DEMOCRATIC REPUBLIC OF ALGERIA PEOPLE
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY MOHAMED BOUDIAF - M'SILA

FACULTY: Mathematics and Informatics
DEPARTEMENT of Computer Science
N° : ……..

DOMAINE : COMPUTER SCIENSE
FILIERE : COMPUTER SCIENSE
OPTION : SIGL

A Dissertation in Fulfillment
for the Requirement of the Degree of MASTER

By: TALLAB Lebna

Subject:

Security Techniques for Protecting Patient Data in Healthcare Applications

Defended to the jury:

Brahimi Belkacem	University of M’sila	Chairman
Noureddin Chikouche	University of M’sila	Supervisor
Tahri.Z	University of M’sila	Examiner

Academic year: 2020 /2021

Dedication

To my family, for their endless love, support and encouragement.

ACKNOWLEDGEMENTS

Foremost, I am grateful to the almighty ALLAH for helping me to complete this research paper.

I would like to extend my appreciation to my advisor CHIKOUCHE Noureddine, for all his guidance, and for his timely and highly up to the mark feedback and support.

I would like to extend my gratitude to my fiancé BOUDIAF Yasser for helping me in this research paper, and having my back all the time of preparation.

My deep gratitude goes to my family, sisters and brothers for their encouragement and inspiration in all my undertakings. I would also like to express my love and gratitude to my friend for her support.

Contents

GENERAL INTRODUCTION

Digitalization is becoming increasingly popular in healthcare, in which documents containing sensitive patient information are developed as electronic healthcare record. When compared to saving information on paper, this raises concerns regarding the security of the documents being stored, such as the confidentiality and integrity of the records.

There is still the issue of access control, namely who is authorized to read or edit the document, as well as the issue of easy copying. Copying a digital document is far easier than copying a paper document. When an attacker gains access to a hospital workstation, they can copy papers from that workstation.

The critical difference between paper documents and electronic records is that an adversary does not have to be present in the hospital, to acquire access to patient information, hackers only need to hack a workstation at the hospital that is connected to the internet. The main problem is how to protect and solve the issue of security and privacy of patient's data.

The main aim of this work is to propose an improved security technique to ensure the confidentiality of the electronic health records (EHR).

We develop a simple system for managing EHR stored in database countian patient's information, such as private information, medical history, physical examination, medication use history, immunization status, we implement one of security technique with a cryptography for achieve our objective to protect patient's data.

We use the attribute-based encryption algorithm to implement the security technique in this system, we use in this work multiple tools and technologies to build the system, such as C# as a programming language, SQL server for relational database. Finally, the research comes to an end with a summary of the results.

Outline:

Chapter 1:

Presentation of healthcare system and his architecture, it includes the patient's information as paper documents and as an electronic health record.

Chapter 2:

The second chapter includes the main concepts of security for EHR such as: security requirement, Attacks on EHR, then, we present security mechanisms for protecting patient's data.

Chapter 3:

The last chapter contain implementation of the solution that we propose in pervious chapter, first we develop EHR system then we apply the security technique.

CHAPTER 01

HEALTHCARE SYSTEM

1.1 Introduction

This chapter starts by defining the health care systems and all the main part of it such as WBAN systems and their communication. Then, a general description about patient's health record and electronic health record.

1.2 Definition of healthcare systems

In the physical world, a system may be thought of as an abstract representation of objects or processes, a model or a natural artefact according to this view, health system can be thought of as an interpretation of the health system based on an abstract representation, a descriptive model representing the functionalities of a health system, or the technological, logistical and administrative infrastructure, which relates to the health system. An explanation of a health system may be any of the three, a combination of them, or all three used together [1].

Field proposed a broad definition of health care system in 1973 [2]; in this definition, health care system is defined as:

"The aggregate of commitment or resources which any nation society "invests" in the health concern, as distinguished for the other concerns. The health system is viewed in a structural-functional perspective: it provides services to individuals whose role performance might be jeopardized by ill-health and it occupies a specific structural position in social space.".

So, from this definition we can say that a healthcare system is a highly complex phenomenon. It is a system whereby the primary purpose is to improve populations' health and well-being, embracing all participants who are active in protecting people against ill health, treating the sick and protecting people from the costs of ill-health [3].

1.2.1 Measure of healthcare system performance

Health systems are subject to nations' economic strength and political stability, but they are also shaped by interaction with other sectors of a society, neighboring countries and international organizations, as well as a range of national characteristics such as cultural inheritance, religion, norms and dominant political ideologies, behavior and social capital [4].

No single universally accepted measure exists to assess health system performance, but in 2000 the World Health Organization [5] made an attempt to establish an index for health systems performance, suggesting three intrinsic factors to be used as measures: health outcomes, responsiveness and fair financing.

- ✓ Health outcome measures were based on disability adjusted life expectancy and health equality in terms of child survival.
- ✓ Responsiveness was a new concept established to measure how well a health system met the legitimate expectations of the population regarding the non-health enhancing aspects of the system.
- ✓ The third factor, fair financing and financial risk protection, measured how health systems assure that households do not become impoverished regarding obtaining necessary health care.

The World Health Organization report from 2000 provoked a strong debate, especially in relation to its methodology and data availability and reliability.

1.3 Digitalization of healthcare systems:

The first appearance of digitalization in the healthcare systems was in 1928 to standardize medical records the American College of Surgeons (ACOS) was founded the Association of Record Librarians of North America (ARLNA) now known as the American Health Information Management Association (AHIMA) [6].

The digitalization of healthcare system focused on how to transform paper medical record to medical electronic record, the first use of electronic record was in 1995 were being used in only 75 hospitals because the technology in that time was expensive and only the larger providers have the capacity to invest in medical record technology.

1.4 Architecture of healthcare systems

In order to understand the architecture of healthcare systems first we need to know the main part of the architecture which is the WBAN.

1.4.1 Definition of WABN

A Wireless Body Area Network (WBAN) it is a multiple of sensors that connect independently and situated in the clothes, on the body or under the skin of a person. The network usually covers the entire human body, with nodes connected by a wireless communication channel [7].

Many interesting new applications in the field of remote health monitoring are available with a WBAN. In the medical field, for example, a patient's body can be fitted with a wireless body area network of sensors that constantly monitor specific biological functions.

The benefit is that the patient does not have to stay in bed and can freely move around the room, if necessary, and even leave the hospital. The patient's quality of life is improved, and hospital costs are reduced. Furthermore, data collected over a longer length of time and in the patient's natural environment provides more meaningful information, allowing for a more accurate and faster diagnosis [7].

1.4.2 The communication architecture in WBAN

Therefore, we present an overview of the communication architecture of WBANs in this section. In the **Fig 1.1** we review the architecture of healthcare monitoring system with WBAN communication.

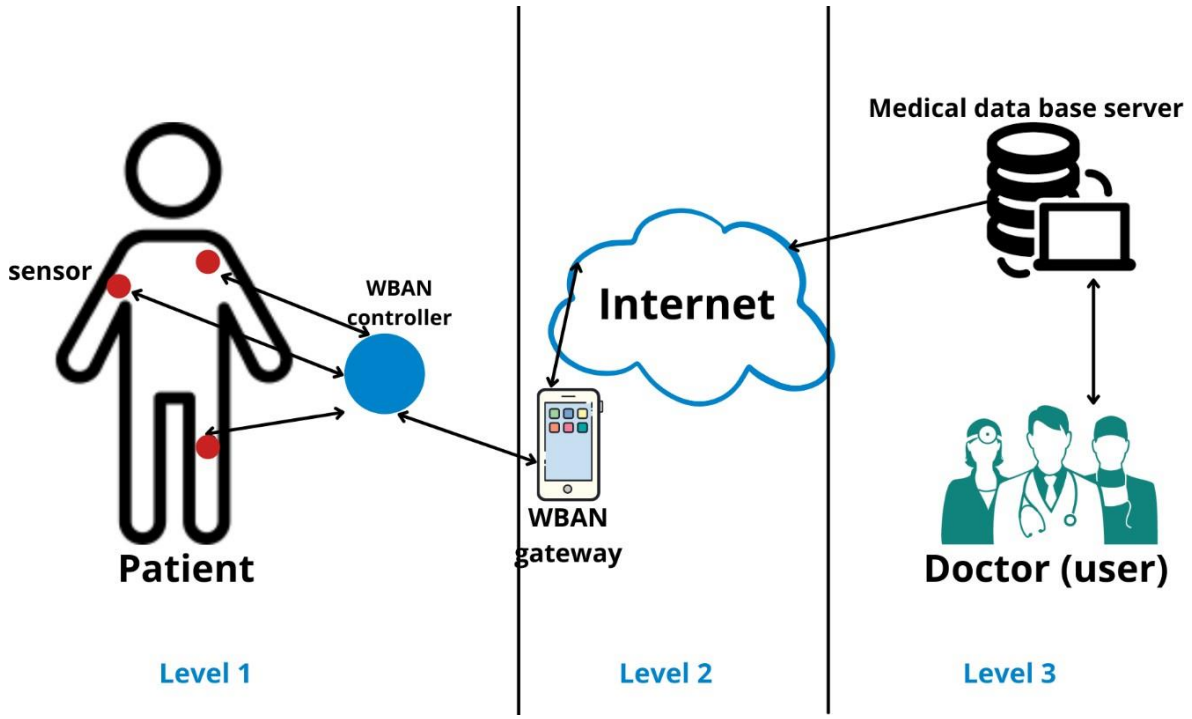

Fig 1.1 The Architecture of Healthcare Monitoring System

According to the studies in [8] most of the WBANs system, the communication design comprised into three separate levels as follows:

Level 1 Intra-WBAN communication: in this level the sensors' interaction is confined within the patient's body, the communication signals inside the region use a gateway (WBAN gateway) to transfer information to the next level.

Level 2 Inter-WBAN communication: this level aims to connect WBANs with other systems or networks so that information may be quickly obtained through various networks. It also bridges the gap between the PS and the user.

Level 3 Beyond-WBAN Communication: in this level a medical environment database is extremely important because it stores the user's medical history and specific profile, also enables retrieval of patient information into an infrastructure that can be ready for appropriate planning.

1.5 Patient's health records

A health record is a written record of a person's medical history. It includes medications, treatments, tests, and notes from visits to a health care provider, (also known as a medical record) [9].

Traditionally, information about patient events and treatments has been kept in paper-based records in order to keep a historical record that can be used for many purposes (further visits, regional or national health indicators, research, etc.). The majority of the collected information in a paper-based system is stored in cabinets grouped by year, patient names, or other organization or classification method that aids in the extraction of the information when needed [1].

This historical paper-based record's details are commonly referred as a patient's health records. Patient health records enabled service delivery with a focus on patient care, in which members of the organization could not only retrieve information but also share it with those in charge of a patient's care [1].

1.5.1 Disadvantage of patient's health records

Although structured paper-based health records provide a method for maintaining relevant information and support in the delivery of health care, it has several downsides:

- Because of the increasing number of forms used to collect information, redundant record keeping, and the loss or misplacement of records, a patient's historical information may become difficult to trace.
- There is no automatic process that could be used to connect or recover relevant information.
- Any collected information may take a significant amount of time to generate.
- The unreadable writing makes patient record hard to understand.
- Misplacement of documents, and also the effect of environmental variables (humidity, temperature, etc.) on the paper, can lead to the destruction of some or all of a patient's historical information.

In contrast, the advancement of health information systems, as well as the introduction of communication and information technology, have enabled the collection, storage, retrieval, and transmission of electronic health information. Electronically produced health records will now capture and digitally store patient information.

1.6 Electronic health records

Professionals have been looking for more efficient systems that provide intuitive access to information they need when they see their patients because as demand to improve medical productivity has increased. The best way to achieve this goal is to keep all information about a patient in electronic files.

Electronic Patient Record is the electronic format of traditional paper-based Patient Records stored on digital devices. In the 1960s, computers were mostly used in hospitals for logistical and financial purposes. It was based on clinical evidence input in order to make clinical decisions and decrease medical errors [10].

The electronic medical record system improves access to patient-specific information and it is a significant contribution to the quality of health care and clinicians' quality of life in practice, clinicians may use emerging communication tools to communicate with their patients in new ways to provide better treatment [11].

1.6.1 EHR in the internet

The Internet provides an attractive infrastructure for effectively communicating health information locally or globally. However, Internet technology aims to optimize information sharing and interoperability, not security. In the field of healthcare, the potential benefits of ubiquitous data communications need to be weighed against personal privacy risks and the risks of data corruption and service interruption [12].

For Internet users who want to access medical information, personal privacy is listed as their top concern [13]. The successful implementation of shared health records must satisfy users' requirements for acceptable levels of security and privacy, and resolve some important legal issues. The Internet gives people the opportunity to access medical information on a global scale, thereby accelerating the transformation of the relationship between patients and clinicians, and sharing decisions Between the patient and the clinician.

1.6.2 EHR characteristics

Information exchange is widely regarded as the key to achieving significant gains in efficiency and higher levels of care quality [11]. As a result, shared electronic health record systems could share certain characteristics and follow a set of specifications, which may serve as the foundation for establishing international standards for electronic health record implementation. that collection of comprehensive and valid scientific medical data through EHR should be:

- Easy to install and maintain with less cost.
- Time-saving for the medical staff who use it in their daily work.
- Able to store all medical information in retrievable format to allow consistency with other systems.
- Able to provide validation of medical data by repeated use of data in patient’s care.

Other benefits of computer-based health records include the ability to integrate information management software and include resources like clinical reminders and warnings, interconnections to knowledge sources for healthcare decision support, and data analysis.

Computer devices today can store a huge amount of data in a limited amount of physical space, using electronic health records, you can easily generate duplicate copies of data for data sharing and other purposes, or you can create backup copies for security reasons. On the other hand, paper records are neither easy nor routinely copied, and may be physically damaged or destroyed by disasters such as fire or flood, or may be lost during transportation.

One of the most important and ideal features of EHR is the function of modifying records and updating information for users. In daily-use health records (paper or electronic), the possibility of entering incorrect information is very high, but it is easier to correct incorrect entries only in the case of computer-based health records.

1.7 Security of healthcare systems

In a healthcare setting, information system privacy and security are critical to creating trust and high-quality services.

In general, computer system security is concerned with the protection and safeguarding of hardware, software, and data, and it usually boils down to three main concepts [14] are : confidentiality, integrity and availability.

The authors identified over twenty security standards based on survey results such as [15]. Due to space constraints, we've compiled a list of the most significant requirements:

- Access control known as the capacity to limit and restrict authorized users' access to resources, it used the three different security and privacy requirements identification, authentication, and authorization.
- The capacity of a system or resource to be accessible, useable, and available on demand by authorized users at any time and from any location within the healthcare system is known as availability, also preventing service disruptions due to hardware problems, power outages, and system upgrades is also part of ensuring availability.
- In an emergency, flexibility allows an unauthorized participant who is not on the permitted list to access certain data in need to save the patient's life.
- Even if there are some risks created by the network dynamic or failure node, dependability ensures that medical data may be retrieved at any moment, in most health conditions, the ability to get precise data is related to network dynamics, which risks the patient's life.

1.8 Conclusion

A health system is a highly complex phenomenon. It is a system whereby the primary purpose is to improve populations' health and well-being. In this chapter we have presented general concepts of this systems, we have seen the architecture of WBANs systems communication, also we have discussed about patient's health record and electronic health record we see the downside and the advantage for each of them. As a result, we see the difference between paper-based system and EHR. In the next chapter we will focus on the security of EHR and how we can make a secure EHR system.

CHAPTER 02

SECURITY OF PATIENT'S EHR

2.1 Introduction

As the health care industry becomes increasingly tech-driven, the privacy and security of data moving through electronic systems becomes important. Securing data ex-change between two systems is a very difficult task, considering a possible intrusion of an attacker on the flow of data. Health data is highly vulnerable to cyber threats and social engineering attacks. In this chapter we review the privacy and security of the current EHR systems and the problems that we face in the security part. As a result, we review an algorithm to implement the concept of cryptography.

2.2 Security and privacy features of current EHR systems

A healthcare security system is developed by applying security safeguards to manage the security vulnerability and risks identified by the organization [16].

A various researches [16] has used the three security-safeguard themes of physical, technological, and administrative in their study. These themes include a variety of security techniques used by healthcare organizations to protect the confidential patient information stored in electronic health records.

2.2.1 The three security-safeguard themes

- **Administrative Safeguard:**

Which includes techniques such as auditing, hiring an information security officer, and making emergency plans [17]. This theme has protections that focus on having security protocols and policies that are compliant.

- **Physical Safeguards:**

Physical security breaches are ranked the second in terms of contributing to security breaches [18] which involves the techniques mentioned under organizational safeguards as well as focusing on physically securing health information so that it is not obtained by unauthorized individuals or others who may damage it [17].

- **Technical Safeguards:**

Which secure the entire information system contained in a health organization's network [17]. Since most security breaches occur via electronic media, such as computers and other transferrable electronic devices, this theme is critical in ensuring the organization's security.

This theme includes security techniques such as firewalls and encryption, virus scanning, and information authentication measures [16]. However, the firewalls and cryptography were the most widely used security techniques.

2.2.2 Security of EHR:

The electronic health records have been secured or protected using cryptography [19]. The use of cryptography has improved the protection of electronic health records during the exchange of health data. The process of exchanging health information has got specifications to be followed through criteria that normally require recording of the exchange procedure to be done by organizations when the encryptions are either enabled or disabled.

The Health Insurance Portability and Accountability Act (HIPAA) designed ways by which cryptography could be used to secure health information and, broadened its standards on security in 2003 when the United States Department of Health and Human Services formed the Concluding Rule [16].

The Concluding Rule enabled HIPAA to expand the organizations' ways of making, receiving, keeping and sending of health information that is protected [16]. Decryption has proven helpful in maintaining the security of patient electronic health records. As patients search their medical records, the use of digital signatures has overcome the issue of violating safe health data.

2.3 Security requirements

There are some basic security requirements for digital medical records that must be implemented in eHealth security systems, which can be summarized into three major aspects as follow [20].

- **Confidentiality:** This ensures that security systems will limit access to medical details to only those who are authorized, in other side it's to keep sensitive information from being shared without permission.
- **Reliability (integrity and authentication):** This ensures that security system can guarantee that the received information has been generated from a trusted source and it has not undergone any modifications.
- **Availability:** This implies that information should be accessible on a regular schedule, which means that ensuring that information is only accessible to those who have been given permission to have it.

2.4 Security issues in EHR

Healthcare services are vulnerable to malware threats or consumers attempting to benefit from them. This reduces the quality of healthcare services or deteriorates their efficiency [21]. Specifically, insulin pump sensors, hospital networks, or the personal health data can be hacked or stolen by malicious users.

In this point we will focus on Attacks at transmission level these assaults may make a few dangers transmission level, for example, spying, adjusting data, interfering with correspondence, sending additional signs to obstruct the base station and systems administration activity.

2.4.1 Several Attacks at transmission level

We depend in this section on two articles [21], [22] to describe a list of attacks that we can find at the transmission level of EHR:

- **Eavesdropping of Patient's Medical Information:**

Monitoring system will record patient's health data from BANs to be transmitted to the healthcare providers. Unprincipled developers can easily build systems with the ability to spy on the patient's data through wireless technology.

- **Man in the Middle Attacks**

The attacker intercepts a communication between the end points and exchange messages between them. The communication is completely controlled by the attacker enable him to read, insert and modify the data in the intercepted communication.

- **Data Tampering Attack**

Where a tampering attacker may damage and replace encrypted data by authorized network nodes.

- **Message Modification Attack**

In this type of attack, the attacker can capture the patient wireless channels and extract the patient medical data to be tampered later, which can mislead the involved users (doctor, nurse, family).

- **Hello Flood Attack**

Where the attacker sends a hello message with a high-powered radio transmission to the network to convince all nodes to choose the attacker for routing their messages. These types of attacks are used to fool the network.

- **Data Interception Attack**

This type of attack can take place through interception the patient's information by the attacker while exchanging them between computers of healthcare system via hospital LAN.

- **Wormhole Attack**

It's a grave attack known as a silent and severe type of attack because it copies the packet at one location and replays them at another location or within the same network without any changes in the content. It aimed to damage the network topology and traffic flow through creating a tunnel between the two attackers to be used for transmitting between them.

- **Others issues**

Several hardware and software issues can cause an interruption in the healthcare system. Hackers may develop new techniques or discover new software vulnerabilities. It is possible also

that the system can be exposed to various types of software attacks such as viruses, worms, Trojans, and spyware attacks.

2.5 EHR access control

People may save huge amounts of information in numerous places because to the interoperability of EHR systems. In many parts of the developed world, healthcare has progressed to the point that people may choose from a variety of providers to meet their various medical requirements, including primary care physicians, specialists, therapists, and even alternative medicine practitioners.

There comes a big problem. Medical misuse and data theft are more likely as a result of information exchange. Patients' personal information, such as their phone number and social security number, is contained in their medical records, which is kept private. Patients may refuse to communicate their diagnosis if it has nothing to do with the conditions for which they are being treated. They just want to provide clinicians with pertinent information.

Access control is a method of ensuring that users are who they claim to be and that they have permission to access customer data, it consists of two main components: authentication and authorization [23].

At a high level, there are two mechanisms of access control RBAC, ABAC as following [24].

RBAC: known as a traditional access control (Rule Based Access Control), Authorities are linked to rules in this model. A suitable role will be assigned to a user when they register for an EHR system. When a user joins a role, they gain the authority of that role. Roles are developed in an organization to execute a variety of tasks. Based on their responsibilities and qualifications, users are allocated to the appropriate role. Users can alter their roles at any time.

ABAC: (Attribute Based Access Control), it's an access that restricted depending on the user's attributes, the resource to be accessed, and the existing environmental conditions.

ABAC mechanisms would enable an acceptable level of access to medical records, even if extraordinary measures were required in an emergency.

2.6 Concept of cryptography

2.6.1 Definition

Cryptography is a security solution that is relatively much safer [25]. The basic idea is to use mathematical methods to transform the original message to a sequence of data that cannot be directly intercepted by a third part. It includes a set of techniques that are frequently used in the computer to ensure the confidentiality, integrity and authenticity of data.

Cryptography is a powerful tool for securely storing and transmitting data [20], but it falls short of meeting all of the requirements listed above. The majority of cryptography techniques in medical information security systems have been presented to fulfill the confidentiality requirements.

It is recommended that the encryption key not be saved on the same server that uses the encryption and decryption algorithms to avoid risking the cryptography technique's security [20].

2.6.2 Classes of cryptographic algorithms:

According to the key, the cryptographic algorithms are known as symmetric or asymmetric.

- **Symmetric cryptography**

Symmetric cryptography is a form of encryption in which the decryption key d is the same as the encryption key e or can be easily derived from it. In most symmetric-key cryptography schemes e equals d. The key is often referred to as a shared key because it is known by both the sender and the recipient of a message [26].

We suppose an example that person A and person B want to communicate with each other, but they do not want an outsider (attacker) to read their messages. They can go to a safe location and talk in person and make sure nobody is in the neighborhood to hear them. However, if both A and B want to communicate over the Internet, they need to use encryption to prevent the attacker from reading their communication. Before they can start sending encrypted messages to each other,

Suppose the attacker wants to read all the communication of A and B, he can intercept all online communication between them, as if he sits in between both of them, and thus he will be able to read the ciphertext. The attacker will not be able to decrypt the ciphertext and read the message if

the algorithm is sufficiently strong, and the key is only known to A and B. The algorithm does not have to be a secret. If designed properly, the security does not depend on the design of the algorithm, it depends on the key. Therefore, A and B should only keep the key secret. In Figure 2.1 we present an example and more explanation of the symmetric cryptosystem

Fig 2.1 Example of symmetric cryptosystem.

We use the following notation to encrypt a message m to get the ciphertext c, and then decrypt the ciphertext to obtain the message again, all using the key k.

$$E_k(m) = c$$

$$D_k(c) = m$$

Here, E and D are the encryption and decryption operation, respectively.

Establishing the shared secret, is one of the disadvantages of symmetric cryptography. When an attacker obtains the key, he is able to decrypt all ciphertexts encrypted with that key. The main issue, however, is obtaining a shared key that only the participants have. A part of the solution to this problem is asymmetric cryptography [26].

- **Asymmetric Cryptography**

In contrast to symmetric cryptography, which uses encryption and decryption keys that are the same or can be easily derived from one another, asymmetric cryptography uses different encryption and decryption keys, making it impossible to compute the decryption key from the

encryption key [26]. These systems have the advantage of allowing the encryption key to be made public. As a result, this system is also referred to as public-key cryptography.

To go back to our example, person B (the receiver) can publish his encryption key, Person A (the sender) can then download the encryption key, or public key of B and encrypt a message. The attacker cannot retrieve the message from the sent ciphertext without the private key of B. However, since the encryption key is public, the attacker can encrypt a message of his own and send it to B. The availability of public keys dismisses the need to establish a shared secret, given that the sender has the public key of the receiver. In Figure 2.2 we present an example and more explanation of the asymmetric cryptosystem

Fig 2.1 Example of asymmetric cryptosystem.

We use the following notation to describe encryption and decryption using asymmetric keys.

$$E_{pk}(m) = c$$

$$D_{sk}(c) = m$$

Here E and D are encryption and decryption, respectively, sk is a private (secret) key, pk is public key, c is the ciphertext and m is the message.

Encrypting and decrypting messages using asymmetric, or public key encryption is much slower than symmetric encryption [26].

As a result, different symmetric and asymmetric encryption algorithms are available to provide security in many digital information applications.

2.7 Attribute-based encryption

2.7.1 Definition

The notion of Attribute-Based Encryption known as new type of IBE by an implementation of their idea of Fuzzy Identity-Based Encryption in 2005 by Sahai and Waters [27] .

Here, each user key is associated with a set of attributes (SE), and each ciphertext is associated with a set of attributes SE0. The prosses of decryption is possible, whenever a user's SE overlaps a ciphertext's SE0 in at least d attributes, where d is a fixed value decided on during system setup, i.e., $|SE \cap SE0| \geq d$.

A property or feature that a subject may have is referred to as an attribute. Any topic may become eligible for a certain attribute at some point in the future, implying that it now possesses the corresponding trait or trait, usually we present the attribute as a string. for example, an attribute called isPatient could be used to describe subjects that are administrators of a certain domain. We denote the set of all attributes used in a specific domain as the universe of attributes.

Attribute-based encryption has two main categories or implementation are KP-ABE and CP-ABE

2.7.2 KP-ABE and PC-ABE:

- **Key-policy attribute-based encryption (KP-ABE):**

Ciphertexts are encrypted with a set of attributes in Key-Policy Attribute-Based Encryption, and each user's secret key is linked to a policy that specifies which ciphertexts he can decrypt as we see in Figure 2.3.

KP-ABE is all about to generate the key depend on a policy which contain a collection of attributes.

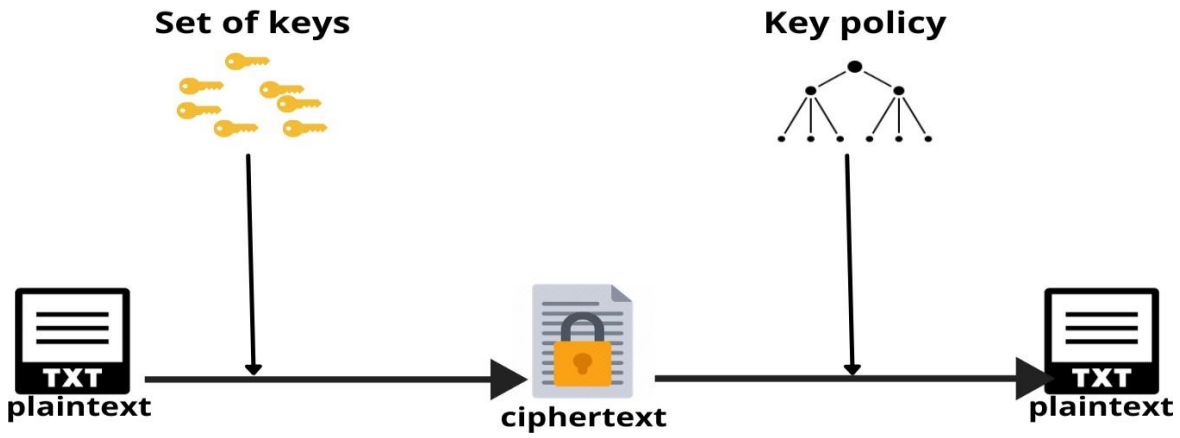

Fig 2.3 Schematic overview of KP-ABE.

❖ **Ciphertext-policy attribute-based encryption (CP-ABE):**

A ciphertext is encrypted using a policy in Ciphertext-Policy Attribute-Based Encryption. The ciphertext can be decrypted by anybody whose attributes fulfill the policy as we see in Figure 2.4. otherwise, the decryption fails. In a nutshell, CP-ABE uses a policy during encryption, whereas KP-ABE uses a policy during decryption. In CP-ABE we use a structure of tree with various keys into order to access given attributes.

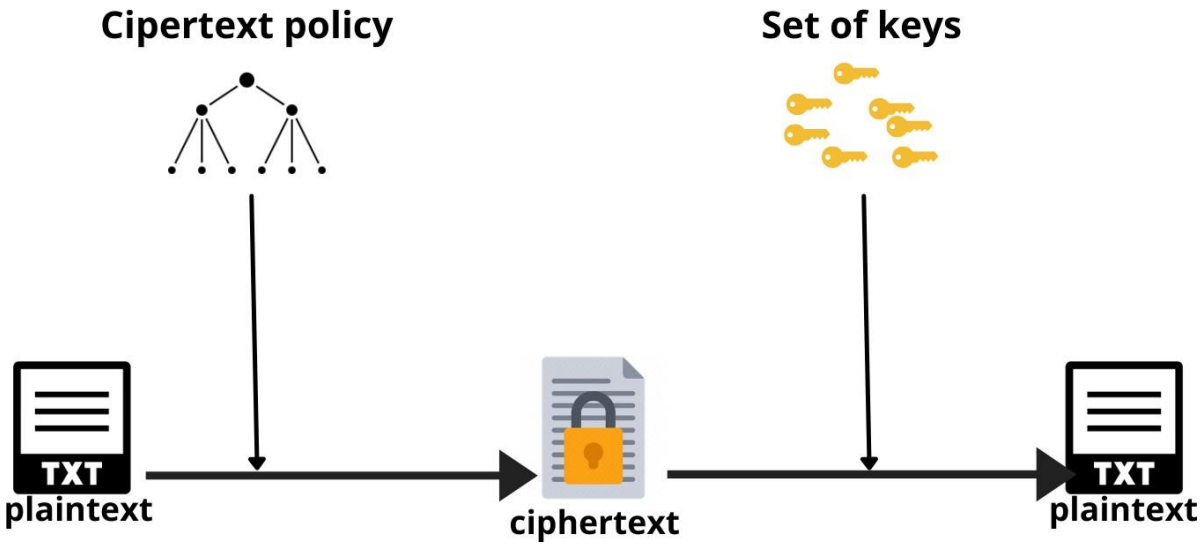

Fig 2.4 Schematic overview of CP-ABE.

The differences between KP-ABE and CP-ABE are summarized in **Table** 2.1

	KP-ABE	CP-ABE
Key	Describes a policy	Describes a set of attributes
Ciphertext	Associated with a set of attributes	Associated with a policy
Trusted Third Party (TTP)	Determines the policy	Determines the attributes
Encryptor	Determines the attributes	Determines the policy

Table 2.1 Differences between KP-ABE and CP-ABE.

In this work we will use the technique KP-ABE in our EHR system for protecting patient data.

2.8 Related works

2.8.1 First work

Description of the work:

This work is a Study on Electronic Health Record and its Implementation by Qian Huang and Qin Yin

In their dissertation, they implement the RBAC model of access control in EHR system.

First and foremost, this study looked into information sharing, often known as interoperability. Technology delays and a lack of finances are now limiting medical information exchange. Standardization and semantic sharing were identified to be the two primary kinds of information sharing.

An attempt is made to construct an EHR system using B/S architecture. The sluggish evolution of the EHR system was discovered during the research phase, even while standards such as HL7 have performed admirably, large-scale implementation remains tough, this is mostly due to the difficult-

to-design systems. Using semantic tools to discover that sharing information is easier than building a new system.

Finally, an EHR system based on B/S architecture was built and implemented based on the previous research. It contains functionalities for information exchange and user access control.

As we mention above, in this study they use RBAC as a technique of security access control of patient's data,

Advantages of the work:

- The system offers a simple and practical structure for future design.
- For building this system, you don't need a lot of money or programmers.
- Medical personnel's workload will be greatly reduced.
- It has the potential to serve as an information exchange platform for the whole city, if not the entire country.
- The system is designed with the patient in consideration. Patients have easy access to their medical information and can permit clinicians to see them. In this system, the patient will become more proactive.

Disadvantages of the work:

- The combination of B/S and C/S systems can be too slow in responding and simple in handle processes.
- These two architectures B/S and C/S can achieve complex processes.
- This system doesn't have a record system for doctors, if the doctor does some changes or updating, the modification should be saved, this can be used as proof in the event of medical misconduct.
- This work doesn't in the security of EHR that much, they just applied the RBAC model and give all the access to the patient.

2.8.2 Second work

Description of the work:

This work is an article of Privacy Preserving Health Record System in Cloud Computing using Attribute based Encryption by Kushal Kulkarni

This article presents an implementation of EHR system with a security technique ABE method, the system is a web site with the users are classified into two security domains called Personal Security Domain and Public Security Domain.

They use Windows Communication Foundation (WCF) which is a framework for building service-oriented applications. Using this framework made them can send data as asynchronous messages from one service endpoint to another.

The ServiceContractAttribute declares that an interface defines a WCF service contract, whereas the OperationContractAttribute specifies which of the interface's methods defines the service contract's operations. WCF refers to a service type as a class that implements the service contract.

Advantages of the work:

- Suggested a new patient-centric platform for secure exchanging personal health records in cloud computing.
- The system supports fine-grained access by using ABE algorithm.
- In this system patients will complete privacy control by encrypting their PHR data files and allowing fine-grained access.
- Using the WCF service improves data security and confidentiality.

2.8.1 Third work:

Description of the work:

- This work is a study of SECURE AND VERIFIABLE ACCESS CONTROL SCHEME FOR BIG DATA STORAGE IN CLOUDS [30], they propose an improved NTRU cryptosystem based on attribute-based encryption and design a secure and verifiable

scheme based on the improved NTRU and secret sharing for big data storage, the suggested system may check shared secret information to avoid cheating and also defend against different assaults such as collusion. They used Asp.net C# as a programming language and SQL server for relational database, and for cryptosystem the used RSA encryption and NTRU decryption with improved way.

Advantages of the work:

- The proposed technique is a secure and verifiable access control scheme to protect the big data stored in a cloud.
- They prove the suggested scheme's correctness and investigate its efficacy and security.
- They provide a comprehensive analysis to show that the system can withstand various assaults such as collusion.
- They offer a novel NTRU decryption process that overcomes the previous NTRU's decryption problems while maintaining NTRU's security strength.

Advantages of the work:

- As multiple users need to mutually verify each other using **multiple RSA operations.**
- The current method should be able to withstand a variety of attacks, including the collusion attack.
- Verification Other people that participated in the discussion confirmed the issue.

2.9 Conclusion

This chapter present the security of EHR, as shown we chose an encryption method for protecting patient's data, also we view some other related works with deferent solutions. The next chapter we will see the implementation of this solution.

CHAPTER 03

PROPOSED TECHNIQUE AND IMPLEMENTATION

3.1 Introduction

In this chapter we review or we will apply the technique that we discus in pervious chapter, the design and implementation of a secure and simple EHR system will be discussed using the solution that we will propose.

3.2 Proposed solution

As mentioned before, our problem is how to secure EHR system and not giving the access to those who are not authorized to the system, we discus that there is tow mechanism to implement the access control RBAC model and ABAC, in this study we are going to work with ABAC by applying ABE algorithm.

As we said in pervious chapter, this algorithm is an encryption method has to type of implementation KP-ABE CP-ABE, and we chose the first technique to use in this study.

A patient should be allowed to choose who has access to his data in a centralized personal health record. The patient can encrypt his data using a CP-ABE technique so that he is the one who decides which doctors have access to it.

3.3 System design

This system is designed based on the previously studies and access control model chosen, it is a desktop application with sharing database, the system based on fine-grained which is achieved by implementing the algorithm of encryption attribute-based encryption.

The system designed to be used only by doctors and patient with limited functions, with sharing database with all the users and the patient's data will be encrypted and accessed only with authorized doctors. So, the data will be decrypted with doctors who has specific attributes such as the doctor who create the EHR, the doctor who consult the patient or if the patient want to see his information.

The architecture of system will be shown on the **Figure** 3.1, as we see we have the doctor (user) want to access to the data (medical data or EHR), in this process the algorithm of encryption executed and give or not give the access to the doctor by sending a key to decrypt the data.

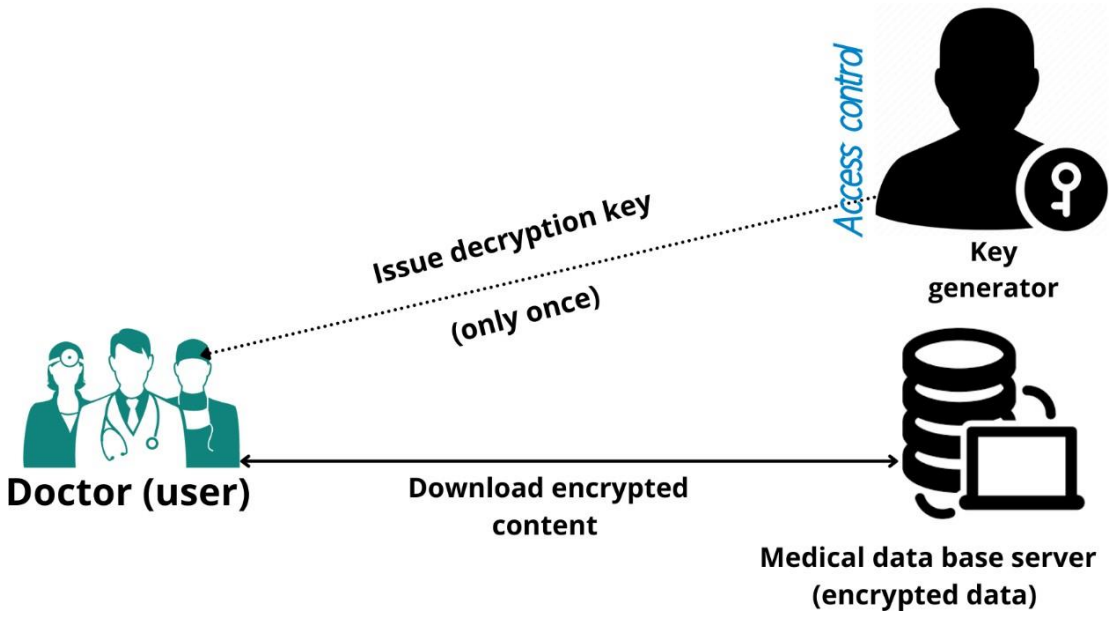

Figure 3.1 Architecture of the system with ABE algorithm

In the doctor's account, there are two possibilities. The first is to look at the doctor's personal information, and the second is to conduct a search. The doctor might choose to update their account password in the personal information section.

After then, the doctor has the option of viewing their patients' records. Similarly, doctors require a medical records search feature due to the large number of patient medical records. Doctors use the same two search techniques as patients when it comes to the search feature.

One is a brand-new patient who has never had a medical record. For him, the doctor must prepare a new medical record.

For the records that doesn’t belong to the doctor (the record didn’t create by the same doctor), it will be encrypted for him.

As the **Figure** 3.3 shown the functions of the user in the system, the admin is just for creating account to the users. It is a simple use case diagram just for showing each user’s function.

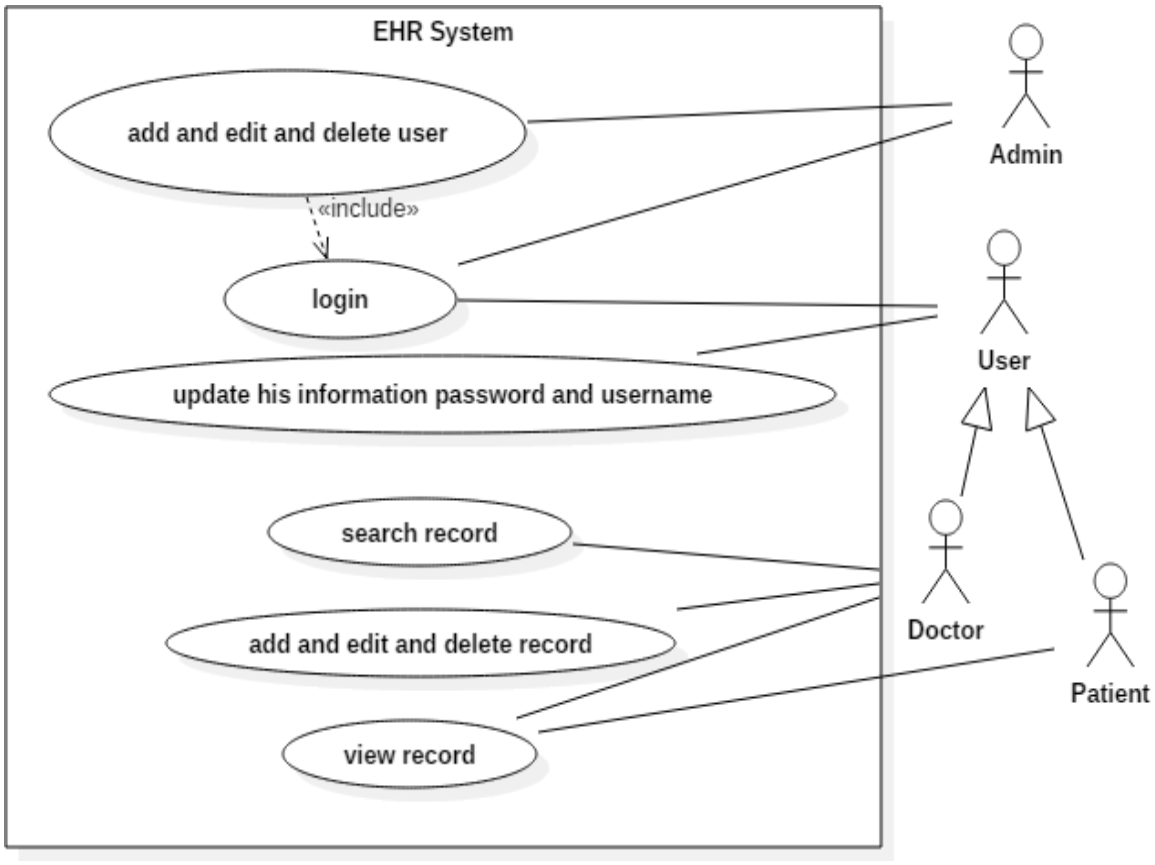

Figure 3.3 Use case diagram.

Database:

The database that shown in **Figure** 3.2 designed by SQL server management studio, it countian only what is important for the system, such as user and patient, doctor, and some other table for managing the system.

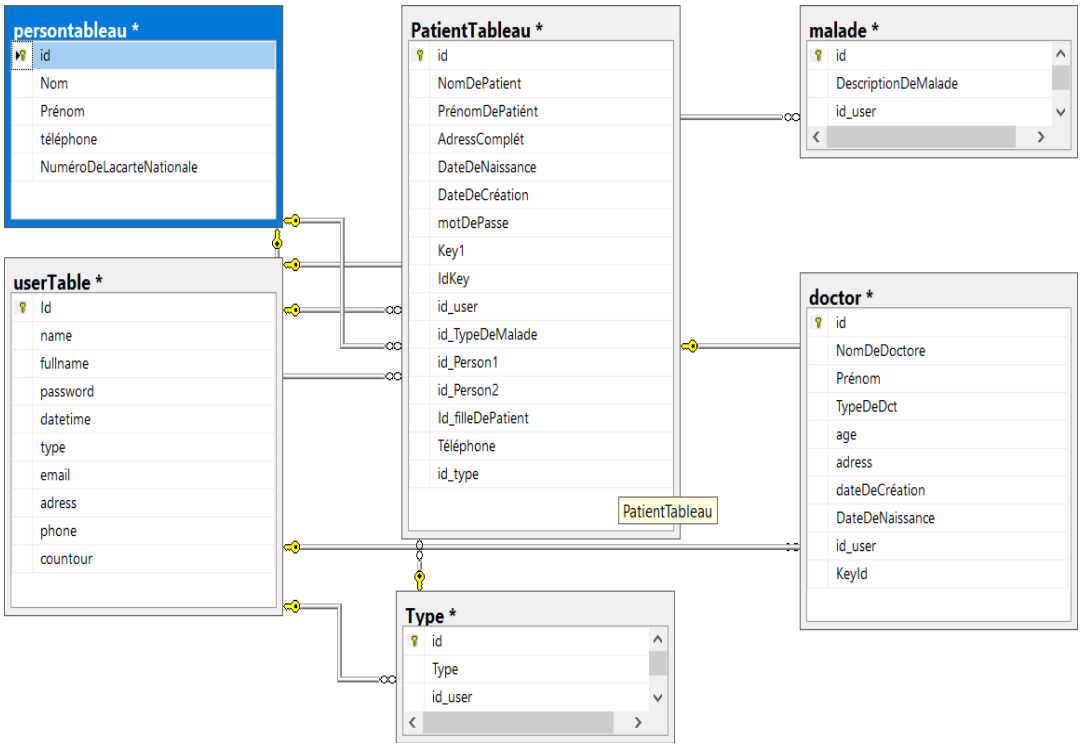

Figure 3.2 Architecture of the database system.

3.4 Tools and technologies used

The tools we used to create a secure EHR system are described in this section. It includes the database, programming language, build software, and database connection tool, among other things. All of the technologies and models were chosen to implement EHR functionalities.

3.4.1 ABAC

It's a security technique that we will depend on it for creation a secure EHR system, (Attribute Based Access Control), it's an access that restricted depending on the user's attributes, the resource to be accessed, and the existing environmental conditions, for applying this mechanism we have to use Attribute-Based Encryption algorithm.

ABE is an encryption algorithm depends on a public-key encryption in which a user's secret key and ciphertext are both determined by attributes, in this study we are going to work with KP-ABE. Using this technique is for encrypt patient data (electronic healthcare record in this case),

and also decrypt it to those who are authorized to see this data such as the doctor who create this record for his patient.

3.4.2 SQL

SQL is an acronym for Structured Query Language, it's a language for interacting with databases. It is the standard language for relational database management systems, according to ANSI (American National Standards Institute).

Databases may be searched, updated, and managed using SQL statements. The SQL language is used by the majority of popular relational database management systems.

3.4.3 SQL server 2014

It's a relational database management system, developed by Microsoft, SQL server 2014 follows the SQL language standard defined by ANSI.

SQL Server 2014 introduced In-Memory OLTP, which allows users to execute OLTP applications against data stored in memory-optimized tables rather than traditional disk-based tables. The In-Memory OLTP engine is built for high concurrency and eliminates locking delays with a novel optimistic concurrency control technique.

Customers may anticipate performance to be up to 20 times higher than SQL Server 2012 when employing this new capability, according to Microsoft.

3.4.4 SSMS 2018

SQL Server Management Studio (SSMS) provides a unified platform for administering SQL infrastructure, ranging from SQL Server to Azure SQL Database. SSMS is a set of tools for configuring, monitoring, and administering SQL Server and database instances, we create the data base by using ssms, also for sharing the data base with deferent users with deferent computers.

3.4.5 Visual studio 2019

Visual Studio is an integrated development environment (IDE) developed by Microsoft. It is used to develop computer programs, such as websites, web apps, web services and mobile apps and for sure desktop apps, visual Studio is a good tool for beginners. Today Visual Studio is most popular and best tools for.

Visual Studio 2019 has been released. This beta release includes numerous changes aimed at improving developer productivity and team collaboration, such as improved search, one-click code cleanup, debugger improvements, and management of pull requests from the IDE.

3.4.6 ADO.NET

ADO.NET is a collection of classes for.NET Framework programmers that offer data access services.it comes with a large number of components for building distributed, data-sharing applications. It's a component of the.NET Framework that allows you to access relational, XML, and application data.

ADO.NET can be used to create front-end database clients and middle-tier business objects that are used by applications, tools, languages, and web browsers.

3.4.7 C#

C# is a multi-paradigm, general-purpose programming language that supports static typing, strong typing, lexically scoped, imperative, declarative, functional, generic, object-oriented, and component-oriented programming.

C# is a modern, general-purpose programming language that can be used to perform a wide range of tasks and objectives that span over a variety of professions. C# is primarily used on the Windows. NET framework, although it can be applied to an open source platform.

3.4.8 DevExpress

DevExpress Universal is a complete software development package for .NET developers. It helps for building applications for Windows, Web, mobile and tablet. DevExpress Universal Subscription includes source code for all WinForms, DevExtreme HTML5 Widgets, ASP.NET, WPF, Dashboard and Windows 10 Apps controls.

3.4.9 Advanced setup

It is a windows installer authoring tool for installing, updating, and configuring your products safely, securely, and reliably, we use this technology for creating a multiple setup for our system.

3.5 Implementation and results

In this section we face a problem of implementing the algorithm of encryption, as a solution we use asymmetric cryptography for encryption with RSA library.

The algorithm that we use is shown in **Figure** 3.4.

```
public static string Cryptage(string c1="",string c2="")
{
    try
    {
        Int64 count = c1.Count();
        string[] xd = new string[count];
        int x = 0;
        for (int i = x; i < count; i++)
        {
            xd[i] = c1.ElementAt(i).ToString();
        }

        for (int i = 0; i < count; i++)
        {
            c2 +=  CréptéLesNuémro(xd[i]) + "";
        }
    }
    catch { }
    return c2;
}
```

Figure 3.4 Encryption method

In the next part when doctor is adding a record the function in the Figure 3.5 is in execution for encrypting the data

```
BaseDeDonner.PatientTableau pt = new BaseDeDonner.PatientTableau();
pt.NomDePatient =master2.Cryprtage.Dct.Numéro_cryptage.Cryptage(fullname.Text) ;
pt.username = master2.Cryprtage.Dct.Numéro_cryptage.Cryptage(username.Text) ;
pt.AdressComplét = master2.Cryprtage.Dct.Numéro_cryptage.Cryptage(adress.Text) ;
pt.DateDeCréation = dt1;
pt.DateDeNaissance = dt2;
pt.id_userForPAtient = us.Id;
pt.motDePasse= master2.Cryprtage.Dct.Numéro_cryptage.Cryptage(password.Text);
try
{
pt.Téléphone = Convert.ToInt32(phone);
}
catch { }
try {
pt.id_user = Properties.Settings.Default.iduser;
}
```

Figure 3.5 Code for encrypt entering data.

Also, we use RSA cryptosystem for encryption and decryption, this library is available in any programming language we used for construct the secret share and reconstruct the secret and RSA is used to verify the users' access legitimacy.

The code below in **Figure** 3.6 shows how we encrypt the data for unauthorized users and decrypt it with authorized users such as the owner the record.

```
4 références
408  public static string CryptWithBiblio(string t1)
409  {
410      RSACryptoServiceProvider csp = new RSACryptoServiceProvider(2048);
411      csp.ImportParameters(publicKey);
412      byte[] cl = Encoding.Unicode.GetBytes(t1);
413      byte[] cls = csp.Encrypt(cl,false) ;
414     return  Convert.ToBase64String(cls);
415  }
```

Figure 3.6 Encryption method with RSA.

```
417  public static string DecCryptWithBiblio(RichTextBox t1)
418  {
419      RSACryptoServiceProvider csp = new RSACryptoServiceProvider(2048);
420      csp.ImportParameters(privateKey);
421      byte[] cl = Convert.FromBase64String(t1.Text);
422      byte[] cls = csp.Decrypt(cl, false);
423      return Encoding.Unicode.GetString(cls);
424  }
425
```

Figure 3.7 Decryption method with RSA.

Login section:

Users must first log in before using the system. On the login screen, as usually he must enter in your username and password, as we see in **Figure** 3.4

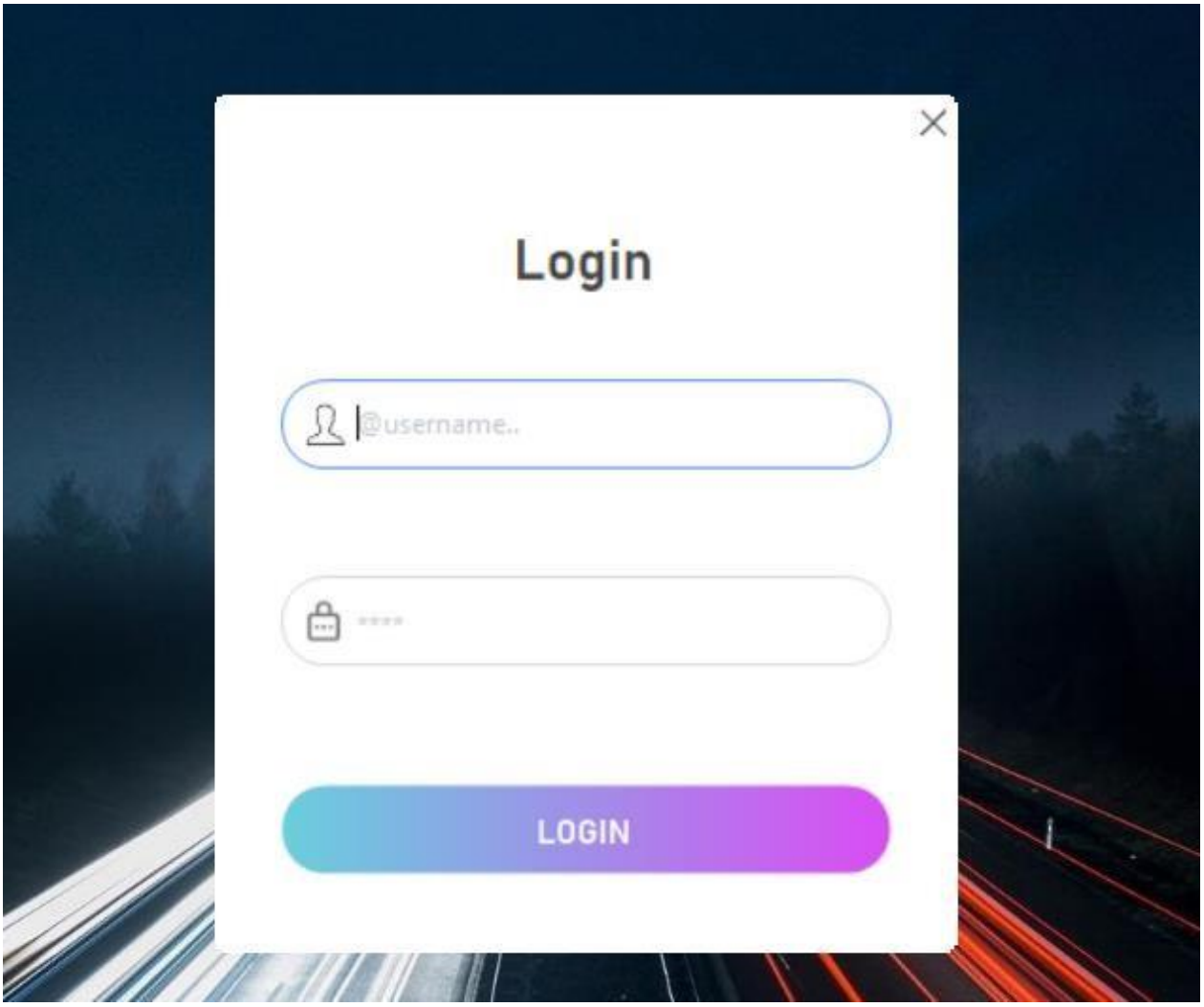

Figure 3.8 Login page

Principal page:

After the user login, the principal page shows on in screen **Figure** 3.5, it includes the list of the patient and their information (EHR) and list of the users and their information.

In section of user's information, the user could update their password and username as we see in **Figure** 3.6.

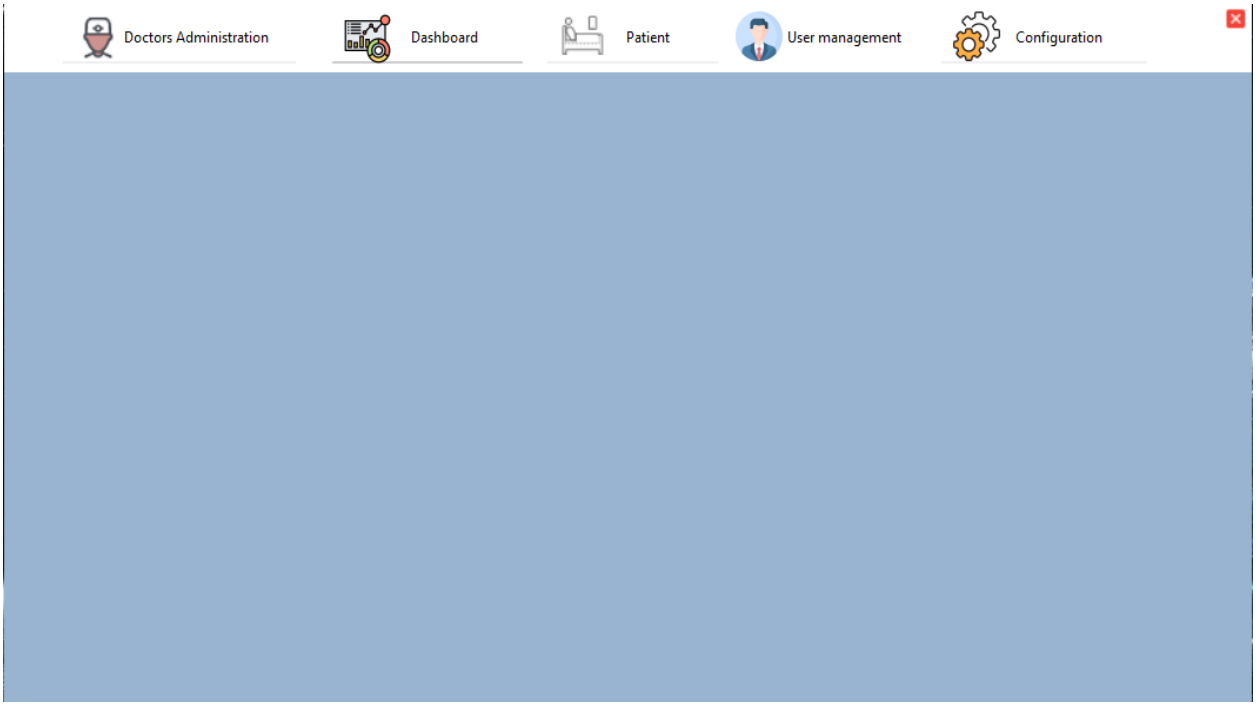

Figure 3.9 The principal page

In section of user's information, the user could update their password and username as we see in **Figure** 3.6.

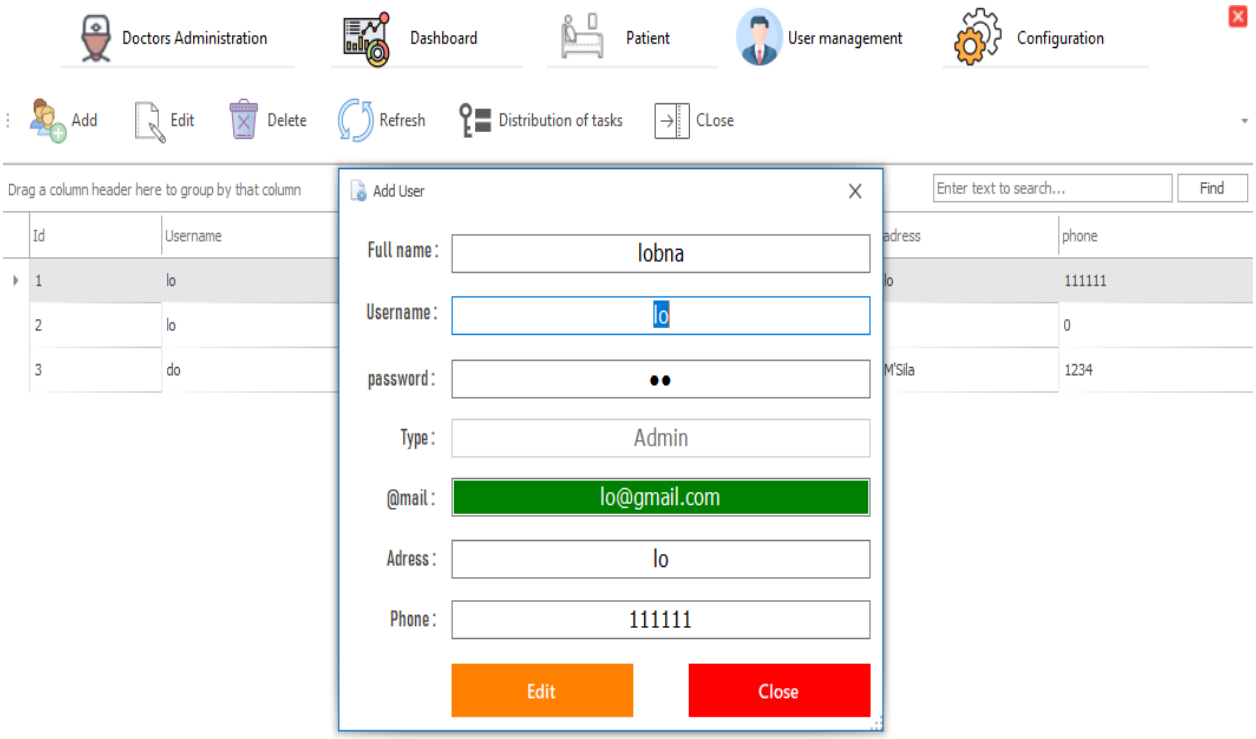

Figure 3.10 Show user's information

If the user wants to see the list of the patients and their information, there is tow possibilities can happen:

Case1: a new user (doctor) he didn't create any EHR in the system, here all the data are encrypted for him and he can't see the list of the patient as we see in **Figure** 3.7

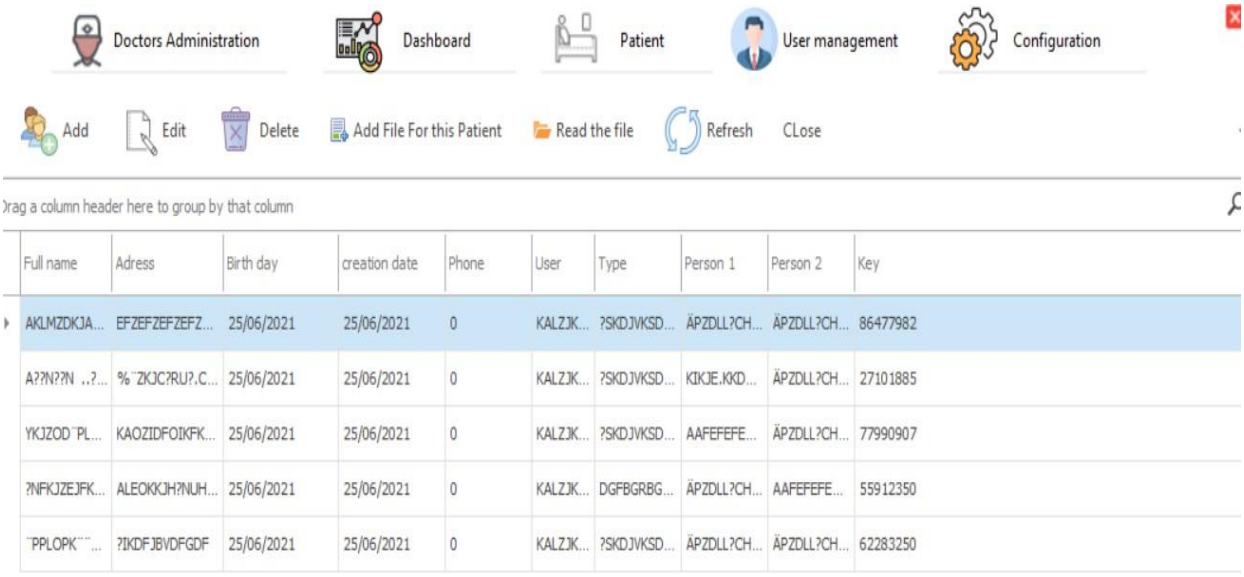

Figure 3.11 Encrypted database.

Case2: if the user (patient) wants to see his information or his medical record

In this case all the data will be encrypted he could see only his record, as shown in **Figure** 3.8.

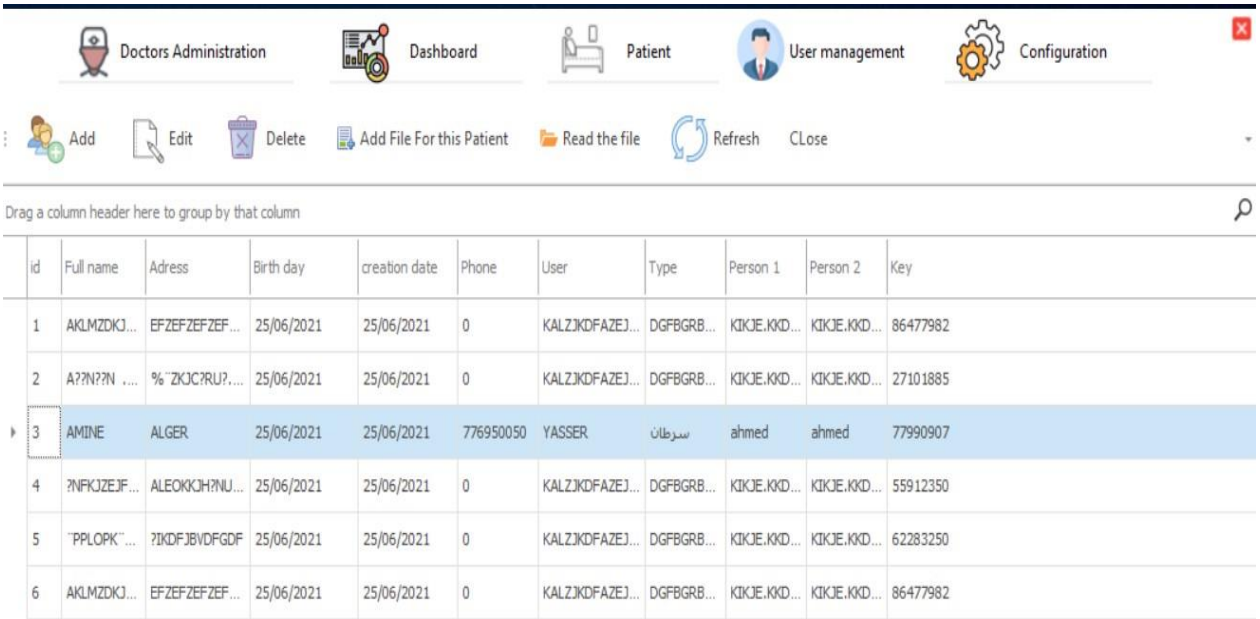

Figure 3.12 Shown record only to the owner.

3.5.1 Discussion

In this section we will discuss the obtained results, as we saw in pervious section the result that we expect is shown in **Figure 3.11** and **Figure 3.12** encrypted data with deferent users, we show two cases for the implementation of attribute-based encryption with tow users in deferent type (patient and doctor).

Case1: depend on the id and the attributes of the user the algorithm attribute-based encryption detects if this user has the access to records (database) or not in this case he is unauthorized to access. So, the algorithm encrypts all the data and he can't see any of it.

Case2: depend on the id and the attribute of the user the algorithm attribute-based encryption detects that this user is authorized to access to only his data so the algorithm decrypts his data and shows the other data encrypted.

We expect from future works to improve this technique and this system, we suggest to work in cloud computing with this technique will be more efficient.

3.6 Conclusion

In this chapter, we create a secure EHR system by implementing a security technique which is ABAC with the algorithm ABE, the system was a desktop app with a shared database by multiple users, for creating this system we use C# as a programming language and SQL for relational database and the framework ADO.NET for build the structure of the system. The result shows that the patient's data are all encrypted with unauthorized users.

GENERAL CONCLUSION

In healthcare application, patient's data are more sensitive and its known as EHR electronic healthcare records, it contains personal information about the patient, medical history, physical examination, medication use history, immunization status, and even some sound and visual data. So, the patient may not be comfortable to share his information with others, and he has all the right to determine whom he gives access to his data.

So, the objective is to build an EHR system with a security perspective to protect patient data from a verity of attacks and to respect the privacy of patient.

In this study we have focused in security and privacy of patient's EHR, by encrypting their EHR data files to allow fine-grained access, he has ultimate control over their privacy; and to achieve that we have studied the EHR access control, we mentioned that there is two access control models RBAC and ABAC, we have also studied the cryptography (symmetric and asymmetric) for do the encryption to the EHR data, we have used ABE algorithm to encrypt the data for achieve fine-grained.

We have used C# programming language for build a desktop application for EHR management, and for protect patient's data we implemented the ABE algorithm for encrypting data, we have used multiple technologies and tools for achieve our objective.

As a result, in the section of implementation we faced a problem in the encryption method, we solved it by using asymmetric cryptography, and in the end all patient's data are encrypted and it's only seen by those who authorized to access them. As a prospect, we will continue to improve our work, it will be better to work in the cloud, it could much easier if we work with another programming language that includes libraries and frameworks in line with the requirement and with the algorithm attribute-based encryption.

BIBLIOGRAPHY

[1] A. Flores, “Secure exchange of information in electronic health records,” 2010.

[2] M. G. Field, “The concept of the ‘health system’ at the macrosociological level,” *Soc. Sci. Med.*, vol. 7, no. 10, pp. 763–785, Oct. 1973, doi: 10.1016/0037-7856(73)90118-2.

[3] H. Tunstall-Pedoe, “Preventing Chronic Diseases. A Vital Investment: WHO Global Report. Geneva: World Health Organization, 2005. pp 200. CHF 30.00. ISBN 92 4 1563001. Also published on http://www. who. int/chp/chronic_disease_report/en.” Oxford University Press, 2006.

[4] C. Carmona, M. Raynor, and M. P. Kelly, “Health systems and health-related behaviour change: a review of primary and secondary evidence,” 2010. Accessed: May 18, 2021. [Online]. Available: https://www.researchgate.net/publication/313106281.

[5] W. H. Organization, *The world health report 2000: health systems: improving performance*. World Health Organization, 2000.

[6] “The History of Healthcare Technology and the Evolution of EHR.” https://www.vertitechit.com/history-healthcare-technology/ (accessed Jun. 13, 2021).

[7] “Wireless Body Area Networks (WBAN) | WAVES.” https://www.waves.intec.ugent.be/research/wireless-body-area-networks (accessed May 19, 2021).

[8] “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications | Elsevier Enhanced Reader.” https://reader.elsevier.com/reader/sd/pii/S1110866516300482?token=0A3D576322DCCDE5ADC43D8C05EB01FF46280D07986FFD41620951BFD88FEB0CEC8D0EAF139154AFA1A3820EBBE17F68&originRegion=eu-west-1&originCreation=20210519070628 (accessed May 19, 2021).

[9] “ONC | Office of the National Coordinator for Health Information Technology.” https://www.healthit.gov/ (accessed May 18, 2021).

[10] R. S. Evans, “Electronic Health Records: Then, Now, and in the Future,” *Yearb. Med.*

Inform., no. Suppl 1, pp. S48–S61, May 2016, doi: 10.15265/IYS-2016-s006.

[11] Y. M. Mohammad, "Information security strategy in telemedicine and e-health systems: a case study of england's shared electronic health record system," *PQDT - UK Irel.*, no. October, p. 1, 2010, [Online]. Available: https://login.pallas2.tcl.sc.edu/login?url=https://search.proquest.com/docview/1314565609?accountid=13965%0Ahttp://resolver.ebscohost.com/openurl?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQuest+Dissertations+%26+Theses+Global&rft_v.

[12] D. B. Baker and D. R. Masys, "PCASSO: A design for secure communication of personal health information via the internet," *Int. J. Med. Inform.*, vol. 54, no. 2, pp. 97–104, 1999, doi: 10.1016/S1386-5056(98)00088-4.

[13] K. Winker, "Obtaining, preserving, and preparing bird specimens," *J. F. Ornithol.*, vol. 71, no. 2, pp. 250–297, 2000.

[14] B. Matt, *Introduction to Computer Security*. 2005.

[15] G. Drosatos, P. S. Efraimidis, G. Williams, and E. Kaldoudi, "Towards privacy by design in personal e-health systems," in *HEALTHINF 2016 - 9th International Conference on Health Informatics, Proceedings; Part of 9th International Joint Conference on Biomedical Engineering Systems and Technologies, BIOSTEC 2016*, 2016, pp. 472–477, doi: 10.5220/0005821404720477.

[16] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egypt. Informatics J.*, no. xxxx, 2020, doi: 10.1016/j.eij.2020.07.003.

[17] S. B. Wikina, "What caused the breach? An examination of use of information technology and health data breaches.," *undefined*, 2014.

[18] "Data Breaches of Protected Health Information in the United States," 2015. Accessed: May 19, 2021. [Online]. Available: https://jamanetwork.com/.

[19] C. J. Wang and D. J. Huang, "The HIPAA conundrum in the era of mobile health and communications," *JAMA*, vol. 310, no. 11, pp. 1121–1122, 2013.

[20] R. Thabit, "Review of Cryptography Applications in eHealth Security Systems," *Int. J. Sci. Eng. Investig.*, vol. 8, no. 89, pp. 110–116, 2019, [Online]. Available: http://www.ijsei.com/papers/ijsei-88919-16.pdf.

[21] M. E. G. Kavita and A. P. K. Bala, "Security and Privacy Issues in EHR Systems Towards Trusted Services," vol. 4, no. 5, 2018.

[22] K. Habib, A. Torjusen, and W. Leister, "Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth," *Researchgate.Net*, no. c, pp. 73–78, 2015, [Online]. Available: https://www.researchgate.net/profile/Wolfgang_Leister/publication/320596844_Security_Analysis_of_a_Patient_Monitoring_System_for_the_Internet_of_Things_in_eHealth/links/59efaa13458515c3cc4369d0/Security-Analysis-of-a-Patient-Monitoring-System-for-the-Inte.

[23] "What is Access Control?" https://searchsecurity.techtarget.com/definition/access-control (accessed Jun. 08, 2021).

[24] W. Stallings *et al.*, *Computer SeCurity PrinciPles and Practice Third Edition*. 2015.

[25] D. Université *et al.*, "Thèse de doctorat Thèse de doctorat," no. Paris VI, 2006.

[26] E. Lastdrager, "Securing Patient Information in Medical Databases," no. August, p. 81, 2011, [Online]. Available: https://essay.utwente.nl/61035/1/MSc_E_Lastdrager_DIES_CTIT.pdf.

[27] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Lecture Notes in Computer Science*, 2005, vol. 3494, pp. 457–473, doi: 10.1007/11426639_27.

[28] E. Chen and E. Chen, "Master Thesis Study on Electronic Health Record and its Implementation," 2012.

[29] K. P. Kulkarni, "Privacy Preserving Health Record System in Cloud Computing using Attribute based Encryption," vol. 122, no. 18, pp. 6–11, 2015.

[30] "SECURE AND VERIFIABLE ACCESS CONTROL SCHEME FOR BIG DATA STORAGE IN CLOUDS." http://1croreprojects.com/blog/SECURE-AND-

VERIFIABLE-ACCESS-CONTROL-SCHEME-FOR-BIG-DATA-STORAGE-IN-CLOUDS.php (accessed Jun. 29, 2021).

Abstract

In healthcare applications, patient's data and his medical data are stored in database, some of this data is sensitive and it should have limited authorized persons, it's accessed only by authorized people. The main aim of this work is to propose an improved security technique to ensure the confidentiality of the electronic health records (EHR). We used Attribute-Based Encryption for achieve our goal to protect the confidentiality and the privacy of the patient's data. The system that we build has been implemented depending on the proposed solution and as we reviewed in the results that the Attribute-Based Encryption has solved our problem.

Keywords: database, encryption algorithm, EHR, healthcare.

Résumé

Dans les applications de soins de santé, les données du patient et ses données médicales sont stockées dans une base de données, certaines de ces données sont sensibles et devraient avoir des personnes autorisées limitées, elles sont accessibles uniquement par des personnes autorisées.
L'objectif principal de ce travail est de proposer une technique de sécurité améliorée pour assurer la confidentialité des dossiers de santé électroniques (DSE. Nous utilisons Attribute-Based Encryption pour atteindre notre objectif de protéger la confidentialité des données du patient. Le système que nous avons construit a été mis en œuvre en fonction de la solution proposée et comme nous l'avons examiné dans les résultats, Attribute-Based Encryption a résolu notre problème.

Mots-clés : base de données, algorithme de cryptage, DSE, soins de santé.

ملخص

في تطبيقات الرعاية الصحية ، يتم تخزين بيانات المريض وبياناته الطبية في قاعدة بيانات ، وبعض هذه البيانات حساسة ويجب أن يكون لها عدد محدود من الأشخاص المصرح لهم ، ولا يتم الوصول إليها إلا من قبل الأشخاص المصرح لهم. الهدف الرئيسي من هذا العمل هو اقتراح تقنية أمان محسّنة لضمان سرية السجلات الصحية الإلكترونية (EHR). لقد قمنا باستخدام Attribute-Based Encryptionمن أجل تحقيق هدفنا و حماية سرية وخصوصية بيانات المريض. النظام الذي قمنا ببنائه تم تنفيذه اعتمادا على الحل المقترح، وكما أظهرت النتائج أن Attribute-Based Encryption قد قام بمعالجة مشكلتنا.

الكلمات المفتاحية: قاعدة البيانات ، خوارزمية التشفير ، السجلات الصحية الإلكترونية ، الرعاية الصحية.