 Introduction

This chapter is about the extensive literature review that has been conducted during the period of this research work. It highlights the applications of IoTs in healthcare industry and the merging of IoTs with Cloud Computing technology for provision of e-Health facilities in an efficient manner. It also gives an overview of the threats to which IoT based Cloud e-Healthcare framework is vulnerable. Moreover, already present solutions to handle the most occurring and rarely addressed issue: Malicious Insiders in IoT based Cloud e-Healthcare framework, is also discussed in detail.

2.2 IoTs in e-Healthcare

In this era of growing technology every entity aims to be connected and this goal is achieved by making the use of IoTs. The idea of IoTs was first given by Kevin Ashton in 1999 [1], where he described that in future, computing will rely more on data gathered by electronic objects rather than the data collected by humans. And so now the time has come when the devices are able to be identified, and are capable to capture and understand the information of their surroundings. These devices are competent enough to exchange the captured data over internet more efficiently, accurately and at a lower cost thus reducing the data loss and increasing the operational efficiency. Therefore, these devices have their applications in daily life including traffic monitoring, agricultural monitoring, healthcare, smart homes, smart grids and many more.

Due to the above-mentioned advantages, IoTs is currently playing a vital role in transforming the healthcare industry [5, 37]. Because of the deployment of IoTs in healthcare environment, patients are treated much better than ever before and at lower costs. Patient monitoring is now done on real time basis, as these devices are capable of

communicating the information continuously. Some of the practices of IoTs in healthcare industry are mentioned below:

IoTs can be used:

- To manage pharmacy, equipment and documents.
- To track patients and hospital staff through wrist bands and badges.
- To perform vital signs monitoring of patients inside hospital.
- To achieve 24-hour care of remote patients.
- To accomplish intensive care in mass casualty disasters.
- For controlling contagious infections, etc.

In spite of all these uses of IoTs in healthcare industry there is difficulty in managing the enormous amount of data generated by these objects as IoTs has limited resources; computing power, storage and energy [2, 3, 32]. So the need of the hour is to combine IoTs with some other technology [4] that would overcome the above mentioned limitations in order to provide an efficient framework for healthcare establishments.

2.3 Integrating IoTs with Cloud Computing Technology for e-Healthcare

Cloud computing is another big hit in IT industry that delivers shared pool of resources on demand including; servers, storage and applications, to different organizations. Cloud Computing integrates grid, parallel and distributed computing [4] and thus is able to provide high computation power as well as real time processing [34]. Moreover, Cloud Computing provides sufficient storage as it eliminates the need of deploying physical resources and thus one can acquire as much space as required.

Because of the aforementioned benefits of Cloud Computing, it can be successfully merged with IoTs to present a system that could be deployed for e-Healthcare services [31, 35] such as handling huge amount of data gathered by IoTs for continuous patient health monitoring, analysis of patients' records etc., economically on the basis of pay-as-you-go plan [2, 33, 36].

A general framework based on the integration of IoTs and Cloud Computing [4] for e-Healthcare organizations is shown in Figure 2.1. This framework is multi-layered and is described below.

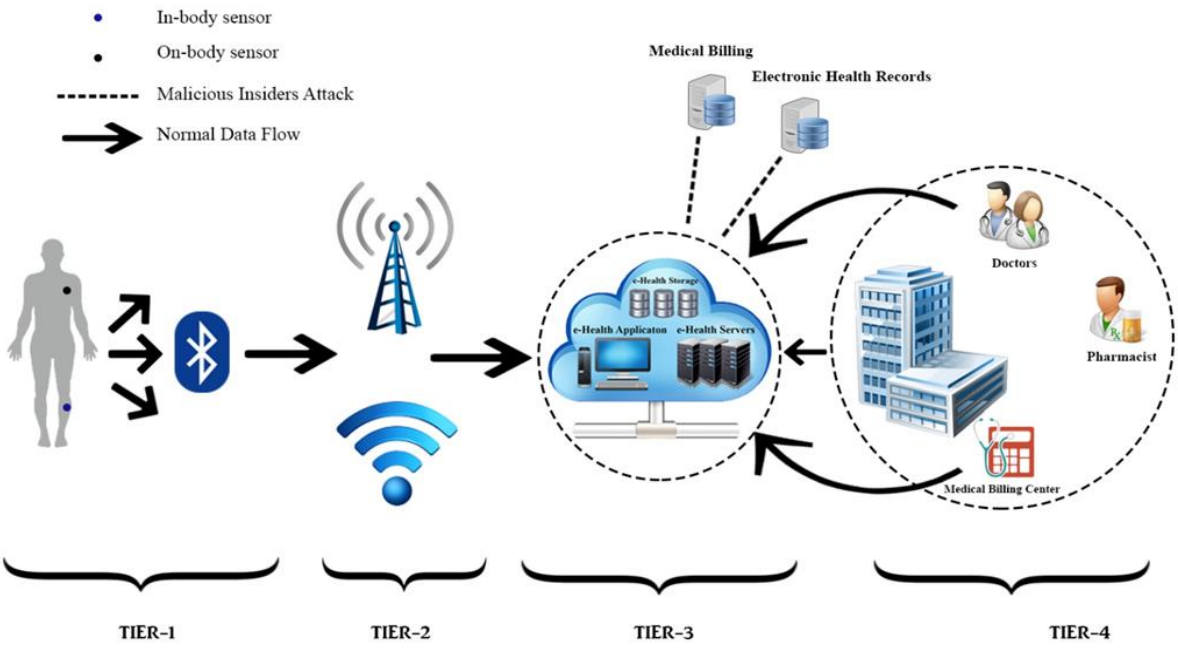

Figure 2.1 IoT based on Cloud Framework for e-Healthcare

Tier 1 represents two phases, one is information gathering phase and the other is communication subnet phase. In Phase 1, the data of the patient is collected by means of IoTs; e.g., sensors and cameras. In Phase 2, short distance communication technology including; Bluetooth, UWB, ZigBee, WiFi etc., will be used to form a peripheral network in order to transfer patient's health information to tier 2.

Tier 2 depicts two networks; Access Network and Core Network. The patients' information from tier 1 transfers to the Access Network which can be either wired or wireless medium to transmit information. Then from Access Network the data travels to the Core Network that can use anyone of the transmission technologies; Packet-based

transport network, Optical Transport Network, Synchronous Digital Hierarchy, 2G, 3G, LTE and Next Generation Network, to further transmit the health information.

Tier 3 consists of the most important part of the framework; Cloud Computing. All the patients' information from tier 2 reaches to the cloud where it is stored and further processed by CSP. This layer is capable of storing and processing huge amount of data collected in tier 1.

Tier 4 depicts that the data is transferred and is now accessible to the staff of the e-Healthcare organizations. At this stage the doctors can see the patients' health information and can provide health services and their recommendations accordingly to treat them in a suitable manner.

2.4 Security Requirements for IoT based on Cloud e-Healthcare Framework

It can be observed that the above-mentioned framework efficiently fulfils the requirements of organizing the huge amount of data generated by IoT devices. But still it cannot be used as it is for e-Healthcare industry by overlooking the most important aspect; security. The essential security requirements for e-Healthcare industry are as follow:

1. **Data Confidentiality:** The patients' data privacy should be maintained in order to keep a bond of trust between patient and a doctor, and also to conform to Health Insurance Portability and Accountability (HIPAA) privacy law; that orders to protect health information.

2. **Data Integrity:** The information related to patients' and staff working for healthcare organization should not be modified/deleted in any case in order to preserve integrity and thus to ensure better patient care along with proper working of healthcare institute.

3. **Data Availability:** The data collected by IoT devices should always be available to the concerned people in order to achieve the aim for establishing an IoT and Cloud based e-Healthcare framework that is 24/7 provision of healthcare facilities.

In order to satisfy the above security needs several solutions have been recommended. But majority of these solutions are there to ensure availability of information by combatting the attacks like DDoS that make the resources unavailable even for legitimate users. And few schemes are there to maintain confidentiality and integrity of data in IoT based on Cloud e-Healthcare Framework.

2.5 Research Questions

In order to avoid scope creep in this research and to remain stick to the topic, the rest of the literature review has been done to answer the research questions that have been formed during the review of related material detailed above.

The objective of this research was to recognize the most significant threats, risks, vulnerabilities and issues faced by IoT based Cloud e-Healthcare environment along with the present solutions to address these challenges. Following two research questions were formed.

2.5.1 Research Question RQ1

Which security attack is mainly addressed in literature review among the top security threats to confidentiality and integrity of patients' data in IoT based Cloud e-Healthcare environment?

2.5.2 Research Question RQ2

Critically analyse the existing solutions available for handling the malicious insiders' attack inside Cloud and e-Healthcare environment.

To cater the research questions, IoT and Cloud based general framework was conceptually analyzed for different types of attacks that could challenge the secrecy and validity of the medical records and other e-Health archives. Furthermore the solutions already present to combat the most challenging attack were also studied in detail to answer the research questions.

2.6 Possible Security Attacks pertaining to Confidentiality and Integrity in IoT based on Cloud e-Healthcare Framework

In order to answer RQ1, the selected material was thoroughly and conceptually reviewed. Based on these studies, the top security threats to the authenticity and covertness of patients' information and other healthcare organization records were identified. A security attack on confidentiality basically reveals health information of a patient under treatment to unauthorized individuals and thus causes a problem in not only maintaining the HIPAA privacy rule to help protect health information but also risking the issue of moral respect along with the bond of trust between a patient and a doctor. Similarly an attack on the integrity leads to the modification/deletion of patients' health information that may result in a number of serious issues related to HIPAA violations and compromised health care. Possible attacks on patients' records pertaining to confidentiality and integrity, in a general IoT and Cloud based framework are described below. Table 2.1 shows the frequencies of occurrence of these attacks in existing literature.

Table 2.1 Frequencies of occurrence of attacks on confidentiality and integrity of information in current literature

Attack Reference	Side-channel attack	Man-in-the-middle attack	Malicious Insiders attack	Session Hijacking attack
[6]	X	X	X	
[7]	X	X		
[8]	X			
[9]				X
[12]	X			
[13]			X	
[15]			X	
[16]			X	
[17]			X	
[18]			X	
[19]			X	
[20]			X	
[21]			X	
[22]			X	
[23]				X
[24]				X
[25]	X	X		

[26]	X	X		
[27]			X	
[28]			X	
[29]			X	

Most likely occurring attacks compromising the confidentiality and integrity of patients' data are defined below.

1. **Side-channel attack**: A perpetrator could attack the confidentiality of data present in the cloud by placing an attacking Virtual Machine (VM) close to the targeted VM in order to perform a side-channel attack. The attacker can then gain an unauthorized access to the patients' encrypted information by obtaining the cryptographic keys through that malicious VM, hence attacking the patients' privacy [6-8, 12, 25, 26].

2. **Man-in-the-middle attack**: This attack occurs when an attacker sits in a communication track linking two users. He can either place himself in a path connecting patient and cloud or between cloud and e-Healthcare organization. In both cases, he accesses patient's information by intercepting it or even alters this data to put its both valuable traits; confidentiality and integrity, in danger [6, 7, 25, 26].

3. **Malicious Insiders attack**: The term malicious insider [17] refers to an individual who has an authorized access to an organization's systems, annals, information and network, and who intentionally misuses his authority to negatively affect the confidentiality and integrity of health records or any other information pertaining to healthcare institute. This insider may be a present or an earlier employee of healthcare organization, a business partner or a contractor who contributes in providing healthcare services and an end user who avails these facilities. [6, 13, 15, 16, 18-22, 27- 29].

4. **Session hijacking attack**: This attack occurs through the exploitation of a valid session by attaining a session key, that leads to an illegal access to patient's data and hence to the disclosure of his information along with targeting its reliability [9, 23, 24].

Among the security attacks that could threaten the CIA (Confidentiality, Integrity and Availability) triad [11], the most important and frequently occurring risk to healthcare organizations is the Malicious Insiders threat as seen in Table 2.1.

If there are any malicious insiders in the e-Healthcare environment then they can modify the patients' data which will lead to wrong treatment of a patient and thus risking a life, or making it public and hence challenging the privacy of the patient. Moreover, amending or leaking of any other information of e-healthcare establishment by an insider can adversely affect the operation of healthcare institute and can cause a great financial loss to that healthcare business along with legal consequences.

The dotted circles in Fig. 2.1, shows the places where the threat of Malicious Insiders is most likely to take place. In an IoT and Cloud based healthcare organization, the data pertaining to patients, health staff, medical equipment and pharmacy is stored in the Cloud. Therefore, the main objective of this research becomes to secure Cloud storage from the threat posed by Malicious Insiders. So in the next section the existing solutions to combat this attack inside Cloud will be mainly focussed.

2.7 Existing schemes to handle the threat of Malicious Insiders

To answer RQ2, a thorough review was conducted on the selected papers. The detailed analysis identified the publications that contained some techniques to handle the Malicious Insiders attack. In Fig. 2.1 the dotted circles showed that where this attack could mostly occur, so the studies related to combatting this attack at those areas mainly served the purpose in answering this question: RQ2. Following are the present solutions associated with managing the malicious insiders' threat specifically in IoT based Cloud environment.

The malicious insiders' threat in the cloud

Mahajan et al. [15] has proposed a solution to ensure the integrity of the users' data kept in cloud, by getting a notification as a pop-up window whenever the file contents are being changed along with the pop-up window showing the list of changes made. A way out to protect the confidentiality of the data kept in cloud by using One Time Password (OTP), was also proposed. Whenever a rogue administrator acting as a malicious insider tries to access

some user's data, the user will be sent OTP at his registered e-mail address that would prevent illegal access to the end users' information.

A Framework to avoid vulnerability incidents in cloud computing

To provide protection against data breach, Kavyashree et al. [16] has proposed an authentic re-encryption scheme that uses attribute based encryption to control the access of users based on their attributes to information. This approach works well when users can fully trust the CSP. Moreover a disorientation scheme has been suggested that provides security against malicious insiders by detecting their suspicious access to data and in order to thwart their nefarious activities, bogus data is provided to them instead of the real one.

Detection of insider attacks in cloud based e-Healthcare environments

In this paper [19] the proposed model makes use of spatial domain watermarking technique along with the auditing methods to ensure the integrity of the medical records. These procedures are able to detect the amendments made in the patients' health documents along with the identification of the person who is responsible for modifying this data. This model has basically introduced a new feature of accountability in already proposed frameworks.

Mitigation of insider attacks through multi-cloud

With the use of multi-cloud [20]: one cloud for storing the encrypted users' data and the other for keeping the cryptographic keys, if a malicious insider gets access to the encrypted data, then he would be unable to attain the keys and vice versa. In this way the data of the organization remains protected against malicious insiders. This is one of the best ways to secure data stored in the cloud.

Context-Aware Access Control Model for Cloud Computing

In this research [38], a system has been proposed that focuses on handling managers who can perform malicious activity to steal the confidential information of an organization. This system mitigates the threat of malicious insiders inside cloud by using context (time, location and platform trust level) along with the principle of duty segregation and the method of least privilege.

Table 2.2 Review and analysis of existing solutions

Research	Reviews	Analysis
The Malicious Insiders threat in the Cloud [15]	The objectives of this paper include: learning about the insider threat in the cloud, detecting the existence of malicious insiders in the cloud and then preventing those malicious insiders to do any immoral activity in the cloud.	The author has proposed an efficient scheme to ensure the reliability of the information through sending notifications to the concerned individuals whenever the data is modified. But for confidentiality the technique of OTP has been put forward that is itself susceptible to a number of attacks including man-in-the-middle attack.
A Framework to Avoid Vulnerability Incidents in Cloud Computing [16]	This paper has highlighted a number of vulnerability incidents in cloud computing to assist the users in identifying the risks associated with those incidents. Subsequently, a framework has also been proposed in this paper that is basically focusing to provide security against data breach and malicious insiders within cloud computing environment.	In authentic re-encryption scheme, a secret key has been shared between the data owner and the CSP, which allows the cloud servers to automatically re-encrypt the data according to their own internal clocks. If this key will be compromised then the attacker can gain access to the data. The disorientation scheme will work fine only if the malicious insiders are

		detected otherwise malicious insider can compromise the confidentiality or integrity of the data.
Detection of Insider Attacks in Cloud-based e-Healthcare Environments [19]	In this paper a framework has been proposed that basically addresses the secure transmission of medical records between the healthcare organizations based on cloud. Moreover, it focuses to ensure the integrity of medical records by proposing a model that would detect any modification made in the data and the individual who is responsible for that alteration	Spatial domain watermarking has been used in the proposed model to detect any modification done in the data. But the weakness is that it can be changed by noise, compression and interpolation. So it may lead to false detection of modification even if it's not done. Moreover, the proposed solution only identifies alteration or malicious insider inside the healthcare organizations and does not cater the malicious insiders residing inside the cloud.
Mitigation of Insider Attacks Through Multi-Cloud [20]	In this paper a technique has been proposed to counter against insider attacks by the use of Multi-Cloud. The data of organization is first encrypted and then kept in a trusted cloud while the keys that are used to encrypt that	Even though the data gets secured through the proposed framework but key management issues are still there. Also some attacks like side channel attacks are possible.

	data, are kept in another cloud.	
Context-Aware Access Control Model for Cloud Computing [38]	This research work has proposed a context (spatial state, temporal state and platform trust level) based model for controlling the threat of Malicious Insiders inside Cloud.	A context based system has been proposed to control the threat of Malicious Insiders posed by managerial role only inside the cloud. No other insider roles have been taken into account while designing this scheme.

Table 2.2 consists of reviews and analysis of the existing solutions to manage the threat of malicious insiders in e-Healthcare environment based on the integration of IoT and Cloud Computing. It can be deducted from the studied literature that the existing solutions have some strengths as well as weaknesses. So the need of the hour is to propose some technique that could overcome the flaws of the existing schemes in order to fight against this Malicious Insiders threat.

2.8 Conclusion

This chapter shows that how better patient care can be achieved by making usage of integration of two emerging technologies; IoTs and Cloud Computing. Besides the commonly arising security issues related to maintaining confidentiality and integrity of e-Health data are also brought to light. Moreover this chapter discussed the need of proposing a solution for controlling the most challenging threat; Malicious Insiders in an IoT based on Cloud e-Healthcare Framework as the existing solutions focus more on handling this threat either inside Cloud or inside e-Healthcare.

Chapter 3

PROPOSED FRAMEWORKS FOR IoT BASED ON CLOUD E-HEALTHCARE ENVIRONMEMT

3.1 Introduction

This is the most important chapter of this research work as it describes the two frameworks that have been suggested in this research. Firstly the overall framework proposed for IoT based on Cloud e-Healthcare environment will be represented. And secondly framework designed to handle the threat of Malicious Insiders inside Cloud in an IoT and Cloud based e-Healthcare atmosphere will be detailed.

3.2 IoT based on Cloud e-Healthcare Framework

Among the present frameworks, a framework proposed by Rui and Danpeng [4] will be considered for this research. The main reason to select this framework is the increased operational efficiency of IoTs based on the implementation of Cloud on middleware layer of the proposed framework. The chosen framework has been deployed for different applications; traffic monitoring, agriculture monitoring etc. But deployment of this framework in e-Healthcare environment is still an open area of research. So, in this research work the selected framework has been deployed for e-Healthcare.

Figure 3.1 depicts the proposed framework for IoT based on Cloud e-Healthcare environment.

This framework consists of the following layers.

1. **e-Health Aware Layer:** This layer is further divided into two other layers: data gathering layer and data communication layer. Data gathering layer collects data from IoT devices; RFID tags (medicines, surgical equipment, documents), RFID badges (medical staff) and wrist bands (patients), WSN (vital signs monitoring of

patients inside hospital), and WSN and Cameras (remote patients monitoring). The Data gathering layer comprises of short distance technology used for communication purpose such as ZigBee, Wi-Fi, UWB and Bluetooth to communicate the e-Health data gathered by IoT devices to the next layer.

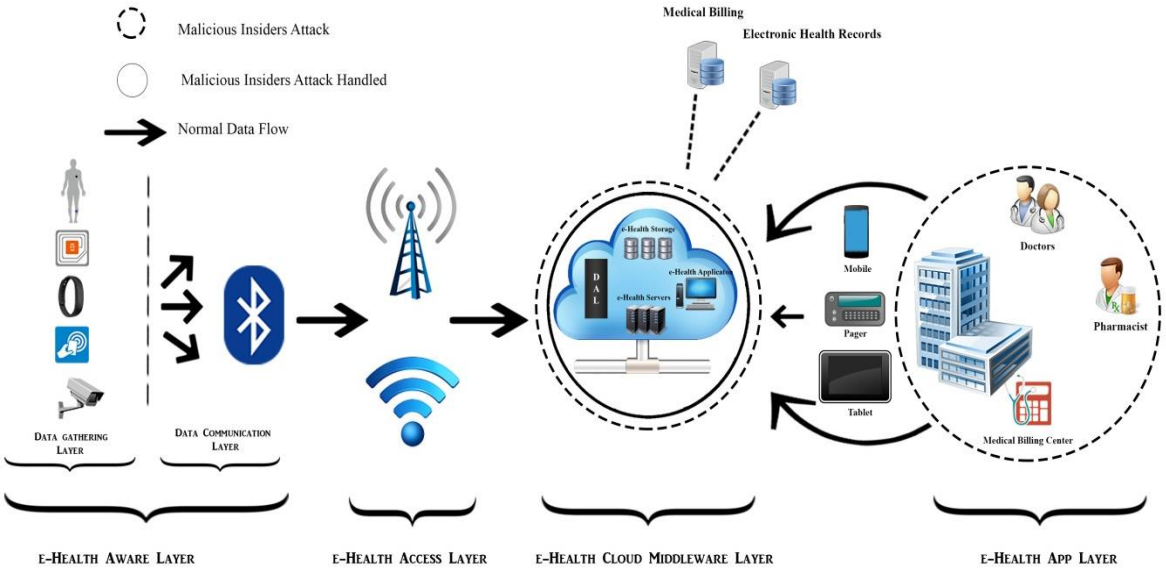

Figure 3.1 Proposed IoT based on Cloud e-Healthcare Framework

2. **e-Health Access Layer:** depicts two networks; Access Network and Core Network. The e-Health data from E-Health Aware Layer transfers to the Access Network which can be either wired or wireless medium. Then from Access Network the data travels to the Core Network that can use anyone of the transmission technologies; Packet-based transport network (PTN), Optical Transport Network (OTN), Synchronous Digital Hierarchy, 2G, 3G, LTE and Next Generation Network, to further transmit the e-health information.
3. **e-Health Cloud Middleware Layer:** consists of the most important part of the framework; Cloud Computing based Middleware Layer. All the patients' information from layer 2 reaches to this layer where it is stored and further processed by the Cloud Service Provider. This middleware layer based on cloud is capable of storing and processing huge amount of data collected from layer 1. The middleware

layer consists of cloud's hardware, software, management and application architecture.

4. **e-Health Application Layer:** This layer includes the e-Health applications such as; Searching patients' health information, Knowing current location of medical staff, Medical billing information, Checking of short medicines, etc. that have been developed to provide the collected data to the concerned end users.

3.2.1 Significance of the Proposed IoT based on Cloud e-Healthcare Framework

The suggested framework will competently provide e-Healthcare amenities to the end users including patients and healthcare staff. It promises better patient care as it communicates real time data collected by IoT devices. It also overcomes the limitations of IoT devices such as storage by integrating IoTs with Cloud Computing technology. Moreover implementing middleware layer services on Cloud increases the operational efficiency of this framework.

3.2.2 Malicious Insiders attack on the Proposed Framework

In Figure 3.1, the dotted circles show that where the malicious insiders attack is possible. It can be seen that this attack can take place anywhere in the proposed framework. But this threat is most likely to occur inside cloud where data gathered by IoT devices is stored. Thus it becomes extremely important to handle this threat inside cloud where a malicious insider can compromise the confidentiality and integrity of the stored data. Therefore in the next section a framework will be proposed to control the threat of Malicious Insiders inside IoT based Cloud e-Healthcare atmosphere.

3.3 Context Based Access Control System (CBACS)

CBACS is the framework that has been proposed to control the threat of Malicious Insiders inside Cloud in aforementioned e-Healthcare framework in order to preserve Confidentiality and Integrity of patients' information and other e-Health data received via IoT devices: RFID tags, RFID wrist bands, RFID badges, and Wireless Sensors for monitoring remote patients as well as patients admitted in hospital.

CBACS is XACML based flexible access control system that has been designed to limit the access of insiders in order to minimize the probability of any malicious activity suspected by

these insiders. This system is using the integration of Role Based Access Control (RBAC) and Context Aware Access Control (CAAC).

RBAC is used to provide security in the computer systems and networks by restricting the access to the resources based on the roles played [43] by individuals in an organization. It can implement both Mandatory Access Control (MAC) and Discretionary Access Control (DAC). It has been adopted by most of the businesses to provide access control. Microsoft Azure Cloud platform also provides RBAC for users.

CAAC provides access based on contextual information gathered. Context [39] is basically defined as any information that is used to identify the current condition of an object or an entity. This information can be about time, location, temperature, connectivity of network, noise, etc.

The proposed system in this research is mainly dependent on the policies defined for each role considering different conditions of the environment (time, location and information to be accessed). Healthcare organizations can create, update or delete the policies according to their requirements. The defined policies are about the data stored in the Cloud storage so to protect Confidentiality and Integrity of this stored information.

In order to access the stored data in Cloud, the authenticated users should be authorized by the CBACS to obtain the required information. Figure 3.2 shows the Cloud Data Storage and CBACS along with the operations that the users' access requests go through to gain access to the stored data. Figure 3.3 gives the details of the operations performed by the proposed access control system in a sequential manner. It shows the sequence of operations carried out to authorize a user to access the desired data. From the access request made till the permission granted or denied based on the defined policies in Policy Repository, are shown in this figure.

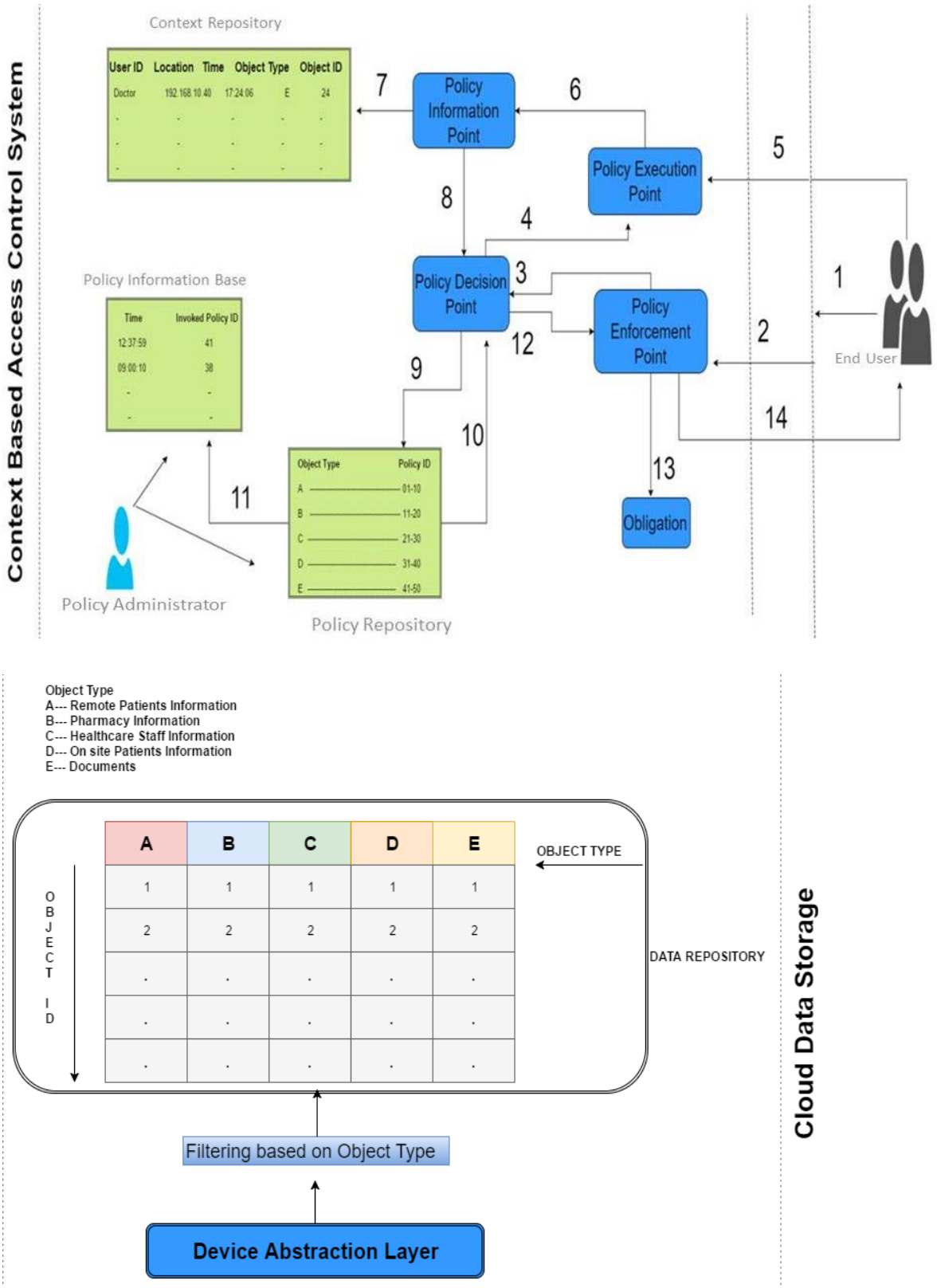

Figure 3.2 Proposed Context Based Access Control System (CBACS)

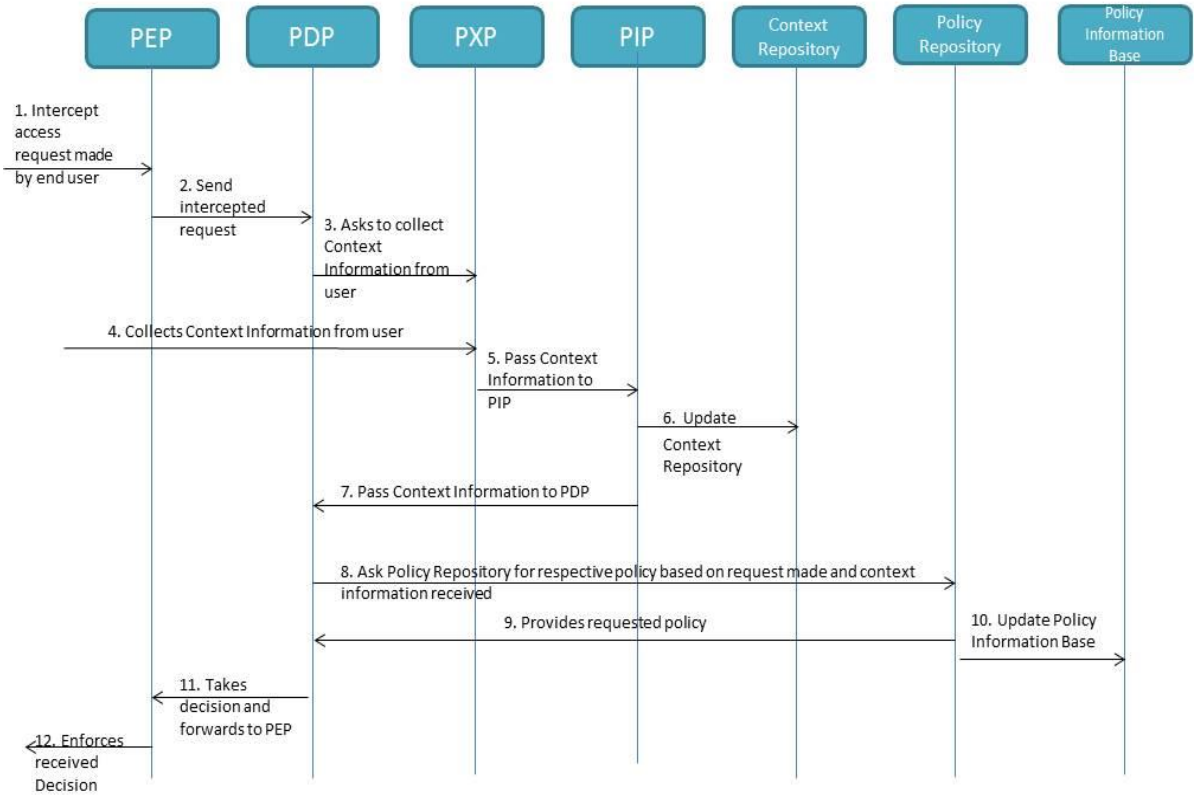

Figure 3.3 Sequence Diagram of CBACS

3.3.1 Cloud Data Storage

Cloud Data Storage consists of three important parts. The description of each part is given as follows:

1. **Device Abstraction Layer (DAL):** The DAL [40] is the first part of Cloud Data Storage and is responsible to collect all the real time data gathered by different IoT devices shown in Figure 3.1. The Core Network interacts with this layer of Cloud to deliver the collected data to data repository.
2. **Object Type Filter:** The data gathered by DAL is filtered on the basis of Object Type [41] by Object Type Filter. Object Types used in this framework are listed below.

   Object Type A Remote Patients' Information

   Object Type B Pharmacy and health equipment information

Object Type C	Healthcare Staff Information
Object Type D	On Site Patients' health information
Object Type E	Documents

After Filtration the data goes to the desired columns of data repository.

3. **Data Repository:** This is the last part of Cloud data storage where the data according to their Object Types are stored. It consists of a database which has a front end showing Object Types in columns and Object IDs in respective rows. Object ID is unique for each data object stored in the database. A data object [41] is the information related to one particular identity; patient, medical staff, equipment and medicine. For example: patient ABC's health, billing information, prescription given to XYZ patient, surgical equipment, insulin, etc. To view, add, delete or modify any information stored, the associated Object ID with an entity must be entered.

3.3.2 The Architecture of CBACS

The Context Based Access Control System is a complex but a flexible system. It is XACML based framework that uses the below mentioned components of XACML standard in order to protect Confidentiality and Integrity of e-Healthcare data gathered by IoT devices from being compromised by Malicious Insiders. Furthermore it will also provide Accountability by detecting the authorized users responsible for performing any nefarious activity pertaining to loss of Confidentiality and Integrity of any e-Health information. This system permits the Cloud personnel to access data stored in the Cloud based on the context information collected and not only on the roles of the individuals on the basis of defined policies. So this system can also cater malicious insiders even if they have the highest privileges among the roles defined.

The components of CBACS are described as follows:

1) **Policy Repository:** Policy Repository consists of pre-defined context aware policies based on the object type. One object type can have a number of policies and it depends upon the requirement of the e-Healthcare organization. Each policy is stored with a unique policy ID and is called with the help of this ID based on the received context information. It is managed by Policy Administrator. The Policy

Administrator cannot modify the Policy Repository without informing higher authorities of e-Healthcare organization.

2) **Context Repository:** Context Repository stores the context information of every request made. Context information is stored in the form of ID of the user who made the request, Location of the user like IP address, Time at which the request has been made, request made to access which object type and data object. The context information along with the type of the Policy triggered can help in ensuring accountability.
3) **Policy Information Base:** Policy Information Base keeps the record of policies triggered. The record in Policy Information Base is maintained by showing the invoked policy against the time at which it has been triggered. Along with the Context Repository, it is required to ensure accountability and to make better access policies.
4) **Policy Decision Point (PDP):** It is the main component of the Context Aware Access Control System. It interacts with [42] Policy Enforcement Point to receive the request made and to enforce the final decision. It tells Policy Execution Point to collect the context information when a certain request has been made. It collects the context information from Policy Information Point. Based on the request made and context information received, it asks Policy Repository for the respective policies. And then finally it takes the decision based on the defined policy and forwards it to Policy Enforcement Point to execute it. If it has decided to take any additional action like sending notification or email, it probes Policy Execution Point to do it.
5) **Policy Enforcement Point (PEP):** It intercepts the request made and forwards it to PDP and finally enforces [42] the decision made by PDP. It is further associated with obligation that defines whether read, write or execute permission is given.
6) **Policy Execution Point (PXP):** It collects the context information from the cloud personnel who have made a demand to access some healthcare data stored in data repository and forwards [42] it to Policy Information Point. Moreover, it is also responsible to execute additional actions like sending notifications or emails to the concerned physician.

7) **Policy Information Point (PIP):** It collects context information of the cloud personnel from PXP and forwards it to PDP and updates [42] this information in Context Repository for future use.

These components are shown interacting with each other in Figure 3.2.

3.3.3 Policies

The policies are created and managed by the Policy Administrator. These policies are stored in Policy Repository against the object type for which they are formed. Each policy has a unique ID by which it is called. In case of policy deletion, this unique policy ID is also deleted and cannot be given to any other policy generated. With the help of policy ID it can be tracked that if any policy has been removed without informing the higher authorities in order to limit the malicious activity at policy administrator's level.

The policies are defined in XACML language. XACML is an XML-based language [44] for the provision of access control. It is a standard of the OASIS Consortium. For defining XACML policies, conditions are set by defining Resource, User, Action and Environment.

- **Resource:** It is the entity that is to be protected by the use of access control policies.
- **User:** It is the user whose access is controlled by forming access control policies.
- **Action:** It is the permission given to user to access the resource. It can be read, write, and update or delete permission.
- **Environment:** It is the defined time, location or any other factor that is considered to control users' access to the resources.

In CBACS; Resource means Data Repository, User is any healthcare staff, patient or third party that has an authenticated access to healthcare data, Action consists of viewing, modifying, adding or deleting of e-Health data, and Environment consists of time and location (internal or external network).

3.3.4 Significance of CBACS

CBACS uses the integration of role based and context aware access control systems. It can be adopted by an IoT based on Cloud e-Healthcare environment to control the malicious

insiders in a more restricted manner in order to ensure the Confidentiality and Integrity of healthcare information for complying with HIPAA privacy law, to maintain the image of organization and to remain safe from any financial loss and legal consequences.

3.4 Conclusion

In this chapter two frameworks have been suggested. One is the overall IoT and Cloud based e-Healthcare framework that shows that how the data from IoT devices will be transferred to the Cloud to provide e-Health facilities efficiently. Moreover in this framework the need for handling Malicious Insiders threat in an IoT based on Cloud e-Healthcare atmosphere has been highlighted by showing that where this attack could occur. The second framework that has been proposed is CBACS. The purpose of this framework is to control the threat of malicious insiders in the framework formerly suggested.

Chapter 4

IMPLEMENTATION AND RESULTS

4.1 Introduction

This chapter gives a proof of concept regarding the proposed CBACS in chapter 3. First of all, a way to implement CBACS is discussed. Secondly the results of the implemented framework are presented along with the discussion about the attained results.

4.2 Implementation

For providing the proof of concept, CBACS has been implemented using WSO2 middleware platform [45]. WSO2 offers open source products that give the ability to digital businesses to move quickly and easily from one platform to another based on their needs. It provides a complete integrated platform where different facilities are delivered to the businesses for building, managing, securing, integrating and analysing their applications, web services and APIs- in Cloud, on- sites, across IoTs and on mobile devices.

Following products of WSO2 have been used to give an idea of implementing CBACS by creating and securing a Cloud Web App.

- WSO2 Developer Studio
- WSO2 Data Services Server
- WSO2 Application Server
- WSO2 Identity Server

4.2.1 Creating E-HealthcareApp

Among the products provided by WSO2 platform, WSO2 Developer Studio is used to design the web Apps. It delivers Eclipse based IDE. A dynamic web app has been created using Eclipse IDE. Following are the steps followed to design front end and back end of web application. This web application performs two functions: Register a patient that is to

perform write function and Search patient details by patient ID that is to perform read function.

1) First of all dynamic web project is created with a name “E-HealthcareApp”. Figure 4.1 shows the components of this project

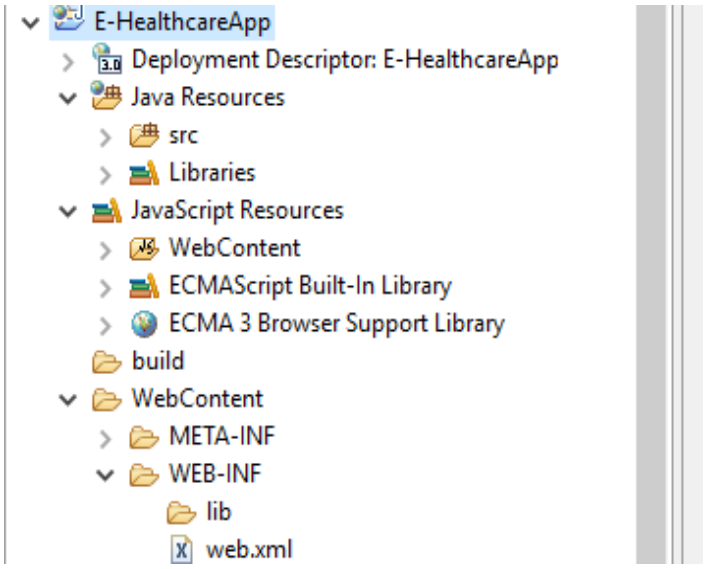

Figure 4.1 Created Dynamic Web Project with name “E-HealthcareApp”

2) Front end pages are designed, the details of which are shown in Figure 4.2.

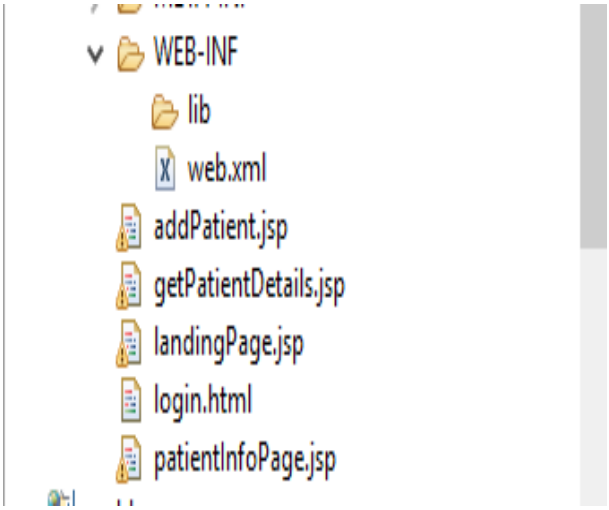

Figure 4.2 Front end pages

3) Back end is designed using MySQL workbench. A database has been created with a name “patient.db”. The created database is shown in Figure 4.3.

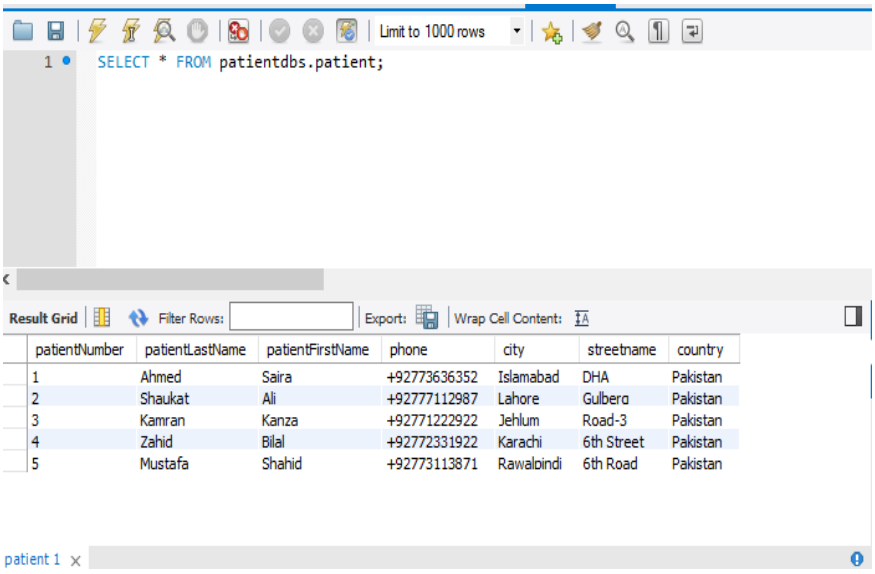

Figure 4.3 MySQL backend Database

4) After creation of database, it is now the time to expose the database tables as web services. For this purpose WSO2 Data Services Server is used. Figure 4.4 shows that the database has been exposed as a web service using WSO2 DSS.

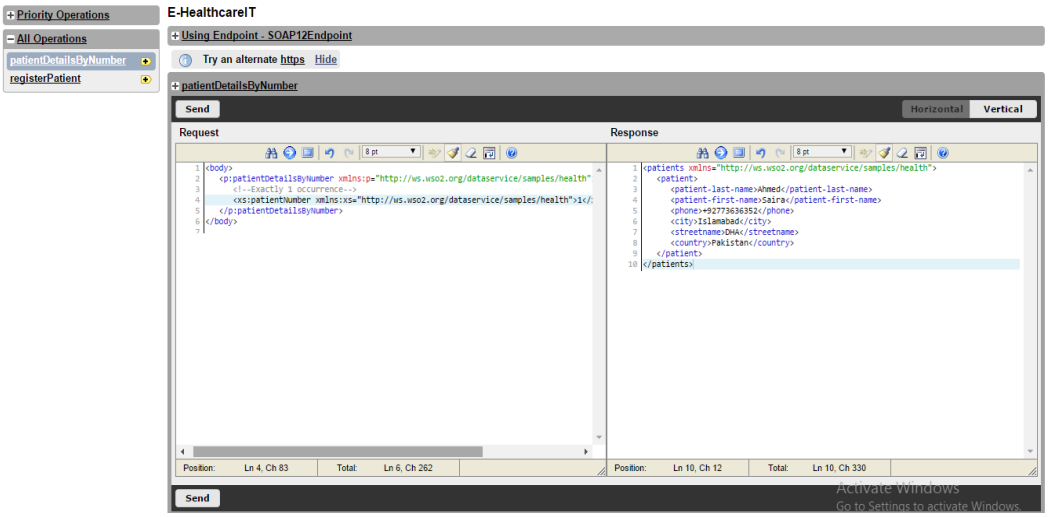

Figure 4.4 a) Query Patient Details Web Service

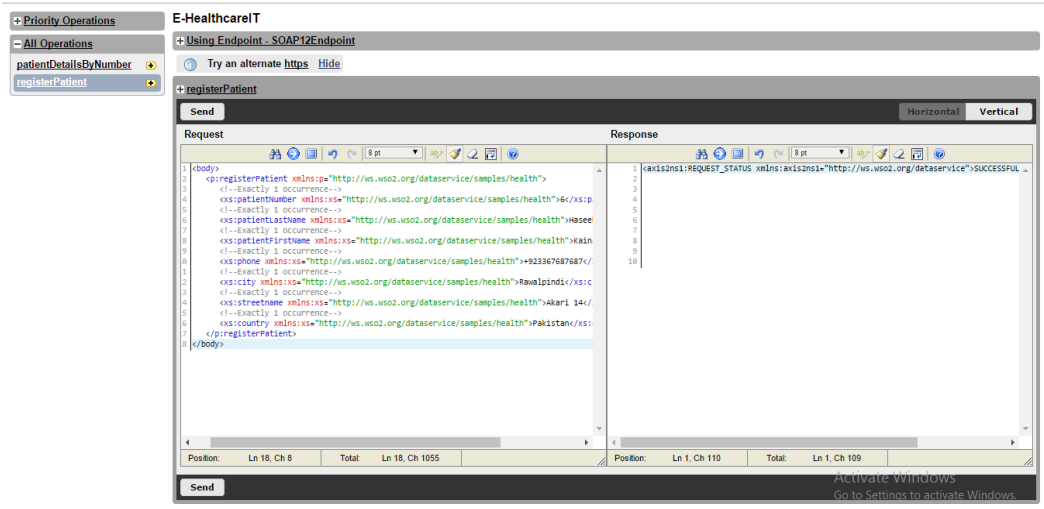

Figure 4.4 b) Register Patient Details as Web Service

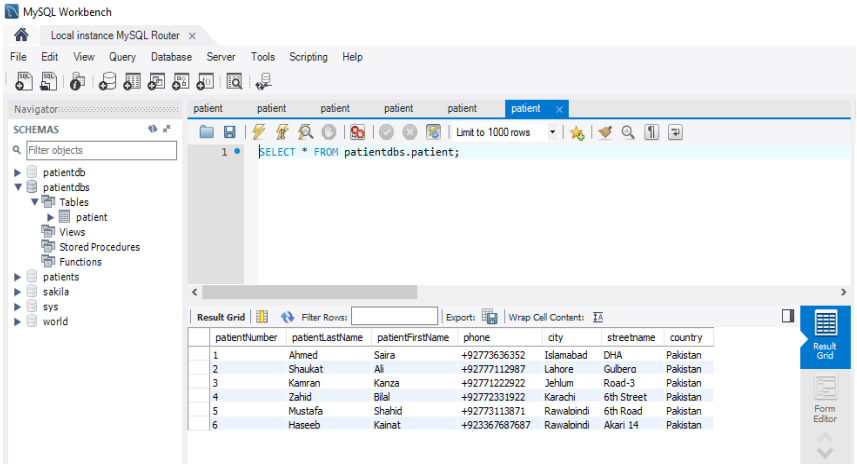

Figure 4.4 c) Resultant Database

5) Now the next step is to implement servlets is a web app to call data services exposed in the earlier step. Figure 4.5 shows the servlets that have been implemented to call data services. These servlets are QueryPatientDetailServlet.java and RegisterPatientServlet.java.

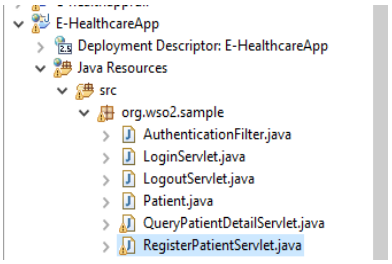

Figure 4.5 Servlets to call Data Services

6) The next step is to compile a .WAR file and deploy it on WSO2 Application Server to make it a cloud web app. As WSO2 AS is a cloud native that is used to provide firm basis for hosting shared, multitenant and scaling SaaS applications. Figure 4.6 shows that E-HealthcareApp.war has been deployed successfully on WSO2 AS.

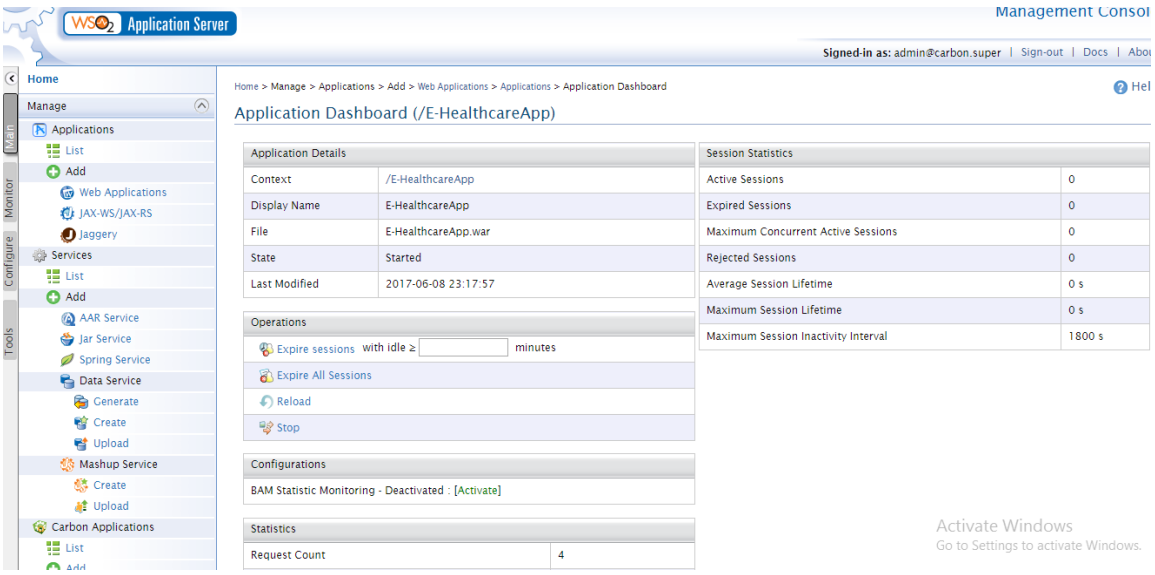

Figure 4.6 Deployed E-HealthcareApp.war

4.2.2 Implementing Security in E-Healthcare App

After creating a simple cloud web app, the next step comes that is the main thing that should be done in order to provide proof of concept for CBACS. This section introduces security in the cloud web app created. The security will be implemented in two phases.

- Authentication
- Authorization

Both these services will be provided by WSO2 Identity Server. Authentication will be done by defining roles and users in WSO2 IS and authorization is accomplished by defining context based XACML policies in WSO2 IS against the roles defined. Firstly introduction of authentication in the created E-Healthcare App will be discussed.

1) The first step is to define roles in WSO2 IS. For this E-Healthcare App two roles have been defined namely: Read role and Write role. Figure 4.7 shows the roles created.

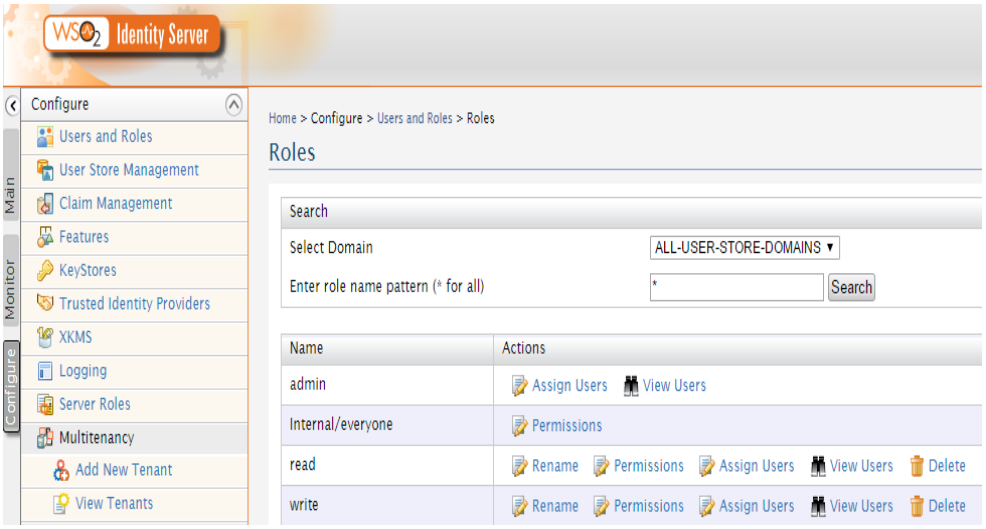

Figure 4.7 Defined Roles in WSO2 IS

2) The next step is to define users and assign them the roles created. Figure 4.8 shows the created roles in WSO2 IS.

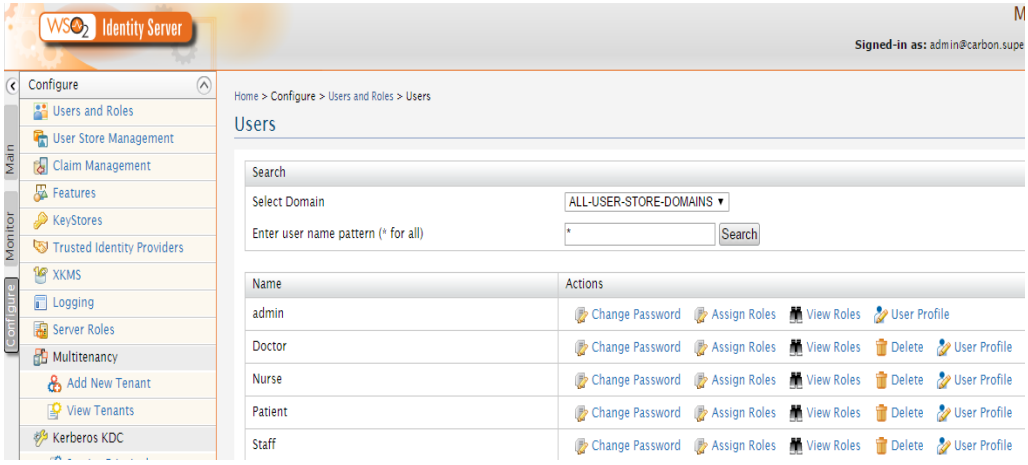

Figure 4.8 Assigned Roles to Users in WSO2 IS

Table 4.1 shows the roles that are assigned to each user created.

Table 4.1 Users and Roles

Users	Roles
Doctor	Read, Write
Staff	Write
Nurse	Read
Patient	Read

3) The next step is to make modifications in the web app in order to ask it to perform authentication first before giving access to the main page of the E-Healthcare App. It can be done by adding login.html, Login Servlet, Logout Servlet and Authentication filter in the app and declare these servlets in web.xml. Figure 4.9 shows the modification made. The additions made for authentication purpose are highlighted.

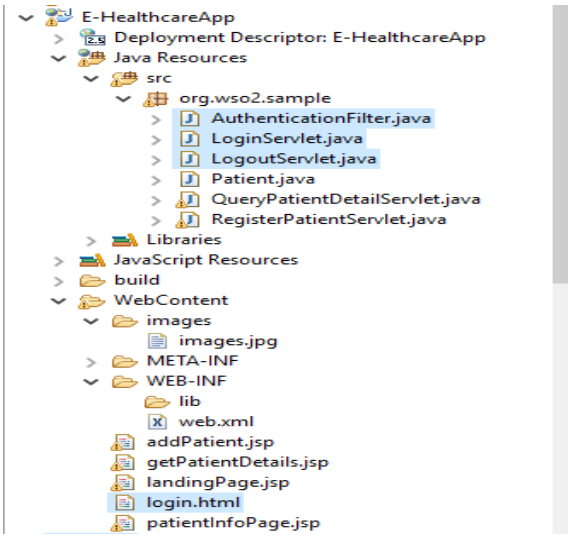

Figure 4.9 Modifications made for Authentication Purpose

4) After introducing the authentication function, the next step is to add the authorization operation. This can be done by writing XACML policy and apply it to the roles and the users defined in order to control their access to the patients' records. WSO2 IS will implement the policies on the resource by calling already defined Entitlement

Filter in WSO2 AS. During runtime this filter will be exposed to E-Healthcare App and filtering will be done on basis of policies defined.

5) New XACML policy is written using simple policy editor in WSO2 IS. Figure 4.10 shows the written policy in XACML.

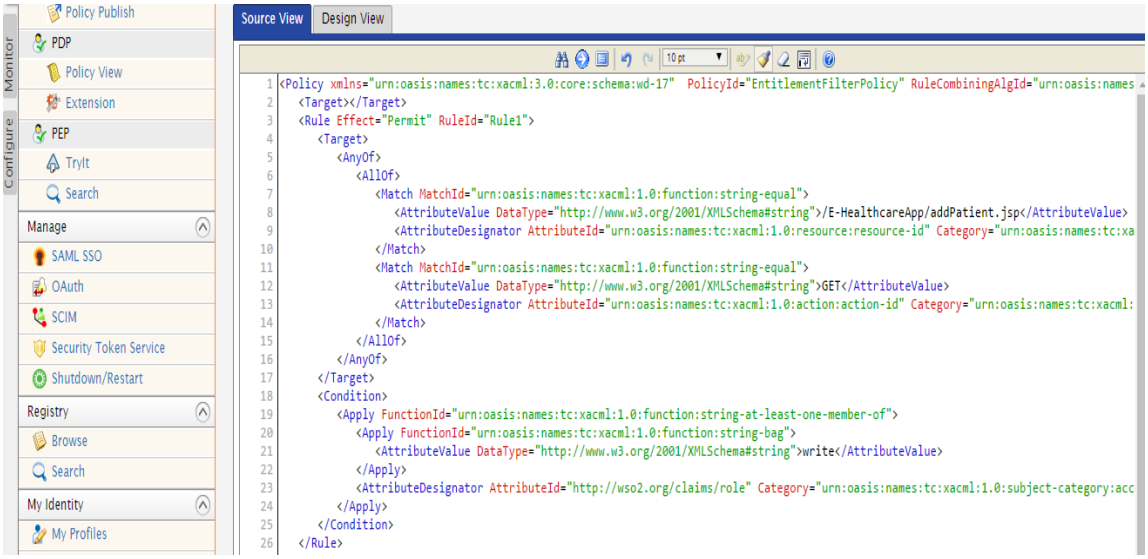

Figure 4.10 XACML Policy

6) After writing XACML policy it is published to my PDP and then enabled. Figure 4.11 depicts that the policy is published and is enabled.

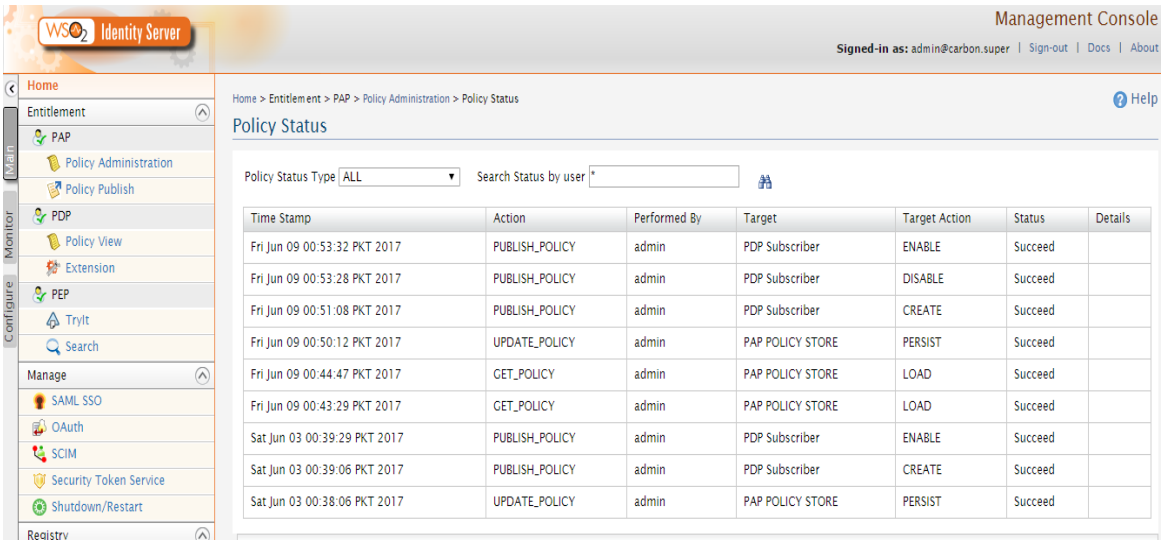

Figure 4.11 Published and Enabled XACML Policy

4.3 Results

After implementing XACML based E-Healthcare App, it is now the time to check the deployed cloud web app in WSO2 AS. After opening the URL of E-HealthcareApp mention in Figure 4.6, we land on to the Login Page shown in Figure 4.12.

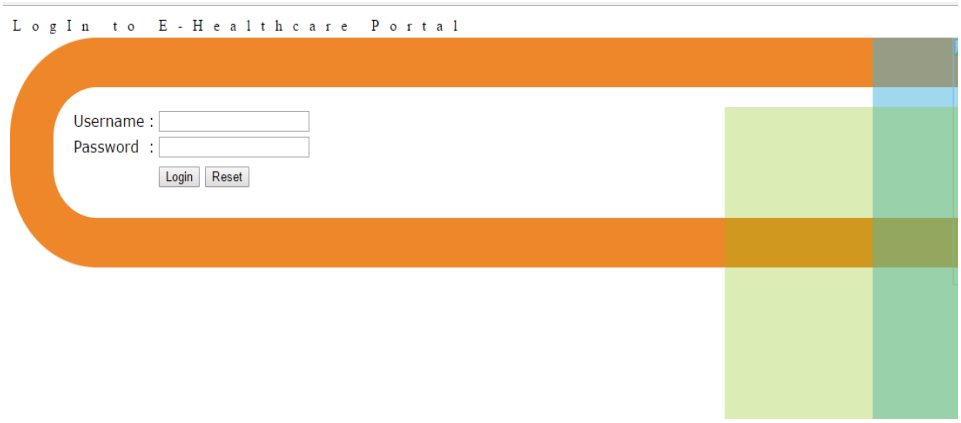

Figure 4.12 Login Page of E-HealthcareApp

If we enter correct username and password defined in WSO2 IS then we will be authenticated successfully and will be landed to the next page that is landingPage.jsp, otherwise entering either wrong username or password will bring us back to Login page along with showing Error, Figure 4.13 shows the successful and unsuccessful authentication.

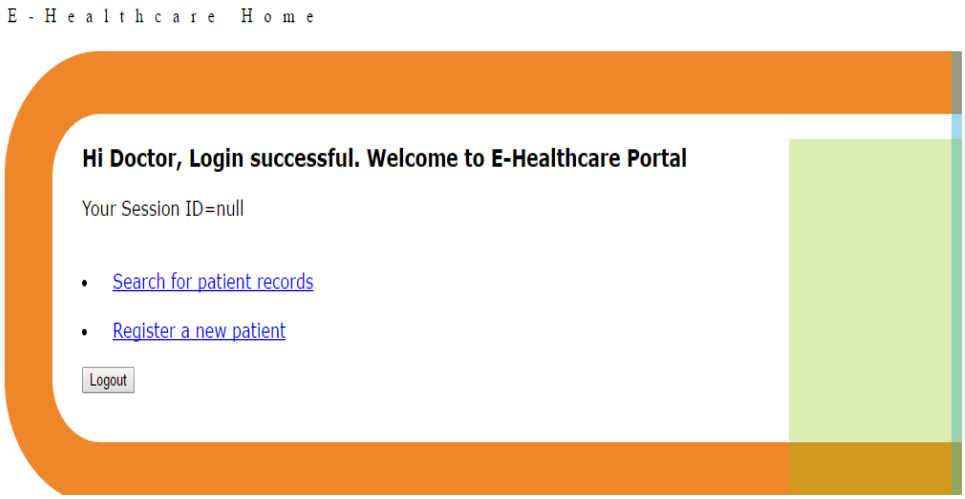

Figure 4.13 a) Successful Authentication

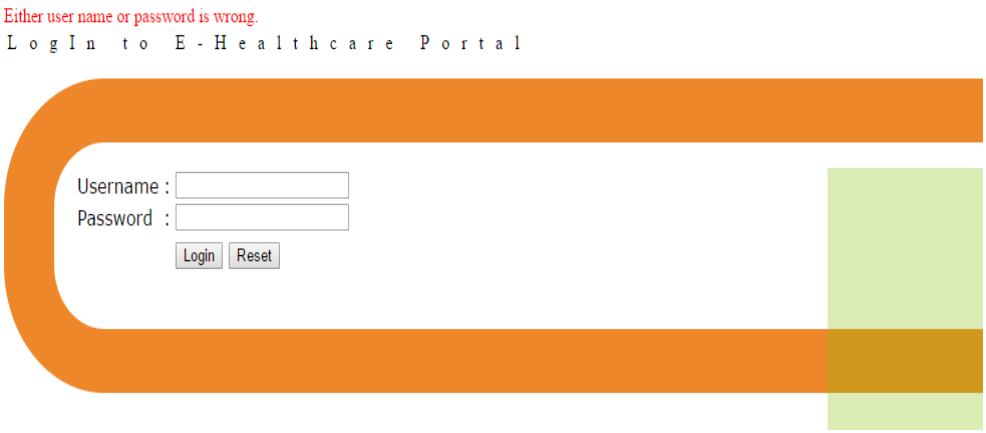

Figure 4.13 b) Unsuccessful Authentication

After authentication, the Doctor is directed to the landing page where two options are available; search patient records and register new patient. As the doctor has been assigned both read and write roles, so he is capable of performing both functions mentioned on the landing page. But here comes authorization that is done on basis of defined XACML policies. If the doctor passes the authorization stage and given permission to perform above functions, only then he will be redirected to next pages otherwise he will be returned to login page. Figure 4.14 shows permission granted and permission denied.

Figure 4.14 a) Search Patient Records page

If the Doctor clicks on Search patient records, then he is directed to the page mentioned in Figure 4.14 a). If he enters a valid patient id then information pertaining to that patient will be shown. This is shown in Figure 4.14 b).

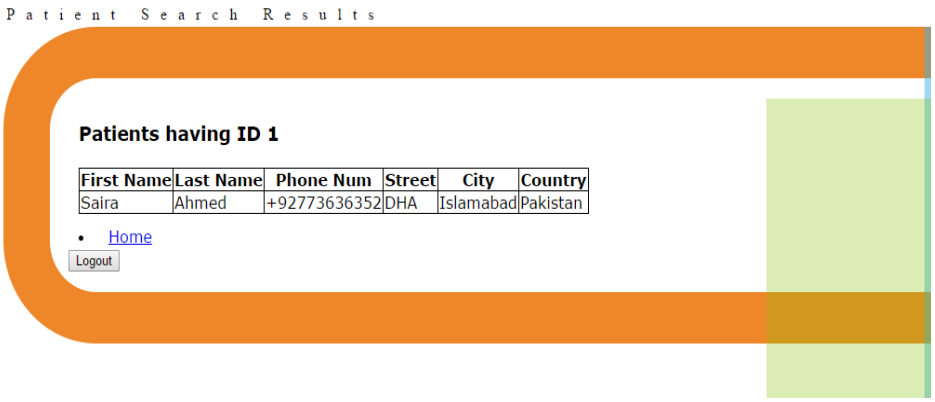

Figure 4.14 b) Record of Patient having ID 1

If a Doctor, clicks on Register New Patient, then after permission given, he will be directed to the page shown in Figure 4.14 c)

Figure 4.14 c) Register New Patient Page

Here the Doctor enters the information of a new patient that is shown in Figure 4.14 d).

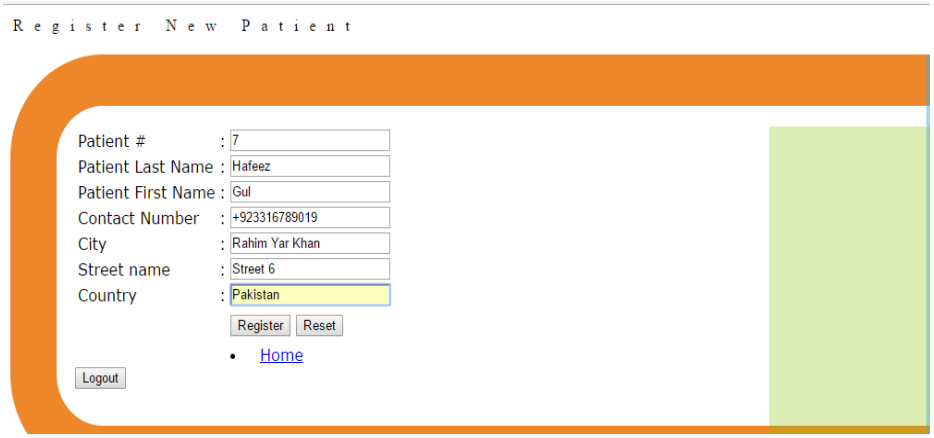

Figure 4.14 d) New Patient's Information

If the registration is successful as shown in Figure 4.14 e), then this entered data will be transferred to the backend database as depicted in Figure 4.14 f).

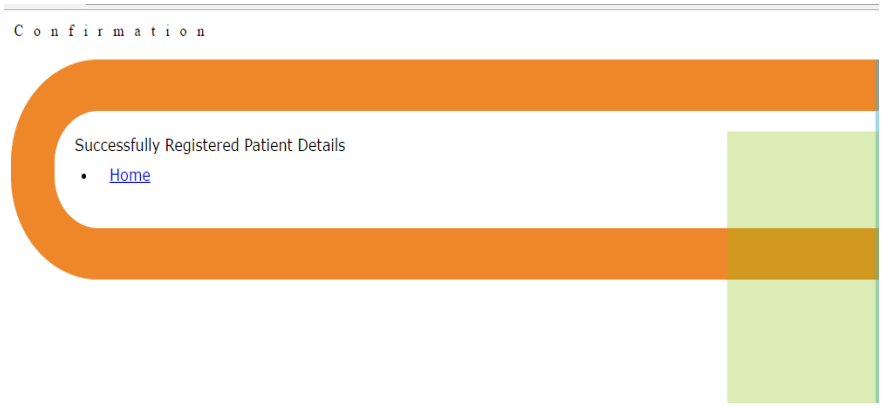

Figure 4.14 e) Patient Registered Successfully

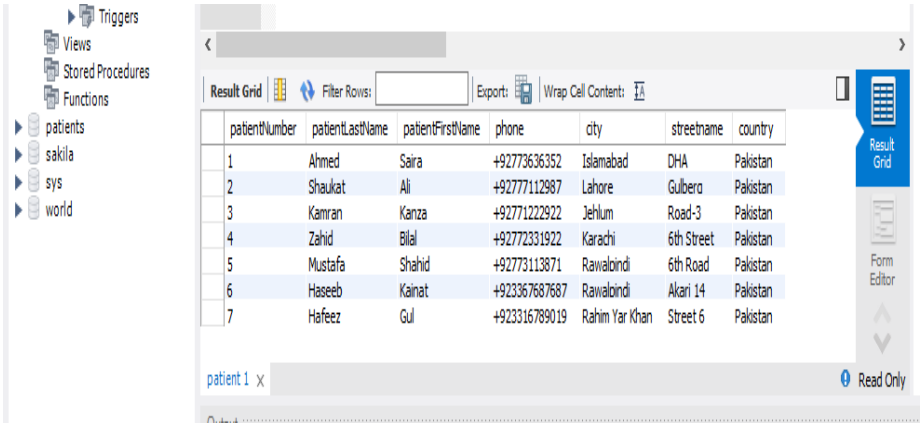

Figure 4.14 f) Registered Patient Details in Database

If a Nurse tries to view patient records then she will be directed to the page shown in Fig 4.14 a). But if she wants to register a new patient then she will be returned to the login page. This redirection means that the access request made by Nurse to enter new information is denied as mentioned in XACML policy defined.

Likewise, according to enabled XACML policy if patient having ID 1 wants to read information of patient having ID 2 or any other than ID 1, then he will be redirected lo login page because the permission to access this resource by this subject is denied.

4.4 Discussions and Analysis

In the discussion phase different scenarios are presented along with XACML policies made for that scenario. These scenarios are formed on the basis of the users and roles declared in Table 4.1. These policies are role and time based.

4.4.1 Scenario 1

A Doctor is able to read patients' information all the time but is restricted to write any information after 17:00 hrs. The XACML policy defined for write role of doctor is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="authn_time_and_role_based_policy_template" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable" Version="1.0">
  <Description>This policy template provides ability to authorize users to a given service provider(defined by SP_NAME) in the authentication flow based on the Roles of the user (defined by ROLE_1 and ROLE_2) and the time of the day (eg. between 09:00:00 to 17:00:00). U
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/E-HealthcareApp/addPatient.jsp</AttributeValue>
          <AttributeDesignator AttributeId="http://wso2.org/identity/sp/sp-name" Category="http://wso2.org/identity/sp" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
        </Match>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">authenticate</AttributeValue>
          <AttributeDesignator AttributeId="http://wso2.org/identity/identity-action/action-name" Category="http://wso2.org/identity/identity-action" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule Effect="Permit" RuleId="permit_by_roles_and_time">
    <Condition>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
        <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:time-in-range">
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
            <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment" DataType="http://www.w3.org/2001/XMLSchema#time" MustBePresent="true"></AttributeDesigna
          </Apply>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">09:00:00</AttributeValue>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">17:00:00</AttributeValue>
        </Apply>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-is-in">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
            <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
          </Apply>

        </Apply>
      </Apply>
    </Condition>
  </Rule>
  <Rule Effect="Deny" RuleId="deny_others"/>
</Policy>
```

In this scenario doctor has been restricted to edit any information of the patient after 17:00 hrs. This policy is defined for the sake of limiting any malicious actions aimed by the doctor. Because of this the doctor will not be able to modify patient's data from another location other than the healthcare organization. Moreover, no other individual with doctor's credentials will be able to alter the data accessible by the role of a doctor from any other

location. But if the doctor needs to make some amendment in the patient's data from his office after 17:00 hrs, then in this case another policy will be triggered that will allow the doctor to take this action. Along with this policy another policy will be executed that defines that whenever a patient's data is altered, he will get a notification. So due to this action the patient can report to higher authorities that his data has been modified without his visit to the doctor.

4.4.2 Scenario 2

The Nurse will be allowed to read information of the patients' till the time she leaves the hospital. Suppose a Nurse 1 leaves hospital at 10 a.m. so after that she will not be able to read any patient's information. The XACML policy defined for read role of Nurse 1 is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="authn_time_and_role_based_policy_template" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable" Version="1.0">
  <Description>This policy template provides ability to authorize users to a given service provider(defined by SP_NAME) in the authentication flow based on the Roles of the user (defined by ROLE_1 and ROLE_2) and the time of the day (eg: betwe
  <Target>
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/E-HealthcareApp/addPatient.jsp</AttributeValue>
          <AttributeDesignator AttributeId="http://wso2.org/identity/sp/sp-name" Category="http://wso2.org/identity/sp" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
        </Match>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">authenticate</AttributeValue>
          <AttributeDesignator AttributeId="http://wso2.org/identity/identity-action/action-name" Category="http://wso2.org/identity/identity-action" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDe
        </Match>
      </AllOf>
    </AnyOf>
  </Target>
  <Rule Effect="Permit" RuleId="permit_by_roles_and_time">
    <Condition>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
        <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:time-in-range">
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only">
            <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment" DataType="http://www.w3.org/2001/XMLSchema#time" MustBePreser
          </Apply>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">08:00:00</AttributeValue>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">10:00:00</AttributeValue>
        </Apply>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-is-in">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
            <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
            </Apply>

        </Apply>
      </Apply>
    </Condition>
  </Rule>
  <Rule Effect="Deny" RuleId="deny_others"/>
</Policy>
```

As a Nurse is only concerned with the patients' data as long as she leaves the healthcare organization. Therefore, this policy has been defined to control any nefarious activity on

nurse's behalf so that she won't be able to read the patients' data from any other location and leak it to unconcerned parties.

4.5 Conclusion

This chapter is giving an idea of how to implement CBACS by integrating RBAC and CAAC. A simple e-Healthcare Cloud web app backed by WSO2 middleware has been developed to demonstrate the results of implementation of authentication and authorization functions. Moreover, in the discussion section two scenarios are presented to restrict the access of authenticated users based on role, time and location based authorization.

Chapter 5

CONCLUSION AND FUTURE DIRECTIONS

5.1 Conclusion

The world is shifting to IoTs to make life more convenient and advanced for human beings. These devices are playing an important part to make this world a global village where everything is connected. Every year there is a rise in the usage of IoTs. According to Gartner [45] 8.4 billion connected devices will be there in 2017. Today IoTs are used in almost every field of life. Nowadays these devices are combined with Cloud Computing technology in order to provide daily life services in a more efficient manner.

The methodology followed during this research is shown in Fig 5.1 and is explained below.

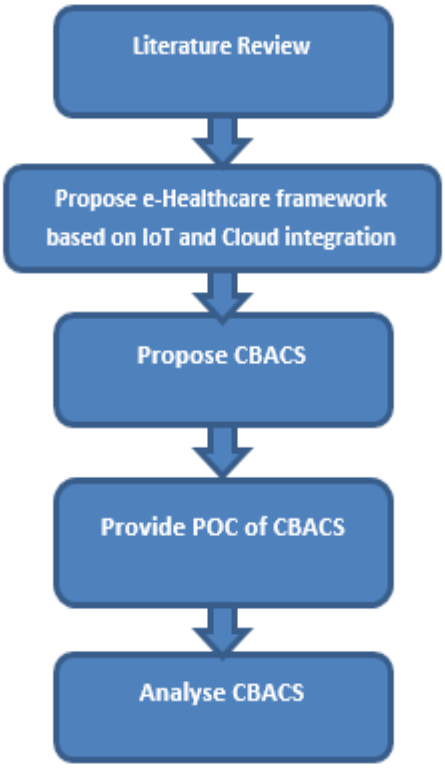

Figure 5.1 Methodology of Research

In this research work an operational efficient IoT based Cloud framework for e-Healthcare has been presented. But from security perspective it is vulnerable to a number of attacks. From the systematic literature survey and review, it has been concluded that the proposed framework for e-Healthcare organizations is most vulnerable to the threat of malicious insiders associated to the attacks on confidentiality and integrity of patients' medical records and other e-Health data gathered by IoT devices. Malicious Insiders can cause a great damage to business and can serve as a great hurdle in its growth as well as in maintaining a better image in market. Moreover, this threat can form the basis of other attacks that lead to the leakage of patients' information and thus to the violation of HIPAA privacy law followed by legal consequences. The malicious insiders can also tamper with the patients' health data that can put a life in danger through the mistreatment of the patients according to the altered data.

Therefore, to make this framework secure from perspective of the most challenging threat, the attack of Malicious Insiders has been handled inside e-Health private Cloud by putting forward CBACS. This system caters the threat of technical malicious insiders who have authorized access to the e-Healthcare resources by forming context based policies for the defined roles of the insiders. This is a policy based flexible access control system that could overcome the limitations of existing schemes to handle this threat in IoT based Cloud e-Healthcare environment by strictly restricting the access of the insiders using temporal and location based conditions. The defined policies are modified according to the requirements of e-Healthcare organization by the Policy Administrator after involving higher authorities in this process. The higher authorities are involved so to avoid any malicious activity by the Policy Administrator. Along with limiting the access of malicious insiders, the proposed framework is also capable for holding the insider accountable for his suspicious activities to avoid future malicious insiders attack threatening two components of information security CIA triad: Confidentiality and Integrity by modifying policies and taking action against that insider.

5.2 Future Directions

During this research the framework shown in Fig 5.2. has been proposed and made secure against the Malicious Insiders attack inside cloud as represented by circle in the figure, by

proposing CBACS. This research has provided open research areas for future researchers as there is still room for further research in this field.

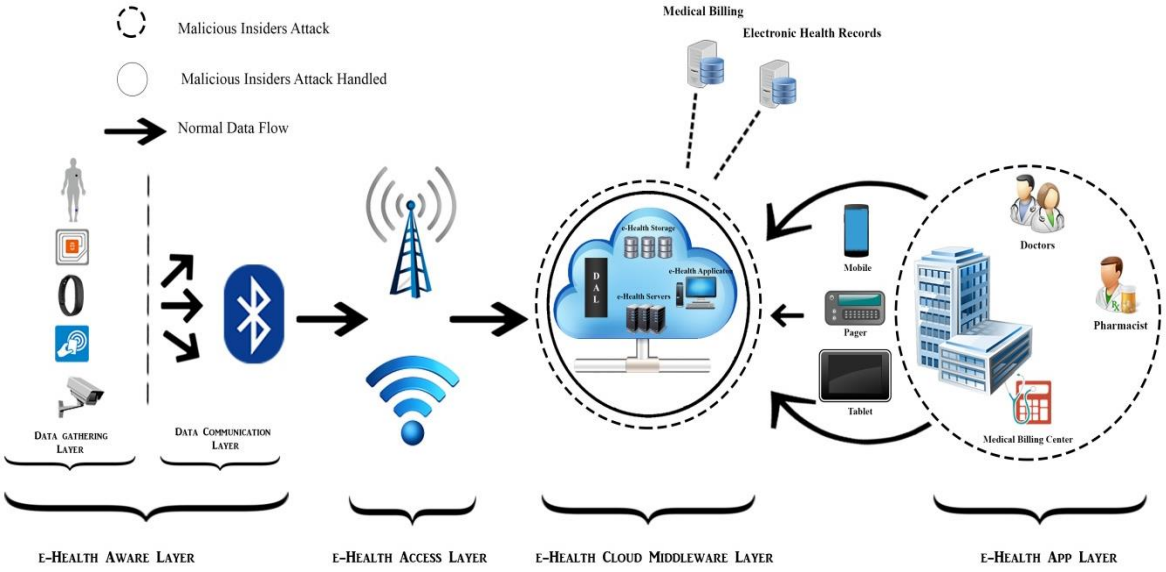

Figure 5.2 Proposed IoT based Cloud e-Healthcare Framework

Following future directions are provided to the researchers as a result of this research work.

1. Deploy the proposed IoT based on Cloud e-Healthcare Framework.
2. Make this framework more secure against other possible attacks.
3. Handle the threat of Malicious Insiders at other layers of the framework including patients' end where the people in contact with patient can intentionally or unknowingly modify the settings of the information gathering devices (IoTs) that could badly affect the response of the healthcare organizations pertaining to patient care. So a technique should be developed that could detect such a change, inform the healthcare organization about this and could also revert the modification in settings.
4. WSO2 middleware platform has been used to give proof of concept about proposed CBACS. In future more better platform providing cloud based middleware services can be used.

5.3 Summary

This chapter has concluded the research work by providing a brief overview of the research conducted. It has given a sketch of the suggested frameworks in this research. Furthermore it has set future directions for the researchers in the fields of Information Technology and Information Security.

BIBLIOGRAPHY

[1] J. Zhou, T. Leppanen, C. Yu and H. Jin, "CloudThings: a Common Architecture for Integrating the Internet Of Things with Cloud Computing", in IEEE 17th International Conference on Computer Supported Cooperative Work in Design, 2013, pp. 651-657.

[2] R. Latif, H. Abbas and S. Assar, "Distributed Denial of Service (DDoS) Attack in Cloud- Assisted Wireless Body Area Networks: A Systematic Literature Review", Journal of Medical Systems, vol. 38, no. 11, 2014.

[3] W. Na, "Internet of Things based on Cloud Computing Architecture", in 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, 2015, pp. 585-587.

[4] J. Rui and S. Danpeng. "Architecture Design of Internet of Things based on Cloud Computing." 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, pp. 206-209. IEEE, 2015.

[5] S. Riazul Islam, Daehan Kwak, M. Humaun Kabir, M. Hossain and Kyung-Sup Kwak, "The Internet of Things for Health Care: A Comprehensive Survey", IEEE Access, vol. 3, pp. 678-708, 2015.

[6] Y. Min, H. Shin and Y. Bang, "Cloud Computing Security Issues and Access Control Solutions", Journal of Security Engineering, vol. 9, no. 4, pp. 135-142, 2012.

[7] S. Singh, B. Pandey, R. Srivastava, N. Rawat and P. Rawat, "Cloud Computing Attacks: A Discussion with Solutions", Open Journal of Mobile Computing and Cloud Computing, vol. 1, no. 1, pp. 1-10, 2014.

[8] B. Sevak, "Security Against Side Channel Attack in Cloud Computing", International Journal of Engineering and Advanced Technology (IJEAT), vol. 2, no. 2, pp. 183-186, 2012.

[9] K. Munir and S. Palaniappan, "Secure Cloud Architecture", Advanced Computing: An International Journal, vol. 4, no. 1, pp. 9-22, 2013.

[10] Kitchenham, B., Brereton, O. P.,Systematic literature reviews in software engineering – A systematic literature review. Journal of Information and Software Technology, pp:7–15 2009.

[11] H. Eken, "Security Threats and Solutions in Cloud Computing", in World Congress on Internet Security (WorldCIS-2013), 2013, pp. 139-143.

[12] Y. Zhang, A. Juels, M. Rieter and T. Ristenpart, "Cross-Tenant Side-Channel Attacks in PaaS Clouds", in CCS'14, Scottsdale, 2014, pp. 990-1003.

[13] T. H.Noor, Q. Z.Sheng and A. Alfazi, "Detecting Occasional Reputation Attacks on Cloud Services", Springer, pp. 416-423, 2013.

[14] "IBM X-Force® Research 2016 Cyber Security Intelligence Index", Www-01.ibm.com, 2016. [Online]. Available: https://www-01.ibm.com/marketing/iwm/dre/signup?source=ibm-WW_Security_Services&S_PKG=ov47123&S_TACT=000000NJ&&S_OFF_CD=10000254. [Accessed: 18- Nov- 2016].

[15] A. Mahajan and S. Sharma. "The Malicious Insiders Threat in the Cloud". International Journal of Engineering Research and General Science, vol. 3, Issue 2, Part 2, pp. 245-256, March-April 2015.

[16] M. U. Kavyashree and H. Manjunath. "A Framework to avoid Vulnerability Incidents in Cloud Computing". International Journal on Advanced Computer Theory and Engineering (IJACTE), vol. 3, pp. 12-16, 2014.
[17] Software Engineering Institute, "Deriving Candidate Technical Controls and Indicators of Insider Attack from Socio-Technical Models and Data", CERT, 2011.
[18] Software Engineering Institute, "Insider Threats to Cloud Computing: Directions for New Research Challenges", CERT.
[19] G. Garkoti, S. K. Pedojuu and R. Balasubramanian. "Detection of Insider Attacks in Cloud based e-Healthcare Environment". 2014 International Conference on Information Technology, pp. 192-200. IEEE, 2014.
[20] T.Gunasekhar, K.Thriupathi Rao, V. Krishna Reddy, P.Sai Kiran and B. Thirumala Rao. "Mitigation of Insider Attacks through Multi-Cloud". International Journal of Electrical and Computer Engineering (IJECE), vol. 5, pp. 136-141, February 2015.
[21] A. Duncan, S. Creese and M. Goldsmith, "Insider Attacks in Cloud Computing", in IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 857-862.
[22] A. Duncan, S. Creese, M. Goldsmith and J. S. Quinton, "Cloud Computing: Insider Attacks on Virtual Machines During Migration", in 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 493-500.
[23] M. Inam ul Haq, "The Major Security Challenges to Cloud Computing", Master's, University of Boras, 2013.
[24] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities", Security and Privacy IEEE magazine, 2011.
[25] A. Singh and M. Shrivastav, "Overview of Attacks in Cloud Computing", International Journal of Engineering and Innovative Technology (IJEIT), vol. 1, no. 4, pp. 321-323, 2012.
[26] P. Chouhan and R. Singh, "Security Attacks on Cloud Computing with Possible Solutions", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, no. 1, pp. 92-96, 2016.
[27] M. Nguyen, N. Chau, S. Jung and S. Jung, "A Demonstration of Malicious Insider Attacks inside Cloud IaaS Vendor", International Journal of Information and Education Technology, vol. 4, no. 6, pp. 483-486, 2014.
[28] Information Security & Critical Infrastructure Protection Research Laboratory, "The Insider Threat in Cloud Computing".
[29] Eberle W., Holder L., "Insider threat detection using graph-based approaches", in Proc. of the Cybersecurity Applications and Technology Conference for Homeland Security, pp. 237–241, IEEE Computer Society, 2009.
[30] Z. Yusop and J. Abawajy, "Analysis of Insiders Attack Mitigation Strategies", Procedia - Social and Behavioral Sciences, vol. 129, pp. 611-618, 2014.
[31] R. Latif, H. Abbas, S. Latif and A. Masood, "Distributed Denial of Service Attack Source Detection Using Efficient Traceback Technique (ETT) in Cloud-Assisted Healthcare Environment", J Med Syst, vol. 40, no. 7, 2016.
[32] R. Latif, H. Abbas, S. Latif and A. Masood, "EVFDT: An Enhanced Very Fast Decision Tree Algorithm for Detecting Distributed Denial of Service Attack in Cloud-Assisted Wireless Body Area Network", Mobile Information Systems, vol. 2015, pp. 1-13, 2015.

[33] H. Abbas, S. Latif and R. Latif, "Distributed denial of service (DDoS) attack detection using data mining approach in cloud-assisted wireless body area networks", IJAHUC, vol. 23, no. 12, p. 24, 2016.
[34] R. Latif, H. Abbas, S. Latif and A. Masood, "A Real-Time Cloud-Assisted Wireless Body Area Network Deployment for Detecting Distributed Denial of Service Attack using A novel Enhanced Very Fast Decision Tree Algorithm", Healthcare on Smart and Mobile Devices, Annals of Telecommunication, 2015.
[35] Y. Hu, K. Duan, Yin Zhang, et al., "Simultaneously aided diagnosis model for outpatient departments via healthcare big data analytics", Multimedia Tools and Applications, DOI: 10.1007/s11042-016-3719-1, 2016.
[36] Yin Zhang, et al., "Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data", IEEE Systems Journal, DOI: 10.1109/JSYST.2015.2460747, 2015.
[37] Yin Zhang, et al., "iDoctor: Personalized and Professionalized Medical Recommendations Based on Hybrid Matrix Factorization", Future Generation Computer Systems, DOI: 10.1016/j.future.2015.12.001, 2016.
[38] Zhou, Zhenji, Lifa Wu, and Zheng Hong. "Context-Aware Access Control Model For Cloud Computing". International Journal of Grid and Distributed Computing 6.6 (2013): 1-12. Web.
[39] P, Priya, Joseph Charles, and Britto Ramesh Kumar. "Context-Aware Architecture For User Access Control". International Journal of Advanced Research in Computer Science & Technology 2.3 (2014): 201-204. Print.
[40] Ajana el khaddar, Mehdia, and Abdelilah Maach. "Policy Based Security Middleware As A Service". Future Internet Of Things And Cloud (Ficloud), 2014 International Conference On. Barcelona, Spain: IEEE, 2014. Print.
[41] Hu, Junzhe, and Alfred C.Weaver. A Dynamics, Context-Aware Security Infrastructure For Distributed Healthcare Applications. 2017. Print.
[42] Research Framework Program Seven (FP7) project SECCRIT. Enhancing Cloud Security With Context-Aware Usage Control Policies. 2015. Print.
[43] Tang Z., Wei J., Sallam A., Li K., Li R. (2012) A New RBAC Based Access Control Model for Cloud Computing. In: Li R., Cao J., Bourgeois J. (eds) Advances in Grid and Pervasive Computing. GPC 2012. Lecture Notes in Computer Science, vol 7296. Springer, Berlin, Heidelberg

[44] "Xacml". www.oasis-open.org. Web. 8 June 2017.

[45] "WSO2 Introduction". WSO2. Web. 8 June 2017.