AUTHENTICATION MECHANISM OF ELECTRONIC HEALTH RECORD (EHR) IN THE CLOUD

MINE HURMUZLU

SEPTEMBER 2015

AUTHENTICATION MECHANISM OF ELECTRONIC HEALTH RECORD (EHR) IN THE CLOUD

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES OF
ÇANKAYA UNIVERSITY

BY
MINE HURMUZLU

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF
COMPUTER ENGINEERING

SEPTEMBER 2015

Title of the Thesis: **Authentication Mechanism of Electronic Health Record (EHR) in the Cloud.**

Submitted by **Mine HURMUZLU**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.

Prof. Dr. Halil T. EYYUBOĞLU
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Müslim BOZYİĞİT
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assit. Prof. Dr. Nurdan SARAN
Supervisor

Examination Date: 16.09.2015

Examining Committee Members

Assist. Prof. Dr. Nurdan SARAN	(Çankaya Univ.)	
Assist. Prof. Dr. Reza ZARE HASSANPOUR	(Çankaya Univ.)	
Assist. Prof. Dr. Fatih Sulak	(Atılım Univ.)	

STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name	:	Mine HURMUZLU
Signature	:	
Date	:	30.09.2015

ABSTRACT

AUTHENTICATION MECHANISM OF ELECTRONIC HEALTH RECORD (EHR) IN THE CLOUD

HURMUZLU, Mine

M.Sc., Department of Computer Engineering

Supervisor: Assist. Prof. Dr. Nurdan SARAN

September 2015, 40 pages

Electronic health record (EHR) is a system that contains patients' complete medical related records from birth to death. These records consist of diagnoses, medications, laboratory tests, and results. The records are created by the patients and accessed by health providers such as doctors, nurses, pharmacies, etc.

The advantages of using cloud computing has helped the health organizations to dispense the local servers and shift all their data to the cloud, which helped them save space, energy, and cost, as well as provide the benefit of accessing the data by patients and healthcare providers from anywhere at any time. Exchanging medical records in the cloud, however, has threatened the security and privacy of e-health systems where the authentication, access control, and integrity of the medical records are the main challenges in e-health clouds.

In this thesis, we study the authentication mechanism of an EHR system and investigate an improved version using attribute based encryption ABE. Patients have full control over their medical records which are stored in a semi trusted servers. The system also works on access policies in case of emergency.

Keywords: EHR, PHR, ABE

ÖZ

BULUT ÜZERİNDE ELEKTRONİK SAĞLIK KAYITLARIN KİMLİK DENETİMİ

HURMUZLU, Mine
Yüksek Lisans, Bilgisayar Mühendisliği Anabilim Dalı
Tez Yöneticisi: Assist. Prof. Dr. Nurdan SARAN
Eylül 2015, 40 sayfa

Elektronik sağlık kayıtları doğumdan ölüme kadar, hastaların tüm tıbbi kayıtlarını içeren bir sistemdir. Bu tıbbi kayıtlar teşhisler, reçeteler, ilaçlar, laboratuar testleri ve sonuçlarından oluşmaktadır. Kayıtlar hastalar tarafından oluşturulur ve doktorlar, hemşireler, eczaneler vb sağlık hizmeti sağlayanlar tarafından erişilir.

Bulut bilişim teknolojisi sağlık organizasyonlarının yerel sunuculardan vazgeçmelerini, verilerini buluta alarak, enerji ve maliyet tasarrufu yapmalarını sağladı. Tüm bunların yanı sıra hastalar ve sağlık hizmeti verenler için verilere her zaman ve her yerden erişme imkânı sağladı. Ancak, tıbbi kayıtların bu şekilde kullanımı e-sağlık sisteminin güvenliğini ve gizliliğini tehdit etmektedir. Bulut bilişim teknolojisinin e-sağlık sisteminde kullanılması için sağlaması gereken temel zorunluluklar kayıtların doğrulanması, erişim kontrolü ve bütünlüğüdür.

Bu çalışmada, bir ESK (Elektronik Sağlık Kayıtları) sisteminin kimlik doğrulama mekanizmasını inceleyip ABE şifreleme mekanizmasını temel alan geliştirilmiş bir ESK sistemini inceliyoruz. Hastalar kısmen güvenilen sunucularda saklanan tıbbi kayıtları üzerinde tam kontrole sahip olacaktır. Önerilen sistemde, aynı zamanda acil durumlarda erişim ilkeleri üzerinde de çalışılmıştır.

Anahtar Kelimeler: Elektronik Sağlık Kayıtları, Kişisel Sağlık Kayıtları, ABE

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor Assistant Professor Dr. Nurdan SARAN for her continuous guidance, comments and remarks through the learning process of this thesis.

I would also like to thank my family to whom this thesis is dedicated to. None of this would have been possible without their unconditional love and support.

Finally, and most importantly, I would like to thank my beloved husband for his support and continuous encouragement throughout my thesis work.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES

LIST OF TABLES

TABLES

LIST OF ABBREVIATIONS

EHR	Electronic Health Record
PHR	Personal Health Records
EMR	Electronic Medical Records
ABE	Attribute-Based Encryption
KP-ABE	Key-Policy-Attribute-Based Encryption
CP-ABE	Ciphertext-Policy Attribute-Based Encryption
HIPAA	Health Insurance Portability and Accountability Act
CDC/NCHS	Centers of Disease Control and Prevention/National Centers for Health Statistics
HHS/ONC	U.S. Department of Human Health Services' Office of the National Coordinator
TVD	Trusted Virtual Domains
PRD	Professional Domain
PSD	Personal Domain
TA	Trusted Authority
AA	Attribute Authority

CHAPTER 1

INTRODUCTION

1.1 Fundamentals of the Electronic Health Record System

Every time you visit a doctor, hospital, or clinic, a record of your personal health information is stored. Lab tests, allergies, past diagnoses, and treatments are all information can help the professionals give you accurate diagnoses as well as fast treatment. The records are protected under the HIPAA regulations [1]. HIPAA restricts the health care providers from accessing it if not necessary, and makes sure that the health records are kept confidential and secure [2]. The HIPAA Privacy Rule obligates the entities that use the medical information for any purpose to report the patient about the use of their records. Moreover, the HIPAA also requires the entities to access the medical records they need as less frequently as possible. [3].

The Electronic health information system (EHI) consists of three parts:

Electronic health record (EHR) is a collection of the patient's medical information recorded by the health care providers (doctors, nurses, specialists). EHRs comprehend the data from hospital records, private clinics, and other health organizations.

Personal health record (PHR) is an accumulation of important health information gathered from several resources, patients, or healthcare providers. It is managed and controlled by patients themselves.

Electronic medical record (EMR) is the digital version of the papers stored in doctor's clinic. It contains the medical history of patients and it is stored in a private database that belongs to a single health organization (a hospital). Every patient has several EMRs stored in multiple places. Once the EMR data is shared among organizations or individuals, they become EHR. Every patient has a single EHR, in other words, an EMR can be considered as a data source for the EHR and PHR [4] [5].

Here it is necessary to mention that the EMR was only stored in offline databases and offline private servers before the cloud got introduced to modern technology. After the breakthrough of the cloud computing techniques, digital medical records were moved to the cloud. Data now can be stored in multiple locations, such as an internet

reachable databases, EHR service providers, home computers, and portable devices [6] [7].

The PHR records can be accessed by several parties like the patient himself, a professional healthcare provider, or an insurance company. It contains information from both EMR and EHR. The collected information can spare patients money and the inconvenience of going for routine medical checkups. The patient should always have complete access to their own PHR, and should have control over who can view his records and the information in PHR, which should be kept accurate and up to date as well [4].

EHR system offers many services such as the ability to create a record, add new data to an existing record, view records and exchange them between doctors for consultation purposes, plan the next appointment, write prescriptions, as well as enabling the patients to share their records with selected family members or friends. The system should offer an encryption mechanism in order to secure the records properly [8] in addition to offering a method for access in case an emergency situation, especially in case of accidents, when the emergency staff should have authority to temporarily access because the patient is unconscious and unable to change the access policy [9].

1.2 E-Health Cloud advantages:

- **Cost effectiveness:** One of the advantages of cloud based electronic health records is its low cost. Any organization can have an efficient IT solution from cloud service providers within a reasonable price without the need to buy software and hire an IT staff to manage and maintain the program. Eventually the burden of managing the system will be on the third party cloud service providers for both small practices and bigger organizations [10].
- **Portability:** Another advantage is that the cloud can make it easy to share medical records and access any record at anytime, anywhere, and between any types of health organization, and if agreed upon regulations, records can be shared across the borders in the future [6].
- **System reliability:** All medical data is stored in redundant servers. Health organizations, including the patients, do not need to worry about losing any data in case of system failure [10].

- **System integration:** The cloud provides integration of EHRs within the health centers that helps medical staff provide health services easily [3].

Aside from these benefits, e-health cloud faces many problems, which are discussed later in this chapter.

1.3 Real World Experience with EHR

Many countries around the world have started evolving in the new health cloud technology; examples of such countries are listed below:

I. USA

EMR systems have been used in the USA health provider organizations for some time, but shifting to the cloud required lots of efforts. According to a survey done by the CDC/NCHS, the usage of any form of EHR system increased from 29%, in 2006, to 73%, in 2011, and the use of the system in emergency departments increased from 46%, in 2006, to 84%, in 2011. The use of any form of EHR means that a medical system is all or partially electronic. Only 10% are using a fully functional system according to 2010 statistics by the same organization [11].

Adopting a full system is considered less; it has been observed that most of the physicians are not satisfied with the EHR software, or are just not familiar with the software because of lack of training as it is considered costly. The cost of adopting any EHR system is reduced only for large health organizations and not in smaller practices due to the lack of efficiency and usability of the current software [12]. Nevertheless, the HHS/ONC for Health Information Technology recently adopted Acumen Solutions, which is specialized in cloud computing services for government organizations. Acumen Solutions intend to develop a software that supports a cloud based EHR system that will be used nationwide in the near future [13] [10].

II. UK

In 2005 United Kingdom initiated the National Health Service (NHS). The goal was to have a fully functional system by 2010. Unfortunately the government had to shut down the project because the system was complex and not usable for the

stakeholders who were going to use it [14]. The cost of this program was over $24 billion, which is considered to be the biggest and the most expensive IT failure in health sectors [15].

III. Australia

Australia is one of the leading countries in EHR technology. The government has focused on developing a fully functional EHR cloud system. Despite the weak participation from the caregivers to install an EHR system, the government intends to deliver the cloud service in all its territories and states [10].

IV. Canada

The province of Alberta has launched an electronic health record named Alberta Netcare EHR. The authorized doctors will have the right to access patient's medical records through it, and this service will soon be given to 4 million residents [16].
The province of Ontario is planning to give the EHR service to all the Ontarians this year [17] [18].

V. Estonia

Estonia is well known for their advanced e-health services. Data collecting process has been going on since 2008. Estonia has become the first country to deliver a full nation-wide EHR system to their residents from birth to death [18].

VI. Jordan

Jordan has started studying the idea of a national EHR system since 2009. The plan was to adopt a low cost, efficient, and national system that includes medical information from birth to death. The government has adopted the US Veterans Health Administration electronic health record system (VistA EHR), and installed the system in three of its largest hospitals in the country. When the installation has covered all the hospitals, Jordan will be the first country to have a single electronic record delivering care to all the patients in its country [19].

VII. Turkey

Turkey's health activities have shown improvements in the same sector, especially after the government started to collect patients' data by using an e-health application called Family Medicine Information System (FMIS), which was implemented with the family physician application. The data collected from physicians is transferred electronically to the Ministry of Health [20]. Recently Turkey started a patient-centric system called E-Nabız. This new system offers health services to all the citizens on two platforms: by a website server and a mobile application. All the medical records are stored in this server where the patient can access them anytime and anywhere to view his past medical treatments, laboratory test results, prescriptions, and can book for an appointment with the doctor. This will be helpful for a fast treatment next time the patient visits the doctor, and will reduce unnecessary tests and treatments. The patient has the option of allowing or preventing the doctors and FMIS to view his records, and he can stop a doctor from viewing his records any time he wants. The patient also has the right to share his personal records with another doctor for a second opinion, and can get a copy of all his records as well. The server allows the patient to freeze or completely delete his/her personal account anytime he/she wants [21].

1.4 EHR Cloud Challenges

EHR cloud may have many benefits for the medical sector; however, the system has undergone many challenges out of which the security and privacy challenges are considered to be the biggest.

The most common security and privacy concerns include:

1. **Integrity:** The service provider must ensure that the input data which was entered by a patient or a physician is consistent, accurate, and is the same information which is or was viewed by authorized users [6].
2. **Confidentiality:** It is one of the major challenges in e-health cloud as the patient's data must be kept completely undercover and safe from attempts for unauthorized access [22].

3. **Authenticity:** The identities of the users that try to access a specific record must be known to the healthcare system; they must be authenticated and recognized by the records' owners [22].
4. **Audit:** The cloud service provider must guarantee the security and safety of the medical data, and ensure that all the accessing events are recorded and monitored [6].
5. **Accountability:** The patient or the people, authorized by the patient, must have the right to monitor the access activities to their sensitive health records by the clinics, hospitals, etc. [22].
6. **Anonymity:** the identities of the patients must be anonymous in the cloud. The cloud service provider should not be aware of any personal information about the patient through his stored medical records [22]. Health care providers, such as pharmacies, should not be able to trace the identity of any patient.
7. **Non-repudiation:** the patient or the healthcare provider cannot, and should not, deny making any communication activity such as sending or receiving data [6].

Despite of all the attempts to improve the approaches that are proposed so far to enhance the security of the medical records, the privacy and security is still one of the main reasons of why many healthcare providers still think twice before purchasing any cloud based EHR system.

Besides the security and privacy concerns, there are many other challenges that must be considered when designing a cloud based EHR system and are as follows:

- **Semi-confidentiality:** Doctors may share sensitive information with an unauthorized entity; some pharmaceutical companies illegally try to buy patient information for marketing purposes. On the other hand the user tries to view as much information as possible about the patient. In some cases, however, sharing patient records can help health researchers to investigate drug side effects, treatments from specific diseases, and hospitals performance in handling patients.

- **Medical identity theft:** This is one of the fast growing problems since the digitizing process of the medical records. Patients do not realize their identity has been stolen until it is too late, and the consequences of such an action can cause serious problems such as unnecessary and sometimes deadly treatments. A solid authentication mechanism and reliable encryption method must be developed to stop further identity theft [23].
- **Revocation:** A mechanism for granting authority and taking it back must be presented. A patient should be able to decide when he no longer wants to have a specific healthcare provider access his medical records.
- **Emergency Cases:** If the patient is unconscious and cannot give the authority needed for quick treatment, a proper mechanism must be available to handle emergency cases.

In the next chapter we will discuss the privacy-preserving methods to increase the efficiency of the e-health cloud system.

1.5 Objectives

The main aim of this study is to make an in depth survey on the most recent works about one of the hottest topics in information technology that is the process of migrating from the paper-based medical data to the cloud, as well as discussing the pros and cons of this procedure in detail. Recent works are evaluated and compared with each other based on the most important requirements that we believe are challenging and must be considered when designing a secure system.

As a result of these evaluations, we have proposed an improved version of a system fully controlled by the patient who is considered to be the core of this system. The improved version is an outcome of the previous works. There is no structure that we can call an ideal system yet as the researches in this field are still limited, and designing a secure system is still a challenging process in addition to the matter of trusting the cloud still bearing a big question mark.

Based on our evaluations, we will try to describe how a patient-centric system based on attribute-based encryption method should be designed.

1.6 Organization of the Thesis

This thesis contains five chapters;

Chapter 1 is an introduction to the fundamentals of collecting the medical data,, the advantages of migrating data to the cloud, and discussing the challenges by giving examples of different countries that have experience in the same field. This chapter also includes the objectives of this thesis.

Chapter 2 includes description of the fundamental approaches that are used in this thesis in addition to a literature review on the same subject.

Chapter 3 includes a thorough comparison between the previously proposed researches in terms of the security and design challenges.

Chapter 4 includes our improved system in detail, and the evaluation of the security and design challenges of this system.

Chapter 5 includes the conclusion and ideas for future works.

CHAPTER 2

PRIVACY PRESERVING APPROACHES

2.1 Fundamentals of the Cloud-Based Electronic Health Record System

The e-health cloud model consists of three types:

Private: An e-health cloud structure that is implemented privately by a healthcare provider where the patients' records are stored in a hospital's private cloud.

Public: An e-health cloud structure maintained by a third party cloud service provider.

Hybrid: An e-health cloud structure that is maintained by both a third party cloud service provider and a private healthcare provider where the patients' records are stored in both platforms.

There have been many approaches proposed to protect the privacy of the patients. These approaches focus on two methods of protection. The first one is to protect the medical records in the cloud platform where all the data is stored and shared. The second one is to protect the medical data in the end-user platform (where patients are the data owners and medical service providers as the data users).

Yang et al. [5] are handling the first method by proposing a hybrid practical solution for preserving the privacy of medical data sharing in the cloud. The statistical analysis and cryptography are joined to provide a flexible data accessing. However, multiple clients simultaneously accessing the cloud is not investigated in this work.

Rodrigues et al. [3] researched about handling the security of the records in cloud where the threats of hosting EHRs on the cloud service providers are studied. To protect the confidentiality of the patient records, the researchers suggest that the cloud clients must be well informed of all the services offered by the cloud provider before moving the data to the cloud. Other suggestions are; the client should be aware of the data security issues because the cloud provider can have access to all the records; the clients must know the location of the servers where the records are stored; and the clients should request a complete transparency. As all the security concerns pointed out by the researchers are only suggestions that must be considered by both cloud service providers and the healthcare clients, it is difficult to fully trust only the cloud service providers. Nevertheless, client platform must have their share

of intensified security, solid authenticity, and access to the right mechanism to ensure a higher level of trust.

In this work, we only focus on the second method of protecting the security of the patients and users.

Securing end-user privacy has two types of technique approaches; cryptographic and non-cryptographic approaches. We only focus on the cryptographic approaches.

- **Identity Based Encryption**

  Identity based encryption method was first proposed by Adi Shamir [24]. The idea is that the public key is already distributed. The key is something that can be a string; for example, the e-mail address of the receiver. Only a person who has this string can access the encrypted document. Figure 1 illustrates IBE mechanism in which Alice wants to send a secret message (M) to Bob. She encrypts the message using Bob's email address as a public key "name=bob@email.com". Bob receives the message and requests the proper authentication from the trusted central key server (PKG). The server authenticates Bob by sending a unique secret key (SK) in order to decrypt not only the current message, but also the future messages from Alice.

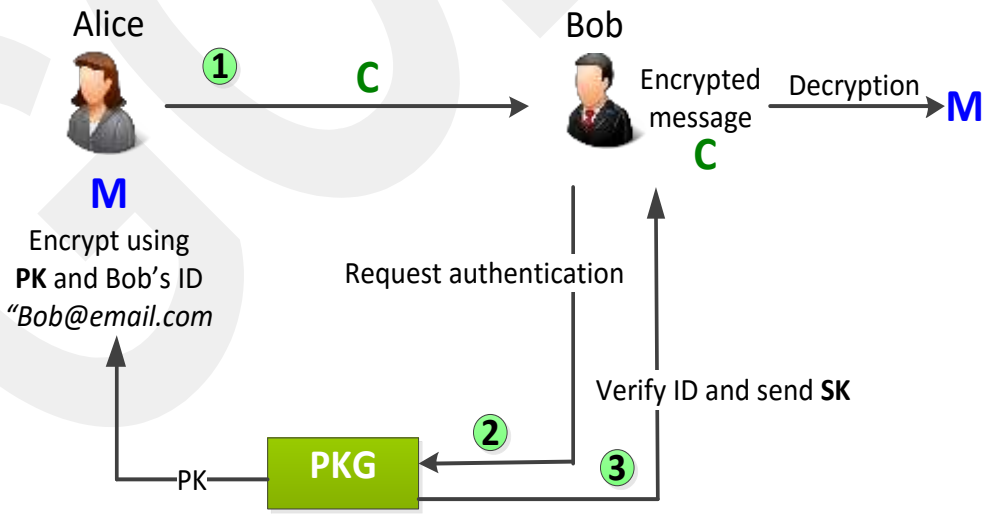

Figure 1: ID-Based Encryption

The benefit of IBE mechanism lies in its simplicity. By using identifications such as email addresses and names, data protection, authentication certificates

are no longer needed and the decryptor does not need to download any software for decrypting messages [25].

A significant disadvantage of ID-based encryption is that the privacy of the PKG must be well preserved as it holds all the private keys.

- **Attribute Based Encryption**

Attribute based encryption (ABE) is an encryption method based on public key encryption PKE. It was introduced by Sahai et al. [26]. ABE has gone one step ahead of IBE by using a set of attributes to encrypt a document; the key generator server issues different private keys to users. The secret keys are attached with a set of attributes that each user possesses, and a user can decrypt the ciphertext only if there is a match between the attributes of the ciphertext and the user's key. For example, Bob uses the attribute ("Doctor" OR "Physical therapist" AND ("Hospital A" OR "Hospital B")) to encrypt a message. Alice who has the attribute ("Doctor" OR "Resident" AND ("Hospital B")) can decrypt Bob's message because she satisfies his attributes, But Dorothy who has the attribute ("Doctor" AND "Physical therapist" AND ("Hospital C")) cannot decrypt the message because she does not satisfy Bob's attributes.

ABE has the following branches:

- *Ciphertext Policy Attribute-Based Encryption*

CP-ABE was first presented by Bethencourt et al. [27]. The message is encrypted under an access structure, and the users' secret keys are attached with a set of attributes as illustrated in Figure 2.

Figure 2: CP-ABE Mechanism

A user is only able to decrypt a ciphertext if his attributes satisfy the policy of the relevant ciphertext. For example, in Figure 3, a medical record is encrypted using a public key under the policy ("Doctor" OR "Physical therapist" AND ("Hospital A")), a ciphertext is created for each "doctor" or "physical therapist" in "hospital A" so they can decrypt a file using their unique secret key. A user with attribute ("Doctor" AND "Hospital B") is not allowed to decrypt the file.

When a new doctor or a physical therapist is added to hospital A, a new ciphertext is encrypted for them so they can decrypt the same file with their secret keys.

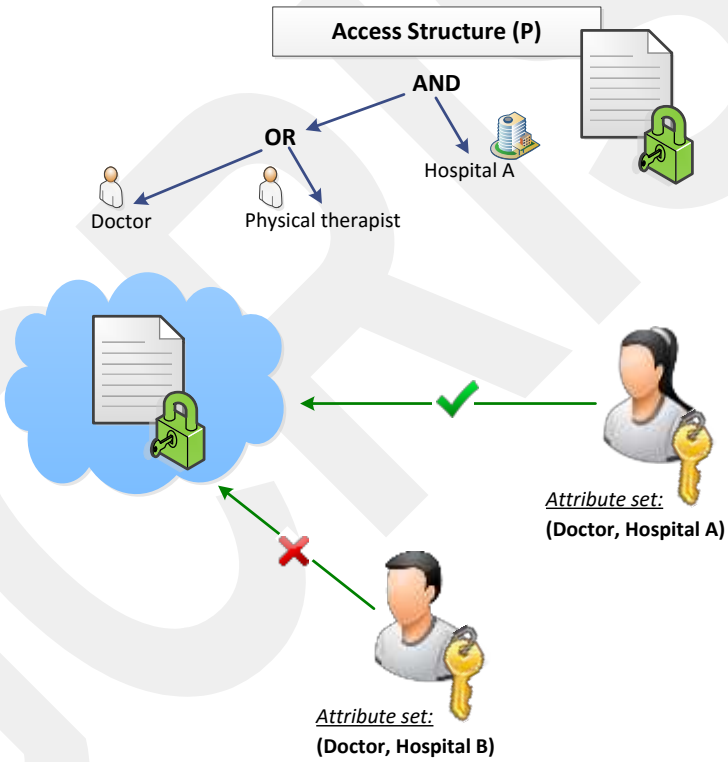

Figure 3: CP-ABE

- *Key Policy Attribute-Based Encryption*

KP-ABE encryption mechanism, which is the opposite of CP-ABE as illustrated in Figure 4, was introduced by Goyal et al. [28]

Figure 4: KP-ABE Mechanism

The owner encrypts the ciphertext under a set of attributes, and the users are able to decrypt only if their secret keys match the access structure. The access structure indicates which ciphertext the user's key can decrypt. For example, in Figure 5, a message is encrypted under the attribute (Hospital B), and Alice has a private key that is associated with the access structure ("Doctor" OR "Nurse" AND ("Hospital B")), and Bob has a private key that is associated with access structure ("Doctor" OR "Physical therapist" AND ("Hospital B")). Alice is able to decrypt this ciphertext because the attributes associated with it satisfies her key's access structure.

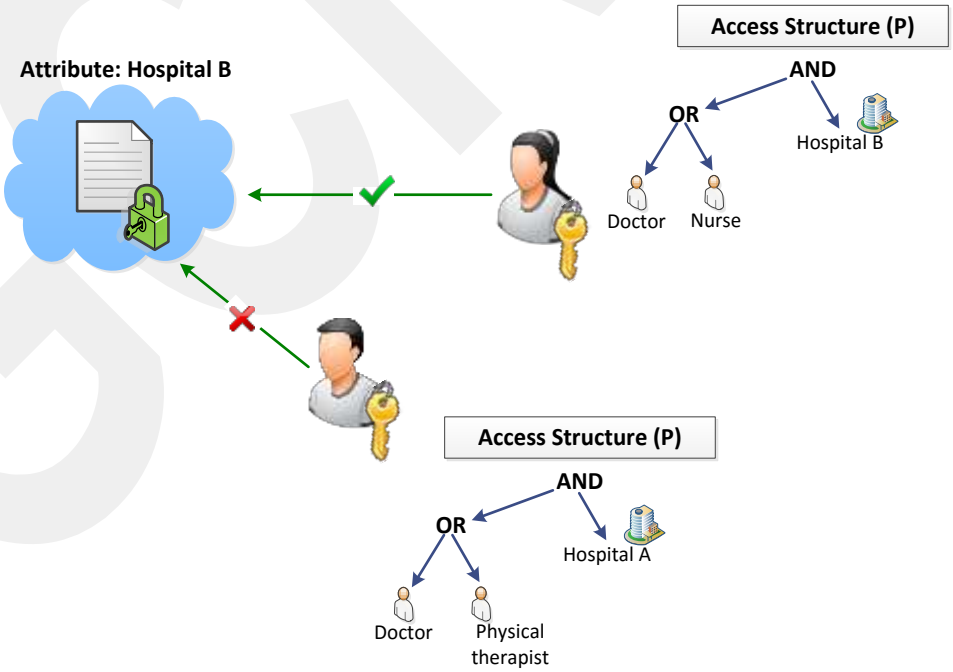

Figure 5: KP-ABE

- *Multi-Authority Attribute-Based Encryption*

MA-ABE was first proposed by Chase et al. [29]. As the name suggests, there are multiple attribute authorities and multiple users. The user will have a part of the secret key from a selected attribute authority, thus, preventing collusion [22]. In a single attribute authority, only one authority is responsible of all the attributes, in other words, any inaccuracy in the single authority will affect the entire system. [29] To overcome this problem, multiple attribute authorities (AA) that are responsible for different subsets of attributes are proposed, as shown in Figure 6. In this case, users' identities are not compromised by the attribute authority service providers as no AA can decrypt a message individually.

Removing the central authority (CA) is also suggested, as the CA's responsibility was to issue a unique key for each user, meaning the CA would have the power to decrypt all the ciphertexts and, hence, access all the records. As stated by [29] the responsibility of the CA can be distributed among the AAs without jeopardizing the privacy of the users and preventing the AAs from gathering data and linking attributes that belong to the same user. For example, as shown in Figure 6, there is an AA for a group of hospitals, an AA for insurance companies and also for pharmaceutical companies. AAs could be set up for dentist clinics too.

Details regarding MA-ABE are discussed in the next chapter.

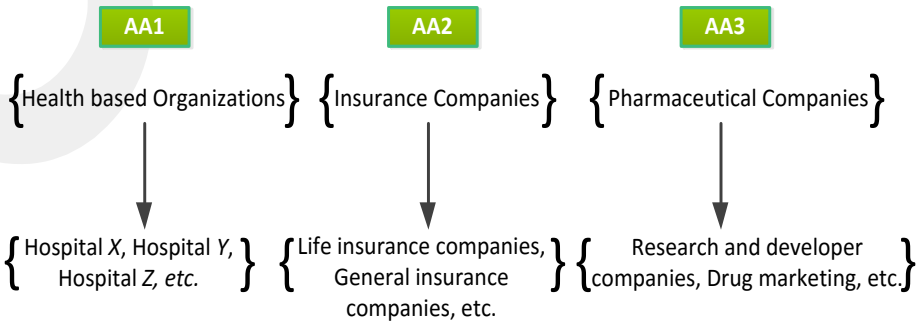

Figure 6: Each attribute authority is responsible for a subset of attributes

2.2 Related Work

Researchers who focused on the privacy of the patients and the users handled the security of both EHRs and PHRs. Some of these researches are reviewed below:

2.2.1 EHR

Löhr et al. [30] are dealing with Germans' experiences in e-health system, as Germany proposed smartcards to assure the security of the EHR data. Smartcards are used for several purposes; to authenticate patients and health care providers and authorize accessing to the EHR; to provide authenticity by signing EHR documents; and to encrypt the data before storing them in the cloud. The German electronic Health Card system (eHC) has been under development since 2010, and it is owned by both health professionals and insurance companies. Each patient has an eHC smartcard that is used for encrypting the EHR data before storing it in cloud, and authorizing access to the data and storing administrative data such as billing papers. Each professional owns a Health Professional Card (HPC) used to authenticate themselves as a permitted personnel, and to electronically sign patient documents. The health care provider holds a card reader to insert both eHC and HPC for accessing requested EHRs. When a doctor wants to update a specific record by uploading or downloading a data to a patient's EHR, the patient must provide his eHC card and enter a PIN code to start encryption when uploading or to authorize access to his EHR when downloading. In order to secure the privacy of the end user, architecture for creating privacy domains in e-health infrastructure is presented. This architecture is comprised of TVD technique to create the access structure.

The TVD creates a security framework for multi domain environments. A TVD is a collection of virtual machines that trust each other and share a mutual security policy. The TVD infrastructure contains the security kernel and some physical components that the virtual machines depend on to implement the security policies.

The advantage of using the TVD infrastructure is the transparency of key management and the policy implementation for the users. On the clients' platform, policy implementation and data encryption are handled by a security kernel without any user interface. TVD-based infrastructure may, however, increase the complexity

and the scalability problem while the security domains are implemented on each client's platform.

Narayan et al. [31] assume that there is a Trusted Authority (TA) who generates keys for users of the system. A user is associated with a unique identifier and a set of attributes. The patient decides who can access his health data and can determine the attribute set. The access policies in the system consist of "AND" and "OR" Boolean formulas in the attributes so that the patient can ensure that his file can be accessed by a specific user only if he was specified in the access policy.

The proposed approach solves the key management issues by using users' attributes for encryption. The system provides a delegation mechanism by allowing the health care providers to generate private key to delegate access rights to a subset of attributes. The system also adds a searchability function using a keyword search mechanism within a health record, and this mechanism is operated by combining the Broadcast ABE (bABE) and Public-Key Encryption with Keyword Search (PEKS). A revocation mechanism is also proposed under the patient's control; however, the scheme has a higher computational cost for the patients due to re-encryption of records when updating necessary access policies.

Zhang et al. [32] described an EHR security model for managing security issues in healthcare clouds through a use-case scenario. The researchers assume a patient centric, untrusted cloud, and role-based EHR model that provides the anonymity by using an anonymous signature mechanism, called group signatures, that allows a member from the group to anonymously sign a signature scheme in the interest of all the group members. This proposed scheme also provides the authenticity and integrity mechanism, and suggests keeping activity logs of all the access and modification attempts in the EHRs.

A research covering the security of EHRs is presented by Alshehri et al. [33]. The researchers used the CP-ABE scheme to encrypt the EHRs according to the health providers' attributes, and when decrypting the EHRs, the health providers must hold a set of attributes that are needed for accessing a specific record. The researchers proposed a design for a secure cloud-based EHR system by using CP-ABE and examined the flexibility and scalability of the system.

For encryption, all the healthcare providers share one public key, but for the decryption, each healthcare provider possesses a unique private key that is associated with a set of attributes, while the ciphertexts are associated with the access policies.

The healthcare provider can decrypt the document when their attributes satisfy the access policy of the corresponding ciphertext.

In the proposed system, the healthcare providers acquire their private keys from the attribute authority (AA) once they login to the system for the very first time, and they must install software for encrypting and decrypting EHRs in their machines. When the health provider wants to access a record, they first download the specific record and use their key and the software to decrypt it. When the health provider wants to upload a new record, they must request the attributes, create access policy, encrypt the record using previously installed software, and then upload the encrypted record. The researchers evaluated the performance of this proposed design by measuring the time and storage overheads. The results indicated that the time performance is realistic for EHR systems and the storage overheads is minor in cloud-based EHR systems, because cloud service providers always provide a large amount of storage within good prices.

2.2.2 PHR

Li et al. [34] proposed a patient-centric PHR system where users are divided into multiple domains. The MA-ABE scheme is used as an encryption method in the public domain where patient privacy is guaranteed and key escrow issue is solved, while the KP-ABE scheme is used in the private domain. The patient has full control over who are authorized to access his PHR. The owner of a PHR can also create, manage and delete his records while the users (friends, doctors, etc.) can read and write to PHR based on their access privileges issued by the owner. The model provides confidentiality, authenticity, accountability, and a revocation mechanism in addition to an access method for emergency issue is also proposed. Unfortunately, the model does not solve the circumstances when access rights are given according to the identities instead of the attributes of the users [22].

Sunny et al. [35] focused on securing PHRs and presented the multiple security domain architecture in order to reduce the key management complexity among patients and other users of the same records. In this patient-centric architecture, the patient has full control over his records and can share them between family, friends, and doctors whenever needed. The owner of the PHR has the right to choose the encryption of his records before sharing his data with others. ABE is used as an

encryption method where MA-ABE scheme is used in the public domain. This model insures the scalability of the system, provides a revocation mechanism, and a great reduction in the cost.

Barua et al. [36] proposed a patient-centric access control (PEACE) scheme where CP-ABE is used for controlling the access to patients' records and IBE is used for securing the communication amongst the patient and the healthcare provider, where the user encrypts a message using the public key of the receiver. The health care provider classifies patient's record based on the attributes set chosen by the patient himself and makes different authority levels based on the role of users that try to access a specific record.

CHAPTER 3

3.1 Comparison

In the first chapter we pointed out the major security challenges that are considered most important to sufficiently, if not completely, overcome when proposing an EHR system, and mentioned the design challenges that must be considered when designing such a system.

In this chapter we analyze a number of previous works in terms of those enumerated challenges to clarify if they cover the challenges or lack in solving them. Table 1 illustrates the works solving the security challenges, and Table 2 illustrates the works solving the design challenges.

	Challenges	PHR	EHR	Cloud Service Providers
1	**Integrity**	[36]	[30], [32]	[5]
2	**Confidentiality**	[34], [36]	[31], [32]	-
3	**Authenticity**	[35], [34]	[30], [32], [33]	-
4	**Accountability**	[34]	[32]	-
5	**Audit**	-	-	-
6	**Anonymity**	-	[32]	-
7	**Non-repudiation**	[36]	[30], [31], [32]	-

Table 1: Security challenges

1. Integrity:

- Yang et al. [5] introduced an integrity checking mechanism to check for the accuracy of the data in the cloud and also to ensure that the medical data is not tampered with or destroyed by unauthorized parties. Two types of integrity checking are proposed; local integrity, applied by the receiver and remote integrity, applied by the owner. In the first, integrity approach is proposed to check the originality of medical data for the data receiver, where

a checksum is added as the header to each record, thus, any modification to the record can be located. In the second, an integrity approach is proposed to ensure the originality of the records stored in cloud for the data owner, where only a piece of the record is selected randomly and checked to verify the integrity.

- Löhr et al. [30] : managed to provide the integrity by proposing the electronic signature mechanism using HPC cards owned by health professionals.
- Zhang et al. [32] : assumed that every patient may have more than one EHR on several health providers' servers, which means a large group of doctors have the access to a patient's record. The researchers insured the integrity of the records by proposing an EHR integrator which has two functions. First, it verifies the EHRs collected from several healthcare providers in terms of authenticity, confidentiality and whether that they satisfy the HIPAA regulations. Then, it integrates the verified EHR records into a unified EHR with a certificate signed by the integrator.
- Barua et al. [36] : managed to provide integrity by adopting cryptographic digital signature mechanism. Data recipient will verify the originality of a document by verifying the patient's signature using his/her public key.

2. Confidentiality:

- Narayan el al. [31] proposed a system that enables the patient to have ultimate control over their medical records by allowing them to decide on who has the right to access a part of their encrypted records and who does not. Owners encrypt their data using the attributes of the selected healthcare providers. The data is encrypted using symmetric key cryptography, and ABE scheme is used for making the symmetric keys available only to the authorized users.
- Zhang et al. [32] : proposed the cryptographic access control paradigm that depends on cryptography to provide confidentiality.
- Li et al. [34] : the proposed system allows the owner of a PHR to specify role-based and fine-grained access policies for their PHRs both in public and personal domains. In this system, the patients do not know the identity of the authorized users after encrypting the record.

- Barua et al. [36] : managed to provide confidentiality by adopting pseudo-identity mechanism where the identity-based encryption technique is used for securing the communication between the patient and the healthcare provider. In only the healthcare provide will know the patient's identity.

3. Authenticity:

- Löhr el al. [30] partially succeeded in solving the authenticity issue as the eHC smartcard allows the patients to decide who to authorize access to their records, On the other hand, there may be situations where the user is unable to authorize access; elder patients tend to forget their PIN; a handicapped patient might not be able to enter his PIN; the patient is unconscious, and is not accompanied by the person who knows his code; etc.. The second card HPC then allows the professionals to identify themselves as the authorized medical doctors who can access an EHR record. In this technique only card holders can authorize any access attempts.
- Zhang et al. [32] offers a signature and verification mechanism, where each physician signs the medical record with his digital signature, hence, creating a final medical certificate, and sends it to the patient; the signature mechanism. The patient, in return, verifies the authenticity of the physicians by checking the digital signature of the medical certificate without uncovering the identities of the physicians who signed the certificate.
- Alshehri et al. [33] proposed a system that offers secure cloud services responsible for storing the encrypted EHRs that are accessible only by the authorized people (healthcare givers, family and friends) through an authentication mechanism and access policies based on the attributes of the healthcare providers.
- Li et al. [34] in the personal domain of the proposed system, the patient who acts as the trusted authority of his own PHR has the control over who has the authority to access his records. This mechanism has helped ensuring the authenticity requirement as the patient will specify the access policy for his PHR file without knowing the identity of the authenticated users. In the public domain, each user obtains a secret key from the AA which is

responsible for distributing keys, and authenticating users who would like to access a specific file based on the owner specified access policy.

- Sunny et al. [35] proposed a patient-centric system where the patient will be in control of all of his medical records. The idea of [34] is used here; the researchers divided the system into two security domains as the MA-ABE scheme is used as an encryption mechanism in the public domain. The attribute authority is responsible for authenticating users that are registered in this AA through specifying an access structure that is based on the access policy defined by the owner of the PHR.

4. Accountability:

- Zhang et al. [32] assumes a trusted third party that acts as a manager, and is responsible for selecting the physicians who are going to participate in signing the medical certificate, which also gives him the right to monitor the activity of the medical group created by him.
- Li et al. [34] in the proposed system, the AAs in a public domain have the right to monitor all the activities, including access attempts to a specific record, which prevent unauthorized users from accessing a specific PHR. In the personal domain, the owner of the PHR monitors all the access attempts to his medical data.

5. Audit:

- None of the surveyed related researches were successful in providing the audit requirement.

6. Anonymity:

- Zhang et al. [32] ensured the anonymity by using the idea of anonymous signature that guarantees the anonymity of the person who signs a certificate.

7. Non-repudiation:

- Löhr et al. [30] covered the non-repudiation issue in case a medical doctor, insurance company, and a patient attempts to access EHR record.

Unfortunately, the problem is not solved in case of emergencies, such as when a medical staff has to access a record without the authorization of the patient because he can or may be unconscious; there is no mechanism that guarantees the emergency staff will not be denied access to the data.

- Narayan et al. [31] proposed a patient-centric system in which the patient has the right to choose who can access his medical record by including his identity in the access policy. The TA verifies the authenticity of the users attributes before giving them secret keys. In this mechanism, none of the users will be denied access to any record as they are all identified by the TA before attempting to make any modification.
- Zhang et al. [32] insured non-repudiation by using a digital signature technique as every practitioner signs the medical certificate with his own digital signature so that access to any file cannot be denied.
- Barua et al. [36] : adopting the digital signature mechanism ensures the integrity as well as the non-repudiation. This technique guarantees that the patient will not deny any modification to a record.

	Challenges	PHR	EHR	Cloud Service Providers
1	**Semi-Confidentiality**	-	[31]	
2	**Medical Identity Theft**	[34], [35]	[31]	-
3	**Revocation**	[34], [35]	[31], [32], [33]	-
4	**Emergency Cases**	[34]	[33], [31]	-

Table 2: Design challenges

1. Semi-Confidentiality:

- Narayan et al. [31] proposed a system which permits the patients to allow access to some of their data based on the identity of the data requester. For example, if a medical researcher wants to access a patient's record for research purposes, then the patient needs to add the identity of the researcher to the medical history or the physical examination ciphertexts.

2. Medical Identity Theft:

- Narayan et al. [31] proposed the Trusted Authority TA party that is responsible for verifying the attributes of the users before granting them private keys.
- Li et al. [34] prevented the identity thefts by proposing the AA concept. Each user has to contact the AA and identify himself to the AA in order to get the secret key associated with his attribute that grants them access to a specific record.
- Sunny et al. [35] suggested the same idea in [34].

3. Revocation:

- Narayan et al. [31] are proposing a revocation mechanism by creating a new policy; a variation of ABE that allows the patient to revoke the access rights of a specific healthcare provider without changing other policies using Broadcast Ciphertext-Policy ABE mechanism.
- Zhang et al. [32] the trusted third party; the manager, is responsible for selecting the practitioners, forming a team consisting of those who are going to participate in signing the medical certificate, and has the right to revoke them after they are done with the treatment.
- Alshehri et al. [33] proposed a system that allows the owners of the EHRs to revoke a user either by adding an expiration date to the access policies, or by re-encrypting the records with a new access policy, thus, preventing the user from accessing a specific record that may have been previously accessable.
- Li et al. [34] proposed that the attribute authorities in the proposed system should be responsible for the revoking operation in the public domain. There are two types of revocation in the public domain done by using the KP-ABE mechanism. First is the revocation of a role attribute of a public domain user. Second is the revocation of the public domain user, which may require removing all his attributes. In the private domain, there are two types of revocation where the patient is responsible of the operation. First is the revocation of a personal domain user's access rights. Second is the revocation of a personal domain user.

- Sunny et al. [35] propose that the attribute authority the user is registered in is responsible for revoking him for a specific reason. The AA will revoke a user or his attribute in the public domain by re-encrypting the ciphertexts and updating all other users' secret keys.

4. Emergency Cases:

- Narayan et al. [31] claim that a temporary access right can be granted for the emergency department by the TA which can override the access right to a record when an emergency case takes place.
- Alshehri et al. [33]: the attribute authority which is responsible of distributing the keys is also responsible of generating a secret key for the emergency department whenever necessary.
- Li et al. [34] proposed a break-glass mechanism, where the owner of PHR delegates the access right to the emergency department (ED) directly. The emergency staff contacts the department and verifies the patient's identity to obtain a temporary key to the patient's records, and after the emergency case ends, the patient can revoke the emergency access by updating the ciphertext and sending a new key to the emergency department.

CHAPTER 4

A MA-ABE BASED PATIENT CENTRIC PHR SYSTEM

4.1 Overview of the Improved System

In the beginning of this chapter we clarify the difference between the Electronic Health Records (EHR) and the Personal Health Records (PHR), and define the entities that play the leading role in designing a complete system.

The entities in an e-health system may be classified in two groups:

Medical data Owner: The patient that is going to use the health system is also the client who has full control over his medical records.

User: The entities that are going to contribute to the owner's medical record based on their access privileges. There are two types of users; private and professional users.

Private users: Family members and close friends chosen by the patient himself in order to help him whenever it's necessary (e.g. emergency cases).

Professional users: Medical care givers that are going to read or write into the patient's medical record based on their access privileges. These users can be doctors, nurses, physical therapists, physician assistants, medical students, etc. The doctors may be from any special field such as a cardiologist, neurologist, psychiatrist, surgeon, etc. There are some professional users such as insurance companies, pharmaceutical companies, and some medical branches, such as dentists and health educators, that are not included in the hospital organization, but can work in conjunction with hospital staff.

In this study, the approach is a patient-centric model, which is by far the most accepted methodology in e-health structure, where the patients should have full control over their medical records. In such a system the PHR is created, managed, and in some cases, deleted by the patient. The data is accessible by healthcare givers upon proper requests and with the condition of acceptance by the patient himself.

The cloud service provider and the parties that are attempting to access any record must agree on the conditions of HIPAA, and must not expose patient's privacy under any condition. However, the data stored in third party servers are exposed to

malicious attacks, which in turn need solid security methods that we will not talk about in this study.

We are assuming that every user has a public and private key pair, and that the server is a semi-trusted cloud server that does not expose the identity of patients intentionally, but it is considered to be “curious”; it will try to know as much information about the patient as possible.

4.2 Brief Description of the Patient-Centric PHR System

In this system, a structure that divides the system into multiple security domains called Professional Domain (PRD) and Personal Domain (PSD) is proposed.

The professional domain includes users like heath specialists, such as doctors, surgeons, nurses, pharmacists and insurance companies, and this type of classification is called role attributes. In order to control the large amount of users with different types of roles, a multi authority ABE (MA-ABE) scheme is adopted. Each PRD operates with a separate MA-ABE scheme. The owner does not need to know the actual list of the authorized users when encrypting his record. In this scheme there are multiple attribute authorities (AA) such as the AAs shown in Figure 6 Each AA is responsible for controlling a subset of a health organization’s attributes.

The users in PRD will acquire their unique key from the corresponding AA according to an access structure without having to communicate with the owner personally.

The access structure in the proposed system is created by the patient and consists of Boolean formulas, where the leaf nodes are the role attributes of the users. Figure 7 is an example for an access structure created by a patient who has health problems that require cardiologist or endocrinologist based on his needs. In this case the patient will create an access policy *P* and puts his criteria as follows:

((“doctor” AND “age > 35” OR “physician assistant” AND “age > 25”) AND (“cardiologist” OR “endocrinologist”) AND (“hospital X” OR “hospital Y” OR “hospital Z”)). By this the patient can make his record available to only doctors who are older than 35 years, or physician assistants who are older than 25 years with cardiology or endocrinology specialty, and are working in hospital X or hospital Y or hospital Z only.

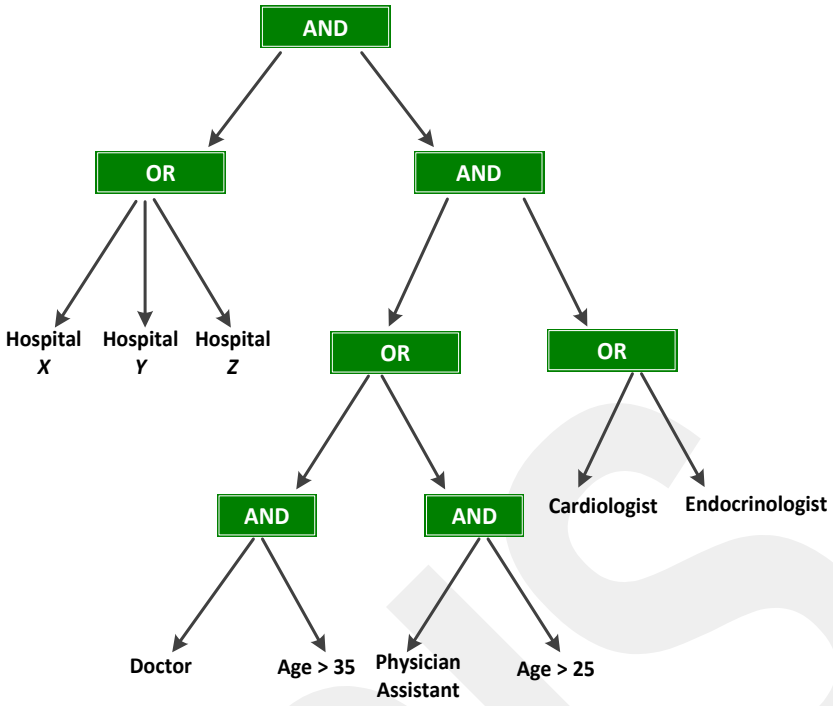

Figure 7: An example for a role-based access structure

The patient creates a PHR file, such as F1, which consists of his personal medical information. This file is created only once, and has a hierarchical structure, where the nodes represent the type of the medical information, such as allergies and prescription; this type of classification is called PHR data attributes. Figure 8 illustrates an example showing the structure of a PHR file.

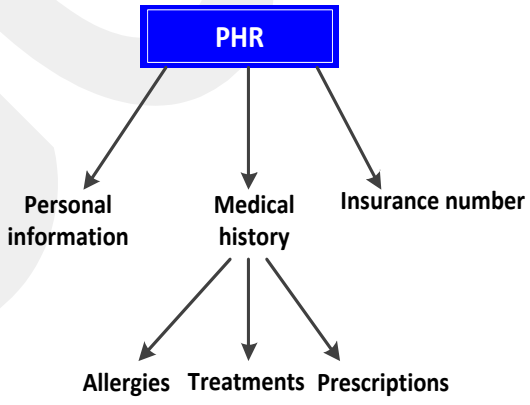

Figure 8: An example for a PHR file

The PSD includes users personally known to the owner (like family and close friends). The access communications between users and the owner will be direct

without the need for any additional attribute authority as the patient can specify these users by granting them access rights. Ciphertext policy-ABE (CP-ABE) scheme is used as the encryption method in PSD to easily revoke a user whenever it is necessary.

The main reason for choosing a multi security domain system is to increase the security performance, hence, there are multiple attribute authorities in PRD, none of which will be able to control the whole system alone or be able to decrypt a record even if they are allied, which may ease the burden of the owner without weakening the security. In the PSD the owner acts as an authority who governs only a handful of users that are close to him, which in return eases the burden of the attribute authorities.

4.3 How the System Works

In the proposed patient-centric system, multi authority concept is used. In this system, there are multiple PHR owners, multiple users, multiple security domains, and multiple attribute authorities AAs. The type of scheme adopted in each security domain is enumerated below.

The owner of a PHR record will encrypt F1 two times. First, encrypts it under an access structure for the users in PSD. Second, encrypts it under attributes for the users in PSD.

4.3.1 Professional Domain

In PRD a MA-ABE method is presented in two combinations, CP-ABE and KP-ABE.

A. CP-based MA-ABE

CP-based MA-ABE method was proposed by Lewko et al. [37]. In order to understand how a CP-based MA-ABE scheme works in the professional domain, we take an example of a patient that communicates with a health-based organization third party. The steps are enumerated below:

Step 1: The patient creates his PHR file for the first time as shown in Figure 8.

Step 2: The patient creates an access structure for the health organization as shown in Figure 7.

Step 3: Using CP-based MA-ABE scheme the patient encrypts his PHR file under an access structure (constructed in step 2) creating a ciphertext and sending it to the AA. In another words a separate ciphertext is created for every role-attribute in the access structure tree.

Step 4: If a healthcare provider, such as hospital X, is registered with trusted third party AA (a health based organization), the hospital administration obtains their private key from the AA labeled with role-attributes. This step is invisible to the patient.

As illustrated in Figure 9 any user in hospital X will communicate with the administration to obtain their secret key. In order to be able to decrypt a file, the user's attribute, which is associated with the secret key, should match the criteria specified in the access structure.

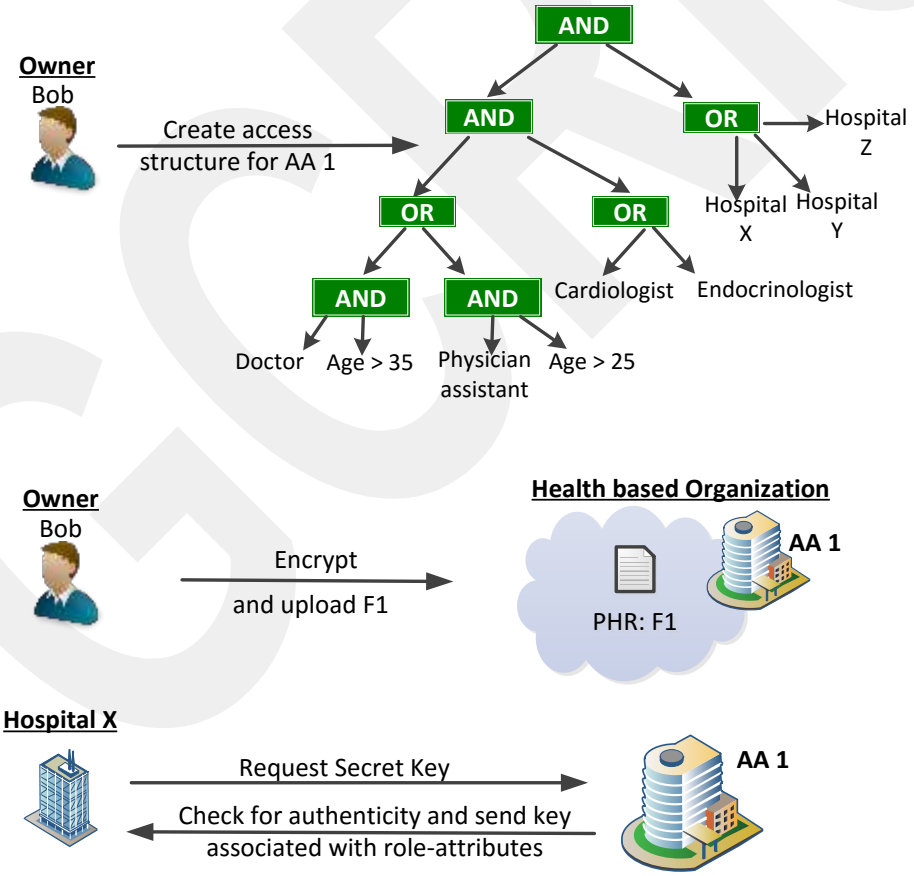

Figure 9: An example for CP-based MA-ABE in PRD

In the example shown in Figure 10, the user Alice, who is a 28 years old physician assistant at hospital X, wants to access F1. She can decrypt the file since the attributes that are associated with her key match the access structure that is associated with the ciphertext she wants to decrypt. On the other hand John who is a 30 years old doctor at hospital Y will not be able to decrypt F1.

The CP-based MA-ABE method consists of five algorithms that are explained in detail in [37].

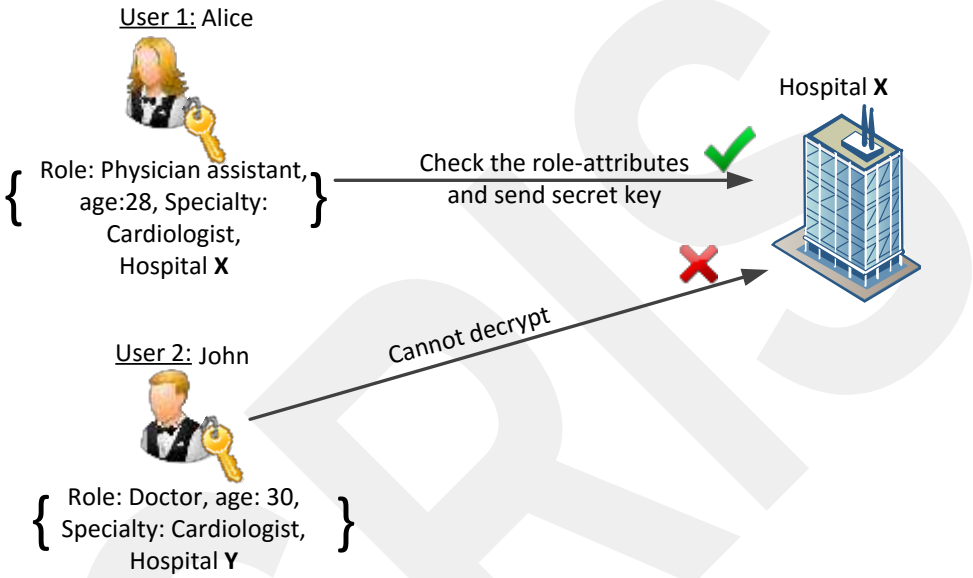

Figure 10: An example for the process in the professional domain

Revocation: in the CP-based MA-ABE structure, the revocation operation is operated by the AA that the user registered to. This takes place in two ways: first; *revoking a user*, which means removing all the attributes of a user, such as revoking hospital Z and all of their attributes. The second is *revoking the role-attribute of a user*, such as revoking one or all the residents from the hospital Z.

In the first way, the process of revocation requires the AA to update the access structure associated with the ciphertext, which the revoked user was previously able to decrypt; there is no need to distribute new secret keys to the unrevoked users.

In the second way, the AA needs to update a specific ciphertext that contains that role-attribute which the revoked role-attribute was able to decrypt previously, and send a new key to other users that have the same role.

Write access policy: after an authorized healthcare provider in a hospital examines a patient he has to access this patient's record in order to add the latest reports and prescriptions, and then has to upload it to the hospital's secure server.

The hospital administration will re-encrypt the record using the corresponding AA's public key. The AA decrypts the record with their private key, has to update all the ciphertexts, and distribute new keys to the users so that other care givers who are authorized by the patient in the access structure can see the latest version of this particular record.

This operation is considered a weakness of CP-based MA-ABE scheme because of the necessity to re-encrypt all the ciphertext and regenerate new keys which is considered to be a time consuming operation.

B. KP-based MA-ABE

The first original MA-ABE scheme, which was proposed by Chase [29], is a KP-based MA-ABE scheme.

The owner encrypts his PHR file under role-attributes using KP-based MA-ABE scheme. The ciphertext is associated with owner specified set of attributes, and sends them to the AA. In another words, a separate ciphertext is created for every set of attributes.

If a healthcare provider such as hospital X is registered with trusted third party AA, the hospital administration will obtain their private key from the AA associated with the owner defined access structure (constructed in step 2), thus, specifying the type of ciphertext this key can decrypt.

A user in hospital X communicates with the administration to obtain his secret key. The user is able to decrypt a file only if his key, which is associated with the access structure, matches the attribute set criteria specified in the ciphertext.

In the example shown in Figure 11, the user Alice is able to decrypt the file since the access structure in her key matches the attribute set associated with the ciphertext she wants to decrypt. On the other hand, John is not authorized to decrypt F1 because the access structure that is associated with his key does not satisfy the set of attributes definite by hospital X.

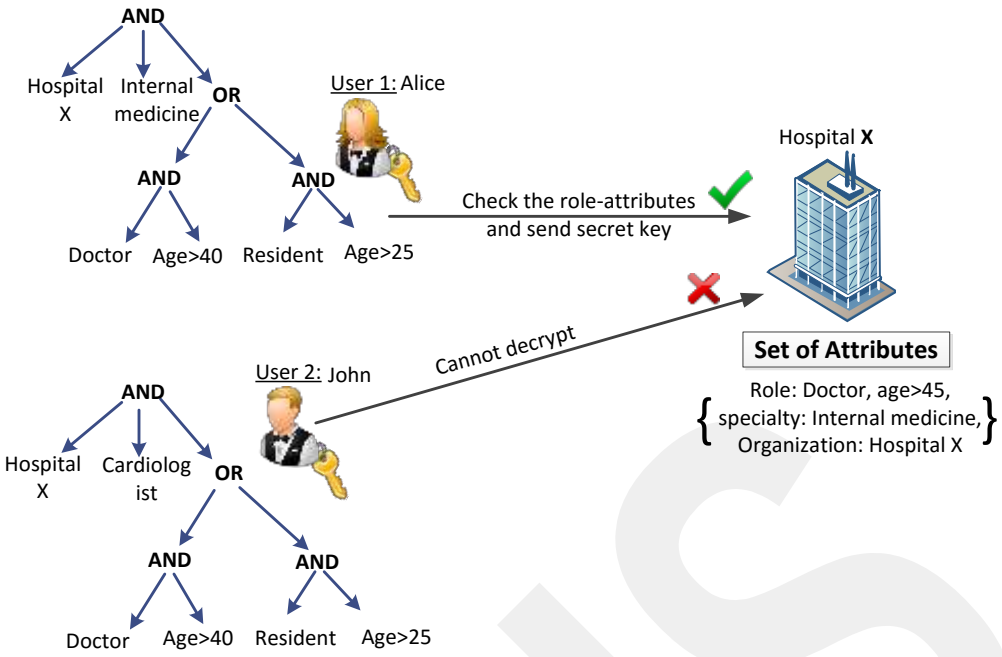

Figure 11: An example for KP-based MA-ABE in PRD

The KP-based MA-ABE method consists of four algorithms based on secret sharing scheme, which is explained in detail in [29].

Revocation: In the KP-based MA-ABE structure, the revocation operation is operated by the AA that the user registered to. It also takes place in two ways, as mentioned in the previous section. The difference here is that, after revoking the user or one of his attributes, the AA needs to update the secret key of other users, and update the ciphertext because it contains the revoked user's attributes.

In the second way, the AA needs to update the ciphertext that contains the role-attribute which the revoked role-attribute was able to decrypt previously, and send a new key to other users that have the same role.

Write access policy: In KP-based MA-ABE, the same writing mechanism is presented, but the most evident difference is that, after the AA receives the encrypted record from the hospital and decrypts it with their private key, it only updates the ciphertexts associated with this attribute, and send new keys to other care givers who have been authorized by the patient in the access structure. After updating, it will be uploaded to the cloud server so the latest version of this particular record can be accessed by other care givers.

This operation is considered easier as compared to CP-based MA-ABE scheme because of the necessity to re-encrypt only a small number of ciphertexts.

4.3.2 Personal Domain

In the PSD, the CP-ABE scheme is used. It was originally proposed by Bethencourt et al. [27]. The simplicity of CP-ABE makes it ideal for the PSD. As mentioned before, the patient is the trusted authority of his PHR document, no need for extra attribute authority as the number of users is not big.

As an AA, the patient is responsible for distributing the secret keys for the users he chooses to share his medical data with. He will encrypt his PHR file under an access structure, thus, specifying which user will decrypt his PHR. Figure 12 is an example of a user, Jack, who wants to access PHR file F1. He first sends a request to the owner. As a standard CP-ABE algorithm, the owner will generate a secret key based on the receiver's attribute.

The number of ciphertexts is linear with the number of role-attributes. There are no problems regarding key management as the number of attributes is limited to only some family members and close friends.

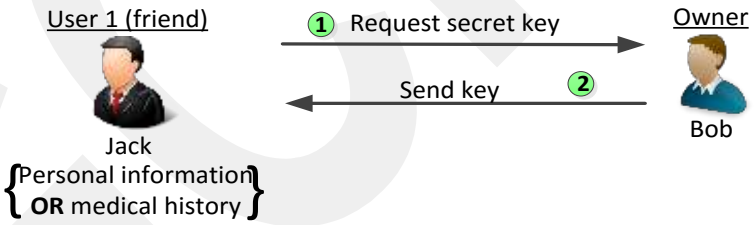

Figure 12: An example for CP-ABE in PSD

Revocation: the revocation of a user is directly operated by the patient himself. The owner of the PHR document needs to update the access structure associated with the ciphertext which the revoked user was able to decrypt previously. No need to distribute new secret keys to the unrevoked users.

4.3.3 Emergency Department

Every patient at some point of his life is exposed to an unexpected health situation that requires him to go to the emergency department. What if the patient had a car accident leaving him unconscious so that he couldn't communicate with the hospital for the standard procedure of authorizing users?

For these kinds of situations, there must be a mechanism to overstep all the routine processes and act as quickly as possible to save a human life. An example of an emergency case is illustrated in Figure 13.

The steps for handling an emergency situation are enumerated below:

Step 1: When the patient encrypts his PHR file in the PSD part of the system using CP-ABE scheme, he will include an emergency attribute in his access structure which is associated with the ciphertext.

Step 2: The patient will generate a secret key and sends it directly to the emergency department.

When an emergency situation takes place, a user will have to contact the emergency department that he is registered in. The emergency department will check for this user's authenticity. If he is authentic, then the emergency department will send a temporary read key to this user. After the emergency is over, the patient must revoke the user, update the ciphertext, regenerate a new secret key, and send it to the emergency department.

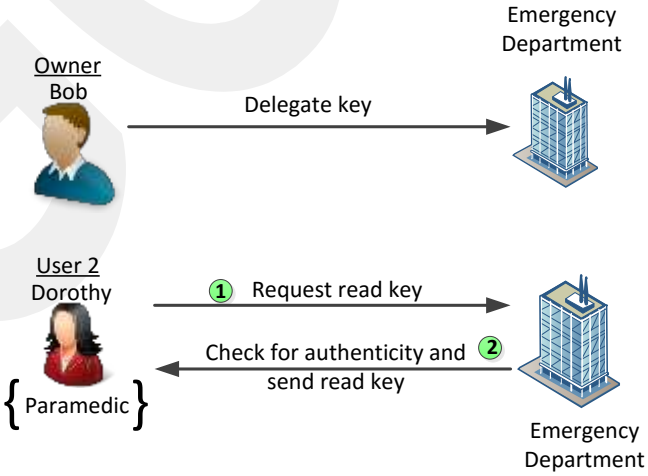

Figure 13: An example of the emergency case

Besides the emergency department, there may be situations where elder patient is unable to authorize access or modify his record and he needs the help of a family member or a friend. In this case family and friends can use their secret key which is previously obtained from the patient in order to access his record whenever an emergency situation takes place.

4.4 Evaluating the Security Challenges of the Improved System

1. **Integrity:**

   It is significant to decide whether or not modifications have been made to a specific document when it is transmitted between users and AAs. The hash function is used to verify the integrity of a document, where the input is a message, and the output is a string called digest. The integrity checking mechanism is utilized by the data user and can be done by comparing the digest before and after transmission. This mechanism insures that the document is unmodified during transmission.

2. **Confidentiality:**

   Adopting the attribute-based encryption mechanism has an advantage of securing the confidentiality of the records. The patient-centric system allows the patient to decide who has the authority to access their medical records by granting them access rights, and creating access structures that authorize only the users chosen by the patient.

3. **Authenticity:**

   To ensure the authenticity of the person who wants to access a record in professional domain, the AA obligates every user registered in it to use a digital signature mechanism. After making the necessary updates on a record, the doctor will sign the document with his private key and send it to the AA. The AA, in return, will verify the authenticity of the doctor by using the user's public key stored in the directory.

4. **Accountability:**

   The attribute authorities in the professional domain are responsible for monitoring all the access attempts by the authorized users in registered hospitals, clinics, and insurance companies. The PHR owner is responsible for monitoring all the access attempts by the authorized entities in the personal domain.

5. **Audit:**

   Healthcare organizations that act as the AA can create and maintain a record of user activities, and use these access logs to investigate possible violations without uncovering the patients' identities. Access to the activity log must be limited to the authorized users only. Thus, only those users who have signed the confidentiality agreement may view the log.

6. **Anonymity:**

   The patient's identity must be kept anonymous to all the users, in our improved system only the attribute authority will know the original identity of the patient. Although Sweeney et al. [38] proposed K-Anonymity approach where the personal information for each patient can not be distinguished from at least k-1 patients who have the same information. The proposed solution is to replace these identifiers with less specific values such as wildcards, but this approach is not suitable in our improved system.

7. **Non-repudiation:**

   Using the digital signature mechanism also ensures the non-repudiation as the user who will sign the document with his digital signature cannot deny accessing any record.

8. **Semi-Confidentiality:**

   There are some situations where sharing patients' medical information can help a researcher to investigate some medical conditions, but this will require the patient to give access to his record. In our improved system the patient

does not have direct communication with any user except the AA, in this case he will not be able to grant access upon request from the researcher.

9. **Medical Identity Theft:**

   Proposing the AA concept helps in preventing identity theft. Each user has to contact the AA and identify himself to him in order to get the secret key associated with his attribute that grants them access to a specific record. As previously stated the AA keeps an activity log for all the access attempts to investigate possible violations.

10. **Revocation:**

    Our improved system provides a revocation mechanism in both professional and personal domain which is described in detail in the previous section.

11. **Emergency Cases**

    Our improved system provides a mechanism to handle emergency situations which is described in detail in the previous section.

CHAPTER 5

CONCLUSION AND FUTURE WORK

- In order to provide full security and ensure the privacy of patients, focusing on securing the health provider platform will not be sufficient. Securing cloud service providers must also considered. In order to assure the security of data stored in cloud, the cloud service providers must agree on some certifications such as SNS70 Type II, PCI D55 Level 1, and ISO 27001. This work takes only the privacy of health care providers and patients into consideration-the security of cloud service providers is out of scope in this study.
- Some EHRs are collected in a smart card which is encrypted with a redundant key. Countries using the smartcard technique, such as Germany and Austria, are requiring the patients to have full authority on their EHR data, which means nobody can avoid the access rights of the patients' data. But a restore method should be presented in case the card was lost, stolen, or the patient can't remember his access code. This restore point must be well protected against any unauthorized access attempts; since the card issuer keeps a backup copy of the keys he will have access to any record he desires and this action will jeopardize the privacy of all the patients, and threatens the confidentiality of the whole system [31].
- The professional domain contains a large number of users, which makes it hard to control them all. The studies concerning this topic are still ongoing, and designing the ideal patient-centric with an efficient access mechanism is yet a challenging topic for the researchers.
- There are two PHR systems proposed in this work and they are presented in the professional domain. The first is the process of handling a CP-based MA-ABE scheme. The second is the process of using a KP-based MA-ABE scheme; both are operated in the professional domain. In this study we conclude that both schemes have their strong and weak points. When the CP-based MA-ABE scheme is used, the PHR document is encrypted based on the access structure tree; there are ciphertexts for every single role-attribute that is included in the access structure tree, which means the time for encryption algorithm increases when the number of attributes increase in the access

structure tree. On the other hand, when a KP-based MA-ABE is used, the PHR document is encrypted based on a set of attributes which makes the number of ciphertexts much more reasonable compared to the first method. Since there are multiple ciphertexts, revoking a user, or one of his attributes, is easier in the CP-based MA-ABE scheme as compared to the KP-based MA-ABE. As when revoking a user, the AA only needs to update the access policy associated with the ciphertext that the user was able to access previously without having to regenerate a secret key for the unrevoked users. On the other hand, revoking a user in KP-based MA-ABE requires updating the ciphertexts and regenerating keys, which requires more time.

The write access policy mechanism in CP-based MA-ABE is considered weaker than a KP-based MA-ABE. In the first scheme, after writing to a record, the AA should update all the ciphertexts and regenerate keys for the users so they can access the updated version of this record. In the second scheme, only the ciphertext containing the specific attribute will be updated.

In the future, a benchmark test may be written for both models to be compared with other existing studies in order to verify the efficiency and privacy. The anonymity and semi-confidentiality challenges can be investigated to be included in our improved system.

REFERENCES

[1] The American Health Information Management Association (AHIMA), "The American Health Information Management Association (AHIMA)," 2015. [Online]. Available: http://www.myphr.com/StartaPHR/what_is_a_phr.aspx.

[2] U.S. Department of Heath and Human Services, "HIPAA Privacy Rule," 02 February 2007. [Online]. Available: http://privacyruleandresearch.nih.gov/pr_06.asp. [Accessed 01 April 2015].

[3] J. J. R. and R. M. D. e. B. , "Analysis of the Security and Privacy Requirements of Cloud-Baesd Electronic Health Records Systems," *Journal of Medical Internet Research,* 2013.

[4] K. Conover, M.D. and FACEP, "ed-informatics," 2015. [Online]. Available: http://ed-informatics.org/healthcare-it-in-a-nutshell-2/emr-vs-ehr-vs-phr/.

[5] J. Y. Ji, Q. L. Jian and N. Yu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," *Future Generation Computer Systems,* p. 13, 2014.

[6] E. A. N. M. and J. A.-J. , "e-Health Cloud: Opportunities and Challenges," *Future internet,* 4 July 2012.

[7] S. Good, "Forbs," 5 February 2013. [Online]. Available: http://www.forbes.com/sites/centurylink/2013/05/02/why-healthcare-must-embrace-cloud-computing/.

[8] Y. Zheng, "Privacy-Preserving Personal Health Record System using Attribute-Based Encryption," 2011.

[9] M. L. S. Y. K. R. and W. L. , "Securing Personal Health Records in Cloud Computing: Patient Centric and Fine-Grained Data Access Control in Multi-owner Settings," *IEEE Transactions on Parallel and Distributed Systems,* 2010.

[10] A. M.-H. K. "Opportunities and Challenges of Cloud Computing to Improve Health Care Services," *Journal of Medical Internet Research,* 2011.

[11] E. J. M. and E. H. , "Centers for Disease Control and Prevention," February 2015. [Online]. Available: http://www.cdc.gov/nchs/data/databriefs/db187.htm.

[12] S. R. Stout, "Real World Experience With Electronic Health Record Software," 2011. [Online]. Available: http://www.plasticsurgerypulsenews.com/6/article_dtl.php?QnCategoryID=57&QnArticleID=126.

[13] "Acumen Solutions® Wins Health & Human Services Contract for Cloud Computing Services in Support of Electronic Health Records (EHR)," 2010. [Online]. Available:

http://www.businesswire.com/news/home/20100217006169/en/Acumen-Solutions%C2%AE-Wins-Health-Human-Services-Contract#.VVd56vmqqko.

[14] S. Soumerai and T. A. , "The Blog," 25 May 2011. [Online]. Available: http://www.huffingtonpost.com/stephen-soumerai/dont-repeat-the-uks-elect_b_790470.html.

[15] R. Syal, "Abandoned NHS IT system has cost £10bn so far," 18 September 2013. [Online]. Available: http://www.theguardian.com/society/2013/sep/18/nhs-records-system-10bn.

[16] Alberta Health, "Alberta Netcare EHR," 2015. [Online]. Available: http://www.albertanetcare.ca/.

[17] Ontario Health, "eHealth Ontario," 2015. [Online]. Available: http://www.ehealthontario.on.ca/en/.

[18] T. Tuten, "8 Countries Doing Electronic Health Records Right," 3 April 2012. [Online]. Available: http://blog.soliant.com/healthcare-news/8-countries-doing-electronic-health-records-right/.

[19] J. Conn, "Jordan EHR project could have global effect: experts," 10 December 2008. [Online]. Available: http://www.modernhealthcare.com/article/20081210/NEWS/312109996.

[20] N. Yurt, "Turkey's e-Health Activities A country Case Study," Ministry of Health, 2008.

[21] T.C. Sağlık Bakanlığı, "e-nabız Kişisel Sağlık Sistemi," 2015. [Online]. Available: https://enabiz.gov.tr/Giris.aspx. [Accessed 2 July 2015].

[22] A. A. and S. U. K. , "A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds," *IEEE Journal of Biomedical And Health Informatics*, 4 July 2014.

[23] Smart Card Alliance, "Medical Identity Theft in Healthcare," March 2010. [Online]. Available: http://www.smartcardalliance.org/publications-medical-identity-theft-in-healthcare/. [Accessed 30 May 2015].

[24] A. Shamir, "Identity-Based Cryptosystem and Signature Scheme," in *CRYPTO*, 1984.

[25] Secure Mail Works, "Identity-Based Encryption," [Online]. Available: http://www.securemailworks.com/Identity-Based-Encryption.asp. [Accessed 1 June 2015].

[26] A. Sahai and B. W. , "Fuzzy Identity-Based Encryption," *IEEE*, 2005.

[27] J. Bethencourt, A. S. and B. W. , "Ciphertext-Policy Attribute-Based Encryption," *IEEE*, 2007.

[28] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in *CCS*, 2009.

[29] M. Chase and S. C. , "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in *In Proceedings of the 16th ACM conference on*

Computer and communications security, 2009.

[30] H. L. A.-R. S. and M. W. , "Securing the E-Health," in *ACM International Health Informatics Symposium*.

[31] S. N. M. G. and R. S.-N. , "Privacy Preserving EHR System Using Attribute-Based Infrastructure," 2010.

[32] R. Z. and L. L. , "Security Models and Requirements for Healthcare Application Clouds," in *IEEE 3rd International Conference on Cloud Computing*, 2010.

[33] S. A. S. R. and R. K. R. , "Designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption," in *Data Management in the Cloud Workshop*, 2012.

[34] M. L. S. Y. Y. Z. K. R. and W. L. , "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption," *IEEE Transactions on Parallel and Distributed Systems,* no. 2012.

[35] S. S. and L. A. , "Secure Data Sharing of Patient Record in Cloud Environment using Attribute Based Encryption," *International Journal of Applied Engineering Research*, 2013.

[36] M. Barua, X. Liang, R. Lu and X. (. S. , "PEACE: An Efficient and Secure Patient-centric Access Control Scheme for eHealth Care System," *The First International Workshop on Security in Computers, Networking and Communications,* 2011.

[37] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," in *Advances in Cryptology-EUROCRYPT*, 2011.

[38] L. Sweeney, "K-Anonymity: A Model for Protecting Privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* vol. 10, no. 5, 2002.

APPENDICES A

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Hurmuzlu, Mine

Date and Place of Birth: 14 November 1988, Kerkük

Marital Status: Married

Nationality: Iraqi, Turkish

Phone: +90 531 732 44 38

Email: mine.hurmuzlu@gmail.com

EDUCATION

Degree	Institution	Year of Graduation
M.Sc.	Çankaya Univ., Computer Engineering	2015
B.Sc.	Kirkuk Technical College, Software Engineering	2010

WORK EXPERIENCE

Year	Place	Enrollment
2010- 2013	Kirkuk Technical Institute. Computer Systems Dept.	Assistant Engineer

FOREIGN LANGUAGES

English, Arabic