

Kurdistan Region Government/Iraq
Presidency of the Council of Ministers
Ministry of Higher Education & Scientific Research
Erbil Polytechnic University Technical Engineering
College Information System Engineering Department



A Robust and Secure Access Scheme for Cloud Based E-Healthcare Services

A Thesis

Submitted to the Council of the College of Technical Engineering at Erbil
Polytechnic University in Partial Fulfillment of the Requirements for the
Degree of Master of Information Systems Engineering

By

Glena Aziz Qadir

B.Sc. Information Systems Engineering

Supervised by

Assist. Prof. Dr. Bzar Khidir Hussan

Erbil- Kurdistan Region

May 2023

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ

(وَقُلْ رَبِّ زِدْنِيْ عِلْمًا)

سورة طه - آية 114

Declaration

I declare that the Master Thesis entitled: “A robust and secure access scheme for cloud-based E-healthcare services” is my own original work, and hereby I certify that unless stated, all work contained within this thesis is my own independent research and has not been submitted for the award of any other degree at any institution, except where due acknowledgment is made in the text.

Signature:

Student Name: **Glena Aziz Qadir**

Date: 13/4/2023

Linguistic Review

I can affirm that I have carefully reviewed the thesis titled “A robust and secure access scheme for cloud-based E-healthcare services” Also, from an English linguistic point of view, I can fully approve that this thesis is free of both grammatical and spelling mistakes.

Signature:

Name: **Assist. Prof. Dr. AbdulKhalik Muhammad Qadir**

Date: 10/02/2023

Supervisor Certificate

This thesis has been written under my supervision and has been submitted for the award of the degree of Master of Information System Engineering with my approval as supervisor.

Signature:

Name: **Assist. Prof. Dr. Bzar Khidir Hussan**

Date: / /2023

I confirm that all requirements have been fulfilled.

Signature:

Name: **Dr. Roojwan Sc. Hawezi**

Head of the Department of Information System Engineering

Date: / /2023

I confirm that all requirements have been fulfilled.

Postgraduate Office

Signature:

Name:

Date: / /2023

Examining Committee Certification

We certify that we have read this thesis: “A robust and secure access scheme for cloud-based E-healthcare services” and as an examining committee examined the student (**Glena Aziz Qadr**) in its content and what related to it. We approve that it meets the standards of a thesis for the degree of Master in Information System Engineering.

Signature:

Name: **Assist. Dr. Shavan Kamal**

Member

Date: / /2023

Signature:

Name: **Assist. Dr. Kamaran HamaAli**

Member

Date: / /2023

Signature:

Name: **Assist. Prof. Dr. Bzar Khidir**

Supervisor

Date: / /202

Signature

Name: **prof. Dr. Subhi Rafiq**

Chairman

Date: / /2023

Approved by:

Dean of the College of Erbil Technical Engineering

Signature:

Name: **Prof. Dr. Ayad Zaki Saber**

Date: / /2023

Dedication

I dedicate this thesis to Allah Almighty my creator, my strong pillar, my source of inspiration, wisdom, knowledge and understanding and has been the source of my strength throughout my life. I also dedicate this thesis to my sincere parent that have never left my side.

A special feeling of gratitude to my loving husband whose words of encouragement and push for tenacity always ring in my ears.

For all friends who never lost hope in me and always believed in me. Hoping that this work will be a good work for all the fellow scholars and researchers.

Acknowledgements

In the name of Allah, the Merciful and the Compassionate. I am grateful to Almighty Allah for supporting us in order to complete this thesis.

I would like to extend my deepest gratitude and appreciation to my parent for their unwavering support and love throughout my studying.

I would like to gratitude to husband for his unwavering support throughout the journey of completing my thesis. His presence by my side has been a source of immense strength and encouragement. He has always been patient and understanding during the long hours I spent researching, writing, and studying.

I am grateful to Assist. Prof. Dr. Bzar Khidir Hussan for being the advisor for us during the completion of this research work requirement in all fields. His ideas and inspirations have helped me make this idea of mine into a fully-fledged project. Without, I may never had tried research works.

Again, I am thankful to my batch-mates for supporting me at times of my implementation part. I am also grateful to all the professors in my department for always being a constant source of inspiration and motivation during the entire course of the project.

We are also grateful to those people who have contributed in the completion of this work.

Abstract

E-healthcare is a digital version of a patient's medical history, which includes information about their medical conditions, treatments, and medications. E-healthcare is typically used by healthcare providers to improve the quality of patient care. E-healthcare systems are essential tools that contain sensitive patient information and are subject to strict privacy and security regulations. Since the rise of the cloud computing many healthcare providers are now storing their E-healthcare data on cloud-based systems. Transferring E-healthcare data to the cloud computing can introduce a variety of security challenges that must be carefully considered and managed. One of the main security concerns when moving E-healthcare data to the cloud computing is the risk of unauthorized access to patient information. The access control is a critical component of E-healthcare systems, and ensuring secure and appropriate access to patient data is essential for protecting security. Also, privacy is maintained for the integrity of the healthcare system by encrypting data when storing it in the cloud. The access control allows only authorized users to access E-health data. In healthcare, timely access to patient data is critical for effective care delivery. Time delays in accessing data can lead to serious consequences for patient care that including delayed diagnosis and inappropriate treatment. For this reason, the time delay of user access is decreased using the proposed algorithms.

In this thesis, the Generate Access Key (GAK) algorithm is proposed based on Message Authentication Code (MAC) and Hashing technique to produce a Security Secret Key (SSK). The GAK would work by providing users with a unique SSK that would be used to allow them to access data in the E-healthcare based cloud system with the minimum of delay. Users are also given flexible access rights based on their role and rights according to User Access Rights (UAR) algorithm. In order to protect the privacy of users, the

data is encrypted using the Database Encryption (DBE) algorithm before being stored in the database and to read by the users the data in the system must be decrypted based on the Database Decryption (DBD) algorithm. The simulation results of our algorithms show that the delay for authenticating two hundred users is 440 milliseconds, and the data response time is 150 milliseconds for 200 participants requesting data simultaneously. The computational cost was compared with other related works and found that in our algorithm, 0.035 milliseconds were needed for all the registration, login, and authentication stages.

Table of Contents

Declaration	III
Supervisor Certificate.....	V
Examining Committee Certification	VI
Dedication	VII
Acknowledgements	VIII
Abstract	IX
Table of Contents	XI
List of Figures	XIV
List of Tables.....	XV
List of Algorithms	XVI
List of Abbreviations.....	XVII
CHAPTER ONE: INTRODUCTION	1
1.1 Introduction	1
1.2 Problem Statement	2
1.3 The Aims of Thesis	3
1.4 Thesis Objectives	3
1.5 Thesis Contribution.....	4
1.6 Outline of The Thesis.....	4
CHAPTER TWO: BACKGROUND THEORY and LITERATURE	
REVIEWS	6
2.1 Introduction	6
2.2 E-healthcare.....	8
2.3 Cloud Computing	10

2.4 Cloud Computing for Healthcare Sectors	10
2.4.1 Cloud based E-healthcare Service Models	11
2.4.2 Cloud based E-healthcare Delivery Models	12
2.5 E-Healthcare Cloud Computing Benefits	14
2.6 Privacy and Security in E-healthcare Cloud	15
2.7 Common E-healthcare Security and Privacy Issues	16
2.8 Classification of Security Solutions in E-Healthcare Systems	17
2.8.1 Access Control.....	17
2.8.2 Cryptography	18
2.9 Methods to Encrypt Health Data.....	20
2.10 Literature Reviews	21
CHAPTER THREE: THESIS METHODOLOGY	25
3.1 Introduction	25
3.2 Proposed System Model.....	25
3.2.1 Registration Phase	28
3.2.2 Login and Authentication Phase.....	28
3.3 Time Execution	31
3.4 Proposed System Members	32
3.5 Security System Database	34
CHAPTER FOUR: EXPERIMENTAL RESULTS AND DISCUSSION	37
4.1 Introduction	37
4.2 Mechanism of E-Healthcare Design	37
4.2.1 Webpage Design.....	37
4.2.2 Webpage Effects.....	38

4.2.3 Data Processing	38
4.2.4 Saving and Retrieving	39
4.3 Implementation of the proposed algorithm.....	39
4.4 Experimental Results and Analysis	48
4.4.1 Simulation Environment	48
4.4.2 Performance Evaluation.....	49
4.5 Comparison with other works	53
CHAPTER FIVE: CONCLUSION AND FUTURE WORKS	55
5.1 Introduction	55
5.2 Conclusion.....	55
5.3 Future Works.....	56

List of Figures

Fig. 2. 1 general structure of E-healthcare based cloud.....	11
Fig. 2. 2 Cloud based E-healthcare Service Models	12
Fig. 2. 3 Hybrid cloud-based E-Healthcare.....	14
Fig. 3. 1 designed system model.....	26
Fig. 3. 2 Flowchart of proposed system model.....	27
Fig. 3. 3 Login and Authentication phase.....	29
Fig. 4. 1 Registration page.....	40
Fig. 4. 2 Verifying the identity of users before they register.....	41
Fig. 4. 3 Login page.....	41
Fig. 4. 4 The sent SSK via E-mail.....	42
Fig. 4. 5 Verifying the identity of users before they register	42
Fig. 4. 6 User roles.....	43
Fig. 4. 7 Arrangement of today appointment.....	43
Fig. 4.8 Current day appointment.....	44
Fig. 4.9 Adding new patient.....	45
Fig. 4.10 Doctor view patient data.....	45
Fig. 4.11 laboratory view a patient's test requests.....	46
Fig. 4.12 drug request by doctor.....	47
Fig. 4.13 Patient took the drugs.....	47
Fig. 4.14 Encrypted data in the database.....	48
Fig. 4.15 Authentication phase (2).....	51
Fig. 4. 16: Data response time.....	53
Fig. 4.17: Computation time Cost Comparison.....	54

List of Tables

Table 2.1 Summaries of literature reviews	23
Table 4. 1 Specifications of the used cloud.....	39
Table 4. 2 specification of the system.....	49
Table 4.3 The authentication phase.....	49
Table 4. 4: Data response time.....	52
Table 4. 5 Comparison of computational time costs with other related works	53

List of Algorithms

Algorithm 1: Generate Access Key (GAK)	30
Algorithm 2: User Access Rights (UAR)	32
Algorithm 3: Database Encryption (DBE).....	34
Algorithm 4: Database Decryption (DBD)	35

List of Abbreviations

Abbreviation	Acronyms
ABAC	Attribute-based Access Control
ABE	Attribute-Based Encryption
AC-AC	data Access Control for Acute Care teams
BLAC	Bilayer Access Control
CP-ABE	Ciphertext Policy Attribute based Encryption
CS	Cloud Server
CSPs	The Cloud Service Providers
CSS	Cascading Style Sheets
DBD	Database Decryption
DBE	Database Encryption
ECC	Elliptic Curve based Cryptographic
E-Healthcare	electronic healthcare
EMR	Electronic Medical Record
GAK	Generate Access Key
H	crypto hash function
HER	Electronic Health Record
HIE	Health Information Exchange
HTML	Hypertext Markup Language
IaaS	infrastructure as a service
IBE	Identity-Based Encryption
ICT	Information and Communication Technology
IDU	Identification Number of User
IoT	Internet of Things
IT	Information Technology

LACO	Lightweight Authentication and Ownership Transfer Protocol
LPAC	Lightweight and Privacy Aware Fine-grained Access Control
MAC	Message Authentication Code
N	Random number generated by the user
OS	Operating System
PaaS	platform as a service
PHP	Hypertext Preprocessor
PHR	Personal Health Record
P_{ID}	Identification Number of P_{user}
PKE	Public Key Encryption
PKI	Public Key Infrastructure
P_{PW}	Password of P_{user}
P_{user}	Patient in the system
PWU	Password of User
SaaS	software as a service
SE	Searchable Encryption
SKE	Symmetric Key Encryption
SSE	Searchable Symmetric Access
SSK	Security Secret Key
UAR	User Access Rights
WBAC	Work-based Access Control
WHO	The World Health Organization
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language
Z	Integer number

CHAPTER ONE: INTRODUCTION

1.1 Introduction

The development made in Information and Communication Technology (ICT) has had a significant impact on all sectors across the globe, and one of its most significant innovations in the healthcare sector is the development of Electronic Healthcare (E-healthcare) through the use of Information Technology (IT) (Kim et al., 2019). E-healthcare is a digital version of a patient's medical history, which includes information about their health status, medical conditions, treatments, and medications. E-healthcare is typically used by healthcare providers to improve the quality of patient care. E-healthcare systems are essential tools that contain sensitive patient information and are subject to strict privacy and security regulations. With the rise of the cloud, many healthcare providers are now storing their E-healthcare data on cloud-based systems. Transferring E-healthcare data to the cloud can introduce a variety of security challenges that must be carefully considered and managed. One of the main security concerns when moving E-healthcare data to the cloud is the risk of unauthorized access to patient information (Abdulmalik et al., 2023, Alzahrani et al., 2020). The access control is a critical component of E-healthcare systems, and ensuring secure and appropriate access to patient data is essential for protecting security. Also, privacy is maintained for the integrity of the healthcare system by encrypting data when storing it in the cloud. So, the access control allows only authorized users to access E-health data. In healthcare, timely access to patient data is critical for effective care delivery (Seol et al., 2018). Time delay in accessing data can lead to serious consequences for patient care, including delayed diagnosis, inappropriate treatment, and even patient harm. For this reason, the time of user access is decreased.

The Generate Access Key (GAK) algorithm is proposed to produce a Security Secret Key (SSK). The GAK would work by providing users with a unique SSK that would be used to allow them to access data in the E-healthcare-based cloud system with the minimum of delay. Users are also given flexible access rights based on their role and rights according to User Access Rights (UAR) algorithm. To protect the privacy of users, the data is encrypted using the Database Encryption (DBE) algorithm before being stored in the database. To be read by the users, the data in the system must be decrypted based on the Database Decryption (DBD) algorithm.

1.2 Problem Statement

Transferring E-health data to the cloud introduces some security and privacy challenges that must be carefully considered and managed.

- Patient data can be vulnerable to a number of attacks and risks, including unauthorized access, data breaches, and compromised healthcare services.
- Illegal users can exploit vulnerabilities in the system to gain unauthorized access to sensitive patient data, such as medical histories, treatment plans, and payment information.
- Patients are also reluctant to use E-healthcare services if they feel that their privacy is not protected.
- Lack of privacy leads to illegal use of patient data.
- Inadequate attention to time may lead to security and privacy breaches that can have far-reaching consequences.
- Latency time in granting or revoking access to patient data can lead to data breaches or the unauthorized use of patient data.
- Access control policies should be implemented in a timely manner to ensure that only authorized users have access to patient data.

1.3 The Aims of Thesis

Viewing the current systems developed by researchers in an earlier year to know the most important methods and strategies used in this field and benefit from them to plan future solutions.

Also, designing a system that ensures the efficient use and distribution of a cloud-based E-healthcare system model that addresses security and privacy concerns. The emphasis is on developing methods that ensure only authorized users have access to E-health data while also minimizing user access time.

1.4 Thesis Objectives

- In order to study methods that are used for secure access scheme for cloud-based E-Healthcare services.
- In order to design and implement new algorithms for E-healthcare based cloud services.
- In order to obtain the security and privacy requirements in the proposed algorithms.
- In order to solve the problem of unauthorized access by getting authentication for only valid users by performing the GAK algorithm that gives a unique SSK to each user.
- In order to address the issue of time delay in data access.
- In order to protect the privacy of the users, the data is encrypted before being stored in the database using the DBE algorithm.
- In order to give users a flexible access rights based on UAR algorithm.
- In order to decrypt the data for reading by valid users according to DBE algorithm.
- Ability to write a program using the new algorithm and apply it to obtain a good result.

- In order to provide a secure transmission channel between the user and the cloud database.

1.5 Thesis Contribution

- GAK algorithm is proposed based on MAC algorithm and Hashing technique that generates unique Security Secret Keys (SSKs) for users, which enables robust and secure access to data in the cloud system.
- The flexible access rights provided by the UAR algorithm that allows for a fine-grained access control mechanism, which enhances data security.
- DBE algorithm is proposed based on AED and SHA algorithms that encrypts the data before storing it in the database, which protects the privacy of users and prevents unauthorized access to sensitive data.
- DBD algorithm enables the decryption of data for authorized users, which ensures that the data remains usable while maintaining its confidentiality.

1.6 Outline of The Thesis

The outline of this thesis is also included with this chapter and the following chapters:

Chapter 2: Contains background and literature reviews of security in E-healthcare systems and highlights the challenges and risks involved in sharing E-healthcare with other stakeholders, emphasizes the importance of reducing delay in data access and protect user privacy.

Chapter 3: proposes the Generate Access Key (GAK) algorithm to produce a Security Secret Key (SSK). The GAK would work by providing users with a unique SSK that would be used to allow them to access data in the E-healthcare-based cloud system. Users are also given flexible access rights

based on their role and rights according to User Access Rights (UAR). To protect the privacy of users, the data is encrypted using the Database Encryption (DBE) algorithm before being stored in the database. To be read by the users, the data in the system must be decrypted based on the Database Decryption (DBD) algorithm.

Chapter 4: Shows the simulation results along with the figures, and evaluates the performance of the proposed algorithms.

Chapter 5: Presents the conclusions and future work about this thesis.

CHAPTER TWO: BACKGROUND THEORY and LITERATURE REVIEWS

2.1 Introduction

E-healthcare is the use of electronic communication and Information Technologies (IT) to improve healthcare services and support healthcare management. E-healthcare encompasses a broad range of applications, such as Electronic Health Records (EHR) (Kim et al., 2019), Electronic Medical Records (EMR) (Khan et al., 2014), home Telehealth (Chumbler et al., 2007), Personal Health Records (PHR) (Flaumenhaft and Ben-Assuli, 2018), and health information exchange (HIE) (Esmailzadeh and Sambasivan, 2016). These applications enable healthcare providers to improve patient care and outcomes by providing timely and accurate information, facilitating communication between healthcare providers and patients, and increasing access to healthcare services. (Susanto et al., 2017). The E-Healthcare system enhances healthcare collaboration and coordination in order to simultaneously raise care levels and decrease costs (Kute et al., 2022).

In the past, health records were stored in a decentralized manner, where each hospital or healthcare institution had its own database server to store patient data. However, with the rise of e-healthcare applications, it has become increasingly important for patient data to be accessible on application servers that are typically hosted in the cloud (Wehde, 2019). With the use of networks, servers, memory, software, and services such as these that can be quickly provided and delivered with the least amount of management work and interaction from service providers, cloud computing enables quick, on-demand access to a shared stock of customizable computational resources. (Xiao et al., 2012). Cloud computing refers to the use of internet accessible healthcare servers to collect, monitor, and analyze healthcare data. E-Healthcare services enable the effective communication of patient data across various entities, such

as patients, nurses, doctors, laboratory staff, receptionists, and pharmacists. The cloud computing model offers several options for enabling flexible and controllable information sharing (Sun et al., 2014).

However, there are difficulties with sharing E-health data in the cloud computing. The health data of patients is very sensitive because it contains personal information, including the details about the patient's medical history, symptoms, treatment, associated diseases, or even family health history (Tari et al., 2015). In addition, privacy and security are significant obstacles to the widespread adoption of cloud in some areas. When users outsource sensitive health data for sharing on cloud servers, it presents many new challenges for data security and privacy. As a result, ensuring the protection of personal health information stored in the cloud is critical, and robust security measures must be in place to prevent unauthorized access. These challenges must be addressed to ensure the safe and effective use of cloud computing in healthcare.

Access control is a critical aspect of E-healthcare systems, and ensuring secure and appropriate access to patient data is essential for protecting security and privacy while also maintaining the integrity of the healthcare system. Access control must be controlled to ensure that only authorized users can access the E-health data. However, a delay in accessing data can have serious consequences for patient care, as healthcare providers may not have access to important information when they need it. (Esposito et al., 2018). Several approaches have been discussed to address issues of access control in E-healthcare systems. A series of procedures are used to grant access to ensure that this person may access the resources they have requested (Kurdi et al., 2019). Usually, these actions include, identification, authentication, and authorization. This chapter focuses on using E-healthcare based cloud security challenges, the importance of data access control is discussed, and related works about access control are reviewed.

2.2 E-healthcare

Information and Communication Technology (ICT) supports E-healthcare, a relatively new field that offers medical information and healthcare services. There are several definitions used in this field, and the commonly used term is “E-Healthcare”. The World Health Organization (WHO) defines E-Healthcare as “the cost-effective and secure use of information and communications technologies in support of health and health-related fields, including healthcare services, health surveillance, health education, knowledge, and research” (Ojo et al., 2007, Omary et al., 2009).

2.3 Applications of E-healthcare

E-Healthcare aims to increase collaboration and coordination amongst healthcare providers in order to simultaneously raise care quality and lower costs. The high advantages and wide-ranging potential will speed up the development of E-healthcare. The main and most deeply researched E-healthcare applications around the world include (Mosa et al., 2012):

- **Electronic Health Record (EHR):** An EHR contains various data points related to a person's health, including medical history, diagnoses, medications, allergies, lab test results, imaging reports, and more. EHRs are designed to be interoperable, meaning they can be accessed and shared between different healthcare organizations to support coordinated care. The purpose of an EHR is to provide a comprehensive and accurate record of an individual's health history that can be used by healthcare providers to make informed treatment decisions (Kim et al., 2019).
- **Electronic Medical Record (EMR):** EMR refers to an electronic record that contains health-related information about an individual and is used

in the medical process. The record can be created, managed, and accessed by authorized clinicians and staff within a healthcare organization. EMRs are designed to improve the management of patient information, enhance communication among healthcare providers, and increase the efficiency of healthcare delivery. (Khan et al., 2014).

- **Personal Health Record (PHR):** A PHR is a digital collection of an individual's health-related information that can be obtained from various sources and managed by the owner. The owner of the PHR has control over who can access the record and can choose to share it with healthcare providers or other relevant parties as needed (Flaumenhaft and Ben-Assuli, 2018).
- **Home Telehealth:** Home Telehealth is the healthcare services provided by home healthcare providers to connect home-based patients with external sources of healthcare information and services. This includes remote monitoring of a patient's vital signs, virtual consultations with healthcare professionals, medication management, and other related services (Chumbler et al., 2007).
- **Health Information Exchange (HIE):** HIE refers to the secure sharing of health-related information among different organizations. This process can involve gathering information from sources such as health research labs, disease communities, and organizations using E-healthcare systems and other related technologies (Esmaeilzadeh and Sambasivan, 2016).

2.3 Cloud Computing

Cloud computing is a form of computing that utilizes virtualized resources and services that can be scaled dynamically and accessed over the Internet. It is not only a technological concept but also a paradigm that offers quickly deployable, distributed, and elastic resources like servers, storage, applications, and networks (Peng et al., 2014). Many companies are gradually reaching various limitations for the number of records they can handle inside their IT infrastructure due to the volume of data in the majority of E-healthcare systems today. Since cloud computing provides "unlimited" computer resources and capacity, it may quickly solve this problem (Shaw-Saliba et al., 2022).

Implementing cloud computing technology would help healthcare professionals deliver higher-quality care that is also more efficient. More significantly, it helps them exchange information, collaborate better, and spend less on infrastructure. The cloud paradigm offers a platform for regional, national, and worldwide data aggregation employing a wide range of topologies that might quickly and affordably combine numerous devices, data sources, and services (Javaid et al., 2022).

2.4 Cloud Computing for Healthcare Sectors

Today's healthcare environments require a system that reduces the time-consuming and costly processes required to get a patient's full healthcare history and universally combines the collection of health data in order to provide it to the healthcare staff. E-healthcare makes it possible for users, insurance providers, and healthcare professionals to produce, manage, and access healthcare data in a variety of situations. General structure of E-healthcare based-cloud is shown in Fig.2.1. All healthcare organizations have as their major goal expanding the number of individuals who have access to

healthcare services (Cresswell et al., 2022). The healthcare sectors require greater computing power to improve the quality of service since the amount of data that has to be stored, analyzed, and updated is growing dramatically. By offering better, quicker, more secure, and universal services at a cheaper cost that satisfy the needs of the healthcare industry, the cloud computing environment enhances patient care. As a result, healthcare providers are more ready to shift their systems to the cloud (Gupta et al., 2022).

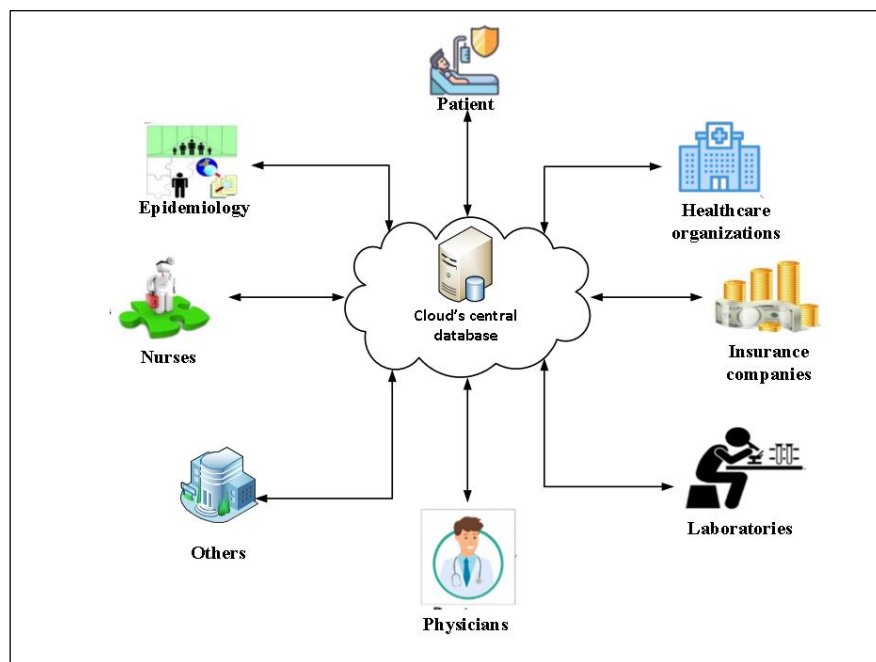


Fig. 2. 1 general structure of E-healthcare based cloud

2.4.1 Cloud based E-healthcare Service Models

There are three different service models for cloud-based E-healthcare as presented in Fig. 2.2:

- **Infrastructure as a Service (IaaS):** Clients can supply virtual storage, virtual machines, virtual infrastructure, and other physical components using IaaS. All infrastructure is managed by the IaaS service provider, while the customer is in charge of all other deployment related tasks. This can contain the software programs, operating system, and user interface (Mahmood, 2011).

- **Platform as a Service (PaaS):** PaaS offers virtual computers, operating systems, services, applications, transactions, development frameworks, and control structures. The customer can either utilize applications that are coded or put their own applications on the cloud infrastructure. using the PaaS service provider's supported tools and languages (Moghaddam et al., 2015). The proposed system model is designed using PaaS.
- **Software as a Service (SaaS):** The top layer of the cloud computing stack, known as SaaS, is the one that the end user actually uses. Customers have the option to use a service provider's application that is stored on a cloud infrastructure. A thin client interface, such as a web browser, allows access from a variety of client devices (Azeez and Van der Vyver, 2019).

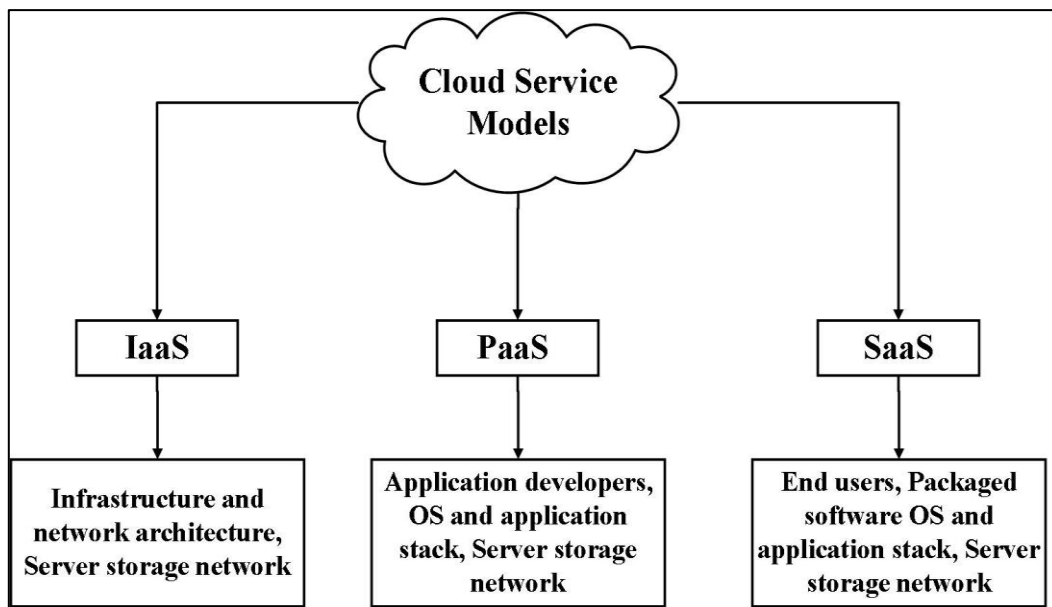


Fig. 2. 2 Cloud based E-healthcare Service Models

2.4.2 Cloud based E-healthcare Delivery Models

Models for cloud-based E-Healthcare services three different types of cloud models are commonly used. Private, public, and hybrid clouds are available.

- **Private cloud:** E-healthcare in a private cloud is only accessible by recognized staff members of healthcare organizations that are considered as trustworthy and reliable (Subashini and Kavitha, 2011).
- **Public cloud:** In this model, the shared infrastructure is entirely the provider's responsibility. Cloud Service Providers (CSPs) provide the services for this type of cloud technology. Due to the fact that E-healthcare is kept on servers that are located off-site and managed by CSPs, they are extremely susceptible to different attacks and manipulations. Effective cryptographic tools and fine-grained access control frameworks are needed to get around this security issue (Subashini and Kavitha, 2011).
- **Hybrid cloud:** This combines both private and public clouds such that each model operates separately but is connected via common technology. This model's implementation for E-healthcare is very beneficial since it incorporates the advantages of both models (public and private). Healthcare providers can easily utilize third party services to store massive amounts of medical data if they have limited financial resources, physical space, and a strong desire to stick with existing systems. However, before it can be used to its full potential, an effective security architecture is required (Azeez and Van der Vyver, 2019). Fig. 2.3 shows the delivery models of clouds. Hybrid cloud is employed in the proposed system model.

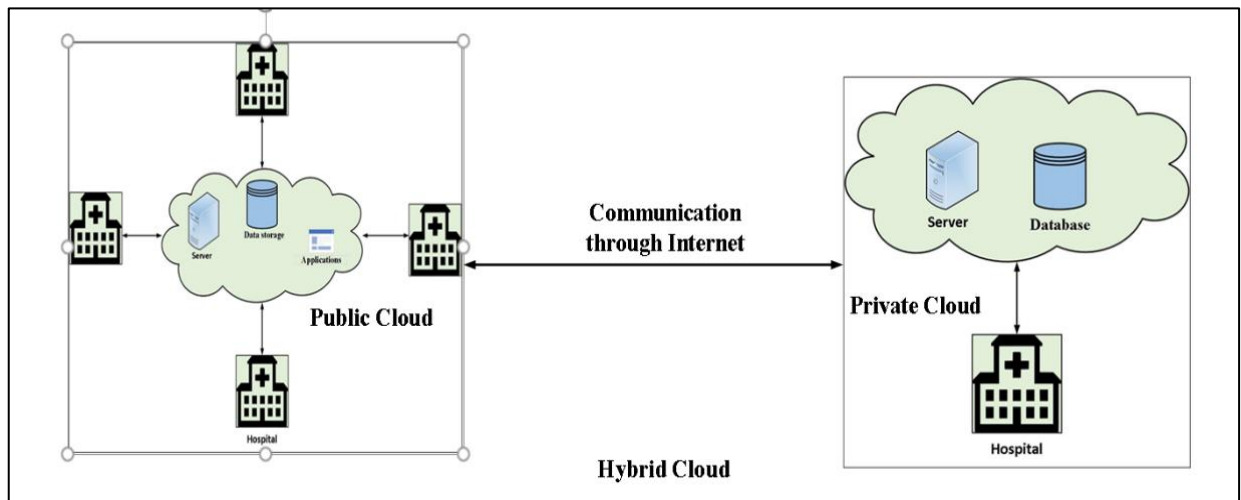


Fig. 2. 3 Hybrid cloud-based E-Healthcare

2.5 E-Healthcare Cloud Computing Benefits

Improved patient care as a result of continuous communication between patients and many healthcare stakeholders. Doctors have access to patient data anytime, anywhere for analysis and diagnosis. E-healthcare cloud computing offers numerous benefits, including:

- 1) Cost savings: buying expensive hardware and software is not necessary. The reductions include all direct costs associated with purchasing hardware and software for on-premises use, as well as support and maintenance costs.
- 2) Energy savings: Since there is no longer a demand for on-site data centers, energy costs will drop along with the need for expensive cooling.
- 3) Robust disaster recovery: Almost all cloud service providers offer backup systems and services in case of an emergency.
- 4) Research: To support national efforts in illness prevention, disease control, and epidemic tracking, the cloud acts as a central data source.

5) Rapid deployment means that software and hardware could be utilized very quickly.

6) Data availability: All entities involved in healthcare, such as doctors, clinics, hospitals, and insurance companies, have easy access to data. (Tahir et al., 2020, Pino and Di Salvo, 2013).

2.6 Privacy and Security in E-healthcare Cloud

The patient health data includes all of the following: personal information, medical history information, symptoms, related conditions, and even family medical history. As a result of its special sensitivity, implementing the practice of sharing electronic health information would increase the privacy and security challenges of such data. As a result, security and privacy must be taken into account while sharing health information.

- **Privacy:** Patients own the health data, despite it being shared. It is crucial to make sure only the patient or the authorized representative can specify who may read the shared health information and for what purposes. Not every piece of data a patient produces is equally sensitive. In other words, some information is shared by the patient for specific purposes and some information is not. It has to deal with the issue of how to logically organize the health data for distribution for a patient's various needs under various circumstances (Sengan et al., 2022).
- **Security:** Security is the guarantee that only authorized people or organizations may access patient data. One of the most common causes of data leakage is employee theft and unauthorized access, along with unintentional exposure as a result of system faults. Unauthorized entry and outside, harmful attacks are another problem. The security of shared

health data must be guaranteed by the providers. Therefore, the identity, encryption, and access control of patient health data are required (Pelekoudas-Oikonomou et al., 2022).

2.7 Common E-healthcare Security and Privacy Issues

In order to address the emerging security and privacy concerns impeding the widespread adoption of cloud computing by healthcare providers, in this section we highlight essential security issues for E-Healthcare systems (Mohamed et al., 2022).

- **Access Control:** Access control is a critical security challenge in E-healthcare-based cloud systems. This is because E-healthcare systems typically contain sensitive and confidential information about patients, such as their medical history, personal information, and treatment plans. Cloud-based E-healthcare systems typically allow access to this information from different locations, devices, and users, which increases the risk of unauthorized access. Therefore, implementing proper access control mechanisms is essential to ensure the confidentiality, integrity, and availability of patient data (Salji et al., 2022).
- **Confidentiality:** One of the most critical concerns in E-healthcare is the confidentiality of patient information. Unauthorized access to sensitive medical data can cause irreparable damage to patients, including identity theft, medical identity theft, and financial fraud.
- **Integrity:** Integrity ensures that the health data collected by a system or presented to any organization is correct and consistent with the intended information and has not been changed.
- **Availability:** For any healthcare cloud to work properly, information must be available at 24/7. The availability of data in critical situations,

especially the capability to continue operations even when several authorities misbehave, is a vital and frequently underestimated feature of the eHealth system (Löhr et al., 2010).

2.8 Classification of Security Solutions in E-Healthcare Systems

The improvement of information technology and data communications increases the sharing of extremely sensitive health data. E-health systems are commonly utilized, and many healthcare centers rely on the internet and local networks for the transmission and receiving of health information. Many security mechanisms have been established over the years to maintain patient privacy and secure the protection of sensitive health data (Idoga et al., 2016).

2.8.1 Access Control

There are certain non-cryptographic ways that can give security as well, but they are not generally employed since they only provide partial protection for the E-health cloud computing when compared to the security provided by crypto methods (Li et al., 2020). Secure access is important for any E-healthcare system. Access control must be controlled using a quick but strong authentication. Access control is a technique for limiting access to a patient's public health data to only authorized parties. Typically, the privilege and right of each authorized practitioner by a patient or other reliable third party form the foundation of the policy of access control. (Kurdi et al., 2019). The security and access control issues have been addressed with a number of methods. A series of procedures are used to give access to ensure that this person may access the resources they have asked for. Usually, these actions include: Identification, Authentication, and Authorization.

- **Identification:** Users must provide identification information such as a username or email address to access the E-healthcare system. This step

helps to verify the user's identity and determine if they have permission to access the patient's health information (Arikumar et al., 2022).

- **Authentication:** After providing identification information, users must authenticate their identity using a password, biometrics, or smart card. This step ensures that only authorized users have access to the E-healthcare system (Nigam et al., 2022).
- **Authorization:** Once authenticated, users must be authorized to access specific patient records based on their role and responsibility. The E-healthcare system should provide a role-based access control model that grants access only to authorized users based on their job responsibilities.
- **Review and Monitoring:** Access control policies and procedures should be reviewed regularly to ensure that they are effective and up-to-date. The E-healthcare system should have mechanisms to monitor user activity, detect unauthorized access attempts, and alert system administrators in case of any suspicious activity (Tawalbeh et al., 2020).

2.8.2 Cryptography

Health data is highly sensitive information that must be protected to ensure patient privacy and prevent unauthorized access. Cryptography can help protect health data by encrypting it during transmission and storage. This ensures that even if a hacker or other unauthorized person gains access to the data, they will be unable to read it. There are several cryptographic techniques that can be used to protect health data, including Broadcast Encryption Schemes, Attribute-based Encryption, Block chain-based Encryption, and Searchable Symmetric Encryption are among the encryption methods utilized in the E-health system (Huang et al., 2018).

- **Public Key Encryption (PKE) and Symmetric Key Encryption (SKE):** Encryption is essential for data protection. Encryption disables

electronic information so that no one other than the key may access it. PKE and SKE are two different methods of encrypting data to protect it from unauthorized access. SKE involves using a single secret key to both encrypt and decrypt the data. This key must be kept secret, as anyone who has the key can decrypt the data. Examples of SKE algorithms include Advanced Encryption Standard (AES). SKE is generally faster and more efficient than PKE, but it requires the secure distribution of the secret key to all parties involved in the communication.

PKE, also known as asymmetric encryption, uses a pair of keys, one public and one private. The public key is available to anyone, while the private key is kept secret by the owner. The encryption process uses the public key to encrypt the data, and only the corresponding private key can be used to decrypt the data. PKE is slower than SKE but provides stronger security as the private key is not shared with anyone else. (Celesti et al., 2019).

- **Broadcast Encryption** : Broadcast encryption is a technology that allows a website to protect its transmissions during mid-stream broadcast and deliver them to a specific group of receivers, while also minimizing the high-speed communication discussed in the article (Schiza et al., 2019).
- **Qualified Encryption**: Qualified Encryption is a form of public key cryptography that prioritizes privacy. It involves using the customer's private key to delete paragraph descriptions, and only allows access to the security area-based security unit if the user key symbols match the text symbols mentioned explicitly by (Lin and Jiang, 2021).
- **Blockchain-Based Encryption**: The electronic health record system faces significant challenges in verifying, protecting, and synchronizing patient data, and the decentralized nature of health records poses privacy risks. To ensure accuracy and integrity of electronic health data,

hash counts and blockchain-based recording are used. To address privacy concerns, patient data details were removed from the Ethereum blockchain, and a new agreement was reached to allow word searches without the need for third-party access, as explained in the article (Khezr et al., 2019).

- **Searchable Symmetric Encryption:** Searchable Symmetric Access (SSE) enables a user to access the data entered without the fear of data loss when transmitting to the cloud. Despite significant interest, present research does not investigate how SSE structures are produced and how they end up in various sections of the SSE system. The inverted file list is used by most programs to determine the proper file size and perform a sublinear search (Li et al., 2020).

2.9 Methods to Encrypt Health Data

The data is secured through data encryption, which encrypts the data using an appropriate cryptographic process. Encrypt data while it's in transit or at rest, such as when it's on a cloud or local database (Khan and Hoque, 2016, Manikandan et al., 2021). Three different types of encryptions are most common:

- **E2E encryption:** Private keys are used to encrypt records at the end device. A safe technique if access to the data on the backend is never required.
- **Database-level encryption:** All of the database's records are encrypted as a single unit. This method is not particularly secure because all the records might be unlocked at once.
- **Record-level encryption:** The records of every patient are individually encrypted. a much safer alternative than database-level encryption since each key can only be used to decrypt a record.

Typically, database-level security is enough for most data. This is what cloud companies deliver to their clients. However, record-level encryption should be used for health data. Each record is encrypted with its own key in this case. End-to-end encryption may be preferable for securing sensitive data. The communication is encrypted before being delivered to the network and can only be deciphered by the recipient. These technologies are not provided by traditional cloud providers.

2.10 Literature Reviews

Addressing security and privacy issues in E-Healthcare has been the subject of extensive research. Some suggested secure E-Health system architectures are reviewed.

In order to survive well-known attacks and provide strong performance, (Yassin et al., 2016) suggested a secure biometric-based remote authentication technique leveraging biometric properties of hand-geometry. They have also developed a system that is resistant to well-known attacks including password guessing, server impersonation, insider attacks, Denial of Service (DOS) attacks, replay attacks, and parallel-session attacks. This approach is effective in terms of computation costs that is 0.0598 milliseconds when compared to other comparable techniques. Using a flexible authentication technique, (Zhang et al., 2017) have suggested a biometric authenticated key agreement approach for e-health systems to secure the privacy of the user. A dynamically verifying table is used in place of the conventional identity-password table to ensure untrace ability, preserving user anonymity. As a result, the suggested technique the computational time cost is 0.0506 milliseconds.

(Taher et al., 2018) proposed an authentication scheme for IoT and cloud servers. The proposed scheme ensures mutual authentication, resists

eavesdropping attacks, and achieves forward secrecy. Effective result to reduce the computation cost is achieved that is 0.0437 milliseconds. An additional storage space in the memory is also provided. (Aghili et al., 2019) presented an authentication and key agreement protocol that preserves anonymity and provides an access control mechanism for the user. Our proposed protocol, called lightweight authentication and ownership transfer protocol for e-health systems (LACO), can also cover the transfer of user/doctor ownership. Both the security and efficiency of LACO are evaluated and demonstrated that the computation time is 0.0521 milliseconds.

A biometric-based user authentication system was proposed by (Kaul et al., 2020) to offer consumers individualized services in a secure and effective manner. A simple data access control procedure has been provided in the suggested authentication so that only authorized users can access the data in accordance with their capabilities. Also, in order to protect user privacy, communication between users instead of using their global identifiers instead uses their temporary local identifiers. But the system is set up such that in an emergency, if necessary, the user's global identification may be recovered. The computational time cost of the suggested authentication technique is 0.046 milliseconds. (Abdulmalik et al., 2023) proposed a secure authentication scheme that uses the authenticated delegating mechanism based on two factors, first is a one-time password and generating a secure variable vector from a legible user's digital image to enable the permission of a user through the back-end database of a cloud server. The proposed mutual authentication can protect the information against well-known attacks, ensure the user's privacy, and key management. Moreover, comparisons with existing algorithms show that the proposed algorithms supplies more privacy, security metrics, and resistance to attacks than the others while being more efficient in computation cost that is 0.096 milliseconds.

Table 2.1 Summaries of literature reviews

References	Proposed model	Result	Numerical result
(Yassin et al., 2016)	The authentication scheme that relies on hand geometry and smart card factors is robust.	It is powerful to attacks and has high capabilities in both communication and computation costs.	The computational time cost is 0.0598 milliseconds.
(Zhang et al., 2017)	Ensuring privacy in E-health systems through the use of a constantly changing authentication key.	Successfully fulfilling the security demands of E-healthcare systems	The computational time cost is 0.0506 milliseconds.
(Taher et al., 2018)	Flexible and efficient authentication of IoT cloud scheme using crypto hash function	The proposed scheme ensures mutual authentication, resists eavesdropping attacks, and achieves forward secrecy.	The computational time cost is 0.0437 milliseconds
(Aghili et al., 2019)	Lightweight three-factor authentication, access control and ownership transfer	Both the security and efficiency of LACO are evaluated and demonstrated that	The computational time cost is 0.052 milliseconds.

	scheme for e-health systems in IoT.	the proposed scheme is secure.	
(Kaul et al., 2020)	A data access control system for healthcare settings that uses secure, privacy-preserving biometric-based user authentication methods.	Sufficiently secure to meet the requirements for use in a healthcare setting.	The computational time cost is 0.046 milliseconds.
(Abdulmalik et al., 2023)	Secure two-factor mutual authentication scheme using shared image in medical healthcare environment	The proposed mutual authentication can protect the information against well-known attacks, ensure the user's privacy, and key management.	The computational time cost is 0.096 milliseconds

CHAPTER THREE: THESIS METHODOLOGY

3.1 Introduction

In this chapter, the Generate Access Key (GAK) algorithm is proposed based on Message Authentication Code (MAC) algorithm and Hashing technique to produce a Security Secret Key (SSK). The GAK would work by providing users with a unique SSK that would be used to allow them to access data in the E-healthcare system with the minimum of delay. Users are also given flexible access rights based on their role and rights according to User Access Rights (UAR). In order to protect the privacy of users, the data is encrypted using the Database Encryption (DBE) algorithm when stored in the cloud database. DBE is proposed based on Advanced Encryption Standard (AES) algorithm and Hashing technique. To be read by the users, the data in the system must be decrypted based on the Database Decryption (DBD) algorithm.

3.2 Proposed System Model

The proposed system model is deployed to provide robust and secure access in a cloud-based E-healthcare system, as Fig. 3.1 shows the designed system model.

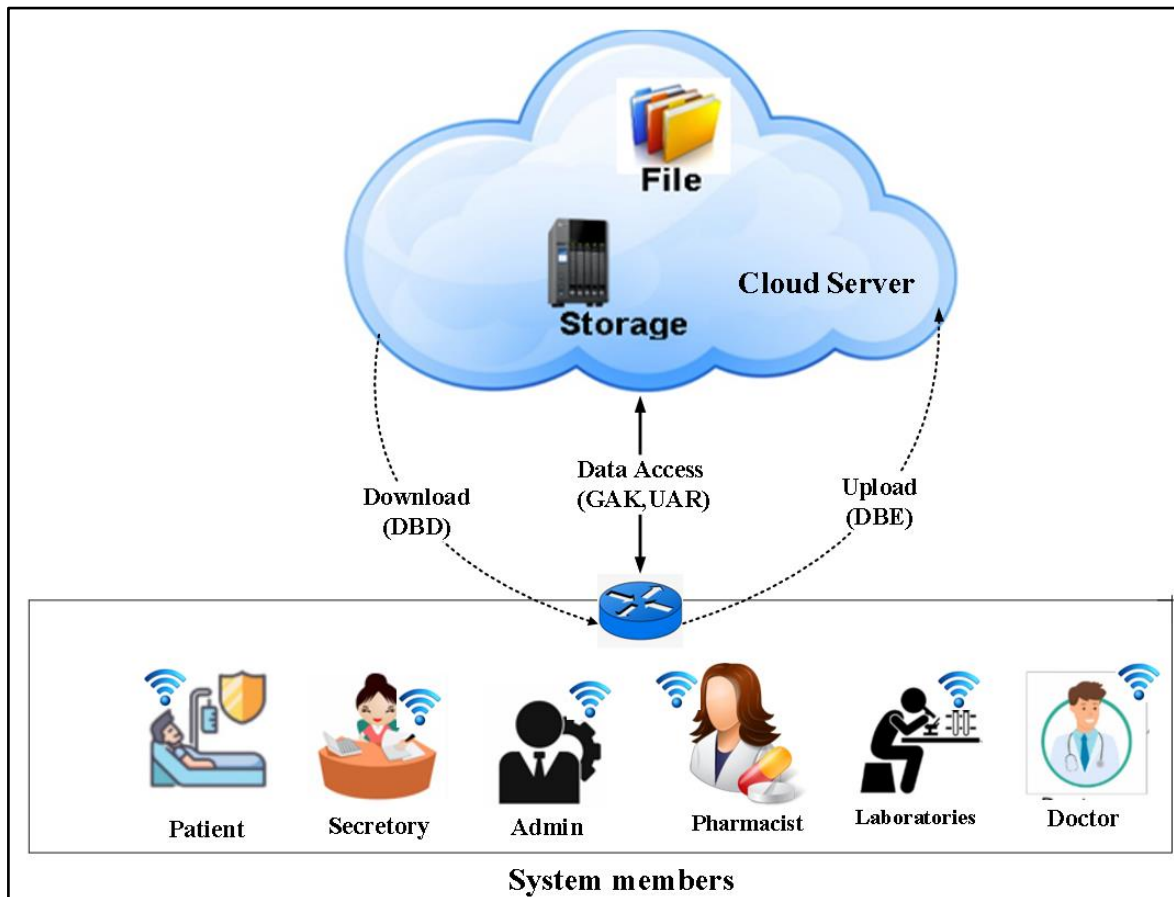


Fig. 3. 1 designed system model

- The cloud provides users with infinite storage space. It provides consumers with simple and effective storage services. The cloud is a semi-trusted third party that provides data storage and download services.
- The user can access the system using IDU and PWU, then use the key obtained from the CS, which is responsible for giving updates to the key. A working system model is shown in Fig. 3.2.

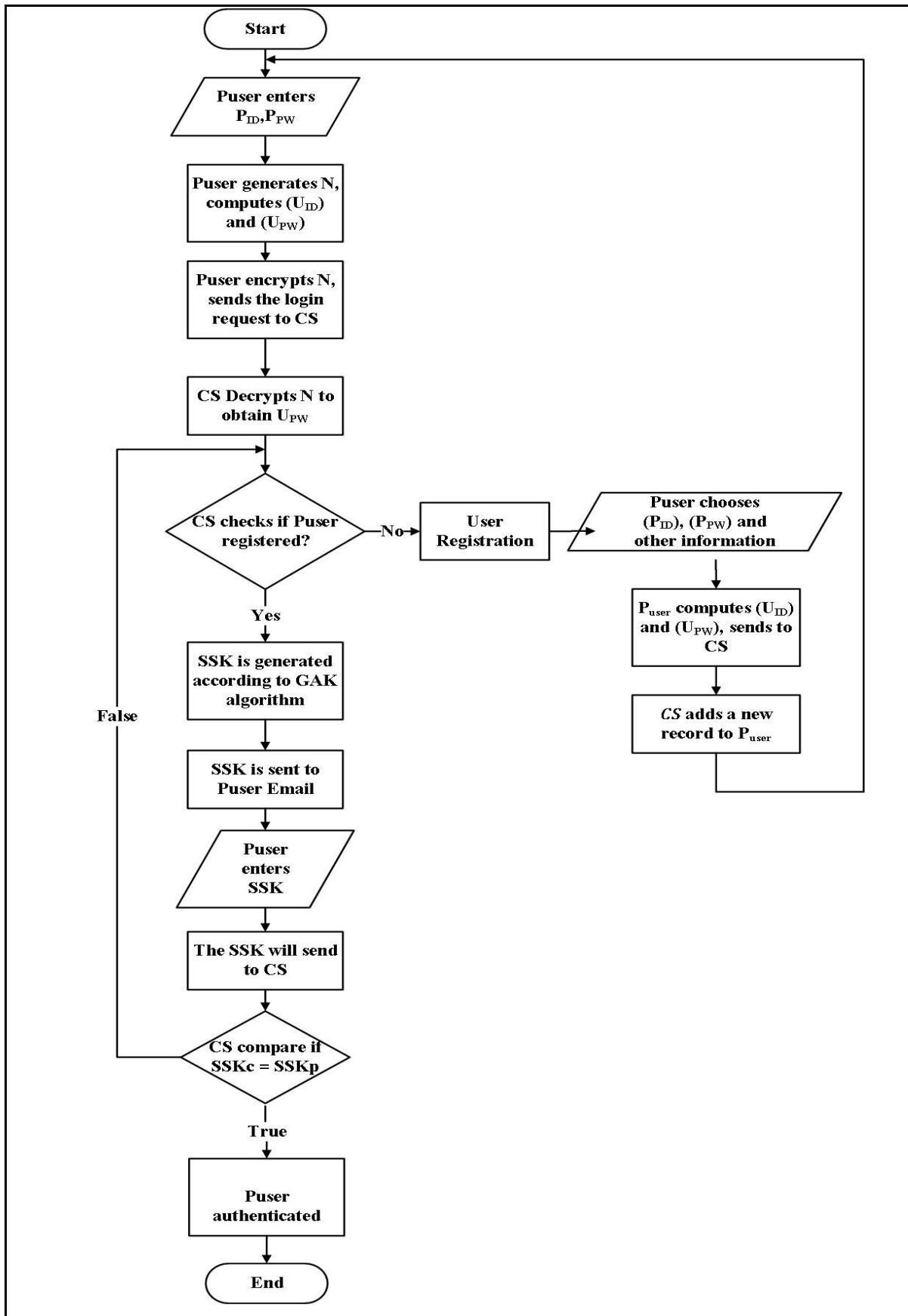


Fig. 3. 2 Flowchart of proposed system model

3.2.1 Registration Phase

Step 1: Patient (P_{user}) chooses his identity (P_{ID}) and password (P_{PW}) in the system of healthcare institute. Also, P_{user} records information about his doctor and relatives in Electronic Healthcare Record (EHR).

Step 2: P_{user} computes the following equations (3.1) and (3.2):

$$U_{ID} = h(P_{ID} \parallel SK_{s,r}) \quad 3.1$$

$$U_{PW} = h(P_{PW} \parallel SK_{s,r}) \quad 3.2$$

Where, U is the user, h is the hash function and SK is a secret key between sender and receiver.

Step 3: P_{user} submits (U_{ID} , U_{PW} , EHR) to Cloud Server (CS).

Step 4: CS verifies its database to check if P_{user} is previously registered. If so, CS terminates this phase. Otherwise, the CS adds a new record to P_{user} according to patient's information (U_{ID} , U_{PW} , EHR) in the main secure database.

3.2.2 Login and Authentication Phase

P_{user} wishes to login the system for checking his EHR , receiving report from his doctor or sending quires to his doctor. Therefore, it is necessary to ensure from the authority of P_{user} to allow him accessing to the system Fig 3.5. shows the login and authentication phase processes.

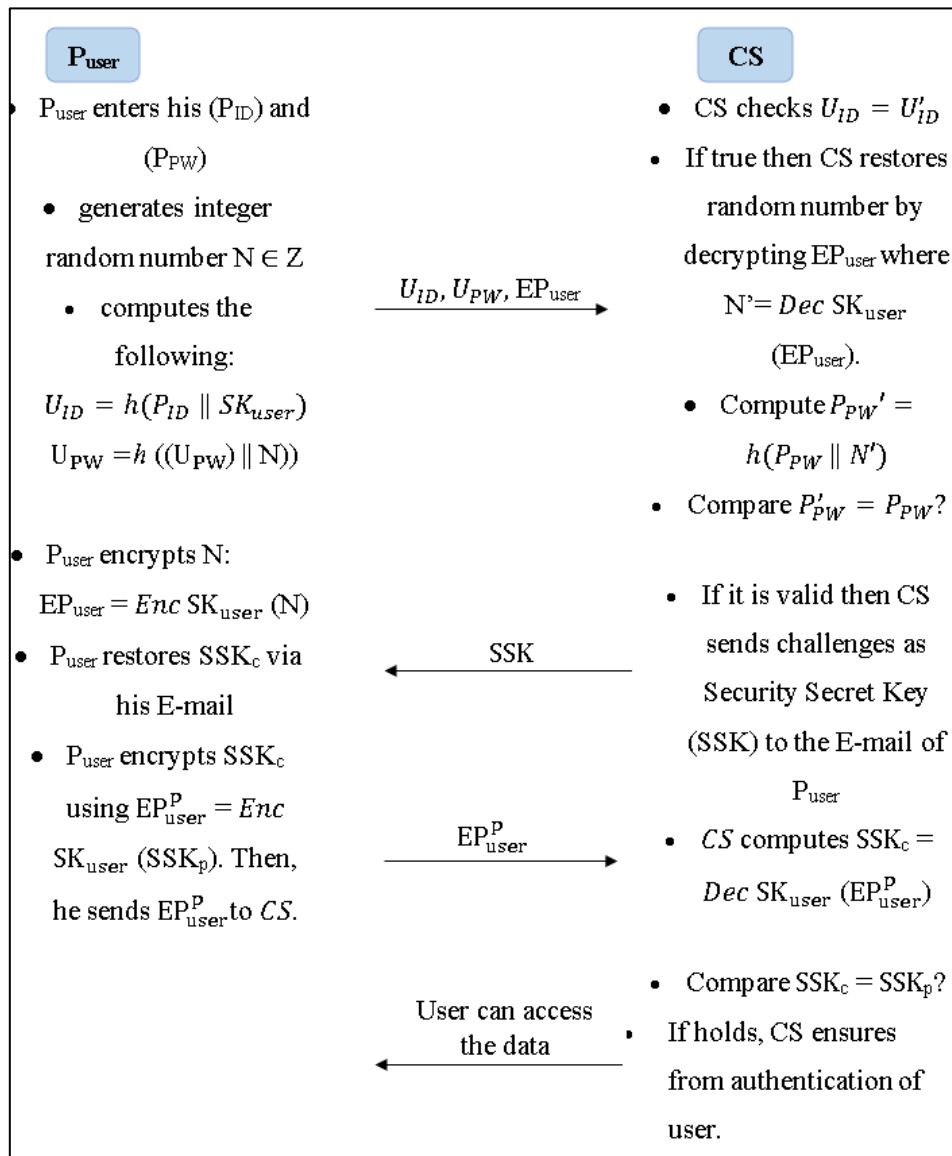


Fig. 3. 3 Login and Authentication phase

The important steps that use in current phase as follows:

Step 1: P_{user} enters his username (P_{ID}) and password (P_{PW}), generates integer random number $N \in Z$, where Z is integer number. Then, computes unknown user identity U_{ID} and unknown user password U_{PW} . where, (U_{ID} and $U_{PW} = h((U_{PW}) \parallel N)$).

Step 2: P_{user} encrypts N, according to $EP_{user} = Enc SK_{E,D}(N)$.

Step 3: P_{user} sends his login request($U_{ID}, U_{PW}, EP_{user}$) to CS.

Step 4: In the *CS*, it checks patients; if P_{user} was found in the database of *CS* or no based on U_{ID} . If false, it terminates this phase. Otherwise, *CS* restores random number by decrypting EP_{user} , where $N' = Dec SK_{E,D}(EP_{user})$.

Step 5: Compare the U_{PW} sent by P_{user} (U_{PW}^p) and the U_{PW} stored in the cloud database (U_{PW}^c), if it is valid then *CS* sends the Security Secret Key (SSK) to the E-mail of P_{user} .

Step 6: At this step, P_{user} restores SSK_c via his E-mail and encrypts SSK_c using $EP_{user}^p = Enc SK_{user}(SSK_p)$, then sends to *CS*. The algorithm 1 demonstrates how SSK is generated according to GAK algorithm.

Algorithm 1: GAK

Input:

h is crypto hash function

SK is private key between sender and receiver

$B \leftarrow 64$ Bytes is number of bytes of blocks

$ipad \leftarrow$ the byte 0x36 repeated B times

$opad \leftarrow$ the byte 0x5C repeated B times.

Output: generate SSK

1: **if** $SK < B$ **then**

2: **do** $SK || padding$ **then**

3: **if** $B == SK$ **then**

4: $SK \oplus ipad \leftarrow SK_{inner}$

5: $h(SK_{inner}) = x1$

6: $SK \oplus opad \leftarrow SK_{outer}$

7: $x1 || SK_{outer} \leftarrow K^o$

8: $h(K^o) = x2$

Generate get offset of $(x2) \leftarrow SSK$

Step 7: CS compares between SSK_c and SSK_p . if true then gives permission to P_{user} for entering the system and applying the main operations included healthcare services at the Healthcare phase. Otherwise, the current phase is terminated.

The GAK algorithm is proposed based on Message Authentication Code (MAC) and Hashing technique to authenticate only valid users.

3.3 Time Execution

Time delays in access control in E-healthcare systems have significant consequences for patient care and treatment. According to the proposed algorithm, three stages are involved: registration, login, and authentication. During the authentication phase, the algorithm creates a unique key for each user's login attempt. The time delay is calculated by measuring the time taken for each operation in each phase. In the registration phase, the Registration Delay (D_R) is calculated by the following equation (3.3):

$$D_R = 2T_h + 2T_{||} \quad 3.3$$

Where function (T_h) is the required time to perform the crypto hash function and ($T_{||}$) is the performing time for the concatenation operation. The coefficient 2 is used for both T_h and $T_{||}$ because the registration phase involves performing these operations twice when a user wants to register.

The login and authentication are another phase before the user can access the data. Login and Authentication Delay (D_A) depends on processing five main operations, which are calculated according to the following equation (3.4):

$$D_A = 5T_h + 3T_{||} + 2T_{Enc} + 1T_{Dec} + 2T_{\oplus} \quad 3.4$$

Where (T_{Dec}) is the processing time for the symmetric decryption function, (T_{Enc}) is processing time for the symmetric encryption function and the processing time for the XOR operation T_{\oplus} . In this phase T_{Dec} is processing

once, T_h is processing five times and $T_{||}$ is processing three times while login and authenticating the valid users, two remained processes ($T_{Enc} + T_{\oplus}$) are performing two times.

So, the Total Delay (D_T) for accessing any user is calculated according to the following equation 3.5:

$$D_T = D_R + D_A \quad 3.5$$

$$D_T = 7T_h + 5T_{||} + 2T_{Enc} + 1T_{Dec} + 2T_{\oplus}$$

D_T refers to the amount of time it takes for users to access data, and this value is derived by combining the processing times in D_R and D_A .

3.4 Proposed System Members

The user can access the data according to his role. There are six roles in our model: admin, patient, doctor, laboratory, secretariat, and pharmacist. The various related permissions and actions are set up in the basic frame based on the varied requirements of each role; that are described below:

- Users are also given flexible access rights based on their role and rights according to User Access Rights (UAR) algorithm as shown by pseudo code.

Algorithm 2: UAR

Input:

U_Q is user request

U_R is user rights

Output: Generate role and rights for each user

1: **Get** U_Q

2: **for all** $U_Q \in$ E-healthcare system **do**

3: **if** $U_Q ==$ patient **then**

4: $U_R =$ view; write;

5: **else if** $U_Q ==$ doctor

```

6:   UR =partial view of related patients; write;
7: else if UQ ==Laboratories
8:   UR =partial view; partial write;
9: else if UQ ==pharmacist
10:  UR = partial view; complete the patient loop;
11: else if UQ ==secretory
12:  UR =write;
13: end

```

- The patient is the person who is admitted to the hospital for a diagnosis or checkup. According to his diagnosis, a particular doctor is assigned to take care of him in the hospital. The patient can view his medical history, make an appointment, get test results, and be assigned drugs.
- Admin is a hospital IT manager who can effectively register the hospital system with the CS. Patients' data are kept in the CS according to the standards established by the hospital IT admin, and the security system provides secure access to the Cloud. Separated their permissions by having roles from the admin, who can control the entire system.
- A doctor is a person who looks after the patients who have been committed to him for treatment. Only the connected doctor should typically have access to the patient's information. The doctor uploads all of the patient data, encrypts it before storing it in the cloud database.
- The laboratories can see the basic information of the patient and send back the test results to the doctor and the patient.
- The pharmacist can see the information report of the patient that contains the drugs written to the patient by the doctor. At the end of all

the checkups in the hospital and consulting with doctors, a patient is provided a medical report and stored in the cloud database.

3.5 Security System Database

The Database Encryption (DBE) algorithm encrypts data before storing it in a database. The process of encryption involves converting plaintext (unencrypted user data) into ciphertext (encrypted user data) using SK. The SK is a secret code that is used to encrypt and decrypt the data.

The DBE algorithm uses a strong and secure implementation of the Advanced Encryption Standard (AES) to convert the plaintext data into ciphertext. AES is a widely used encryption standard that is considered to be one of the most secure encryption algorithms available. Next, the DBE algorithm uses a hashing algorithm to securely manage the cryptographic key used in the encryption process. A hashing algorithm takes the cryptographic key and produces a fixed-size SK. Then the SK is used as a key for encrypting and decrypting the data. By using a SK instead of the original key, the DBE algorithm can ensure that the key is securely managed and cannot be easily accessed by unauthorized users. The algorithm3 demonstrates how the data is encrypted.

Algorithm 3: DBE
<p>Input:</p> <p>Pl is plaintext</p> <p>SK is secret key</p> <p>h is hashing</p> <p>Range $j=[0,1,2,3,4,5,6,7,8,9]$</p> <p>Nr number of rounds</p> <p>Output: Encrypted data</p> <p>1: $h(SK_{E,D}) \leftarrow SK_h$</p>

```

2:  $h(\text{Ptxt}) \leftarrow \text{Ptxt}_h$ 
3:  $\text{state}(\text{Ptxt}_h) \leftarrow \text{state}$ 
4: AddKey(state,  $\text{SK}_{h(0)}$ )
5: for  $j=1$  to  $N_r-1$  do
6:   SubBytes(state)
7:   ShiftRows(state)
8:   MixColumns(state)
9:   AddKey(state,  $\text{SK}_{h(j)}$ )
10: End
11: SubBytes(state)
12: ShiftRows(state)
13: AddKey(state,  $\text{SK}_{N_r-1}$ )
14: Generate Ctxt

```

Once the data is encrypted and the cryptographic key is securely managed, the DBE algorithm stores the encrypted data in the database. When the data needs to be accessed, the DBE algorithm uses the same cryptographic key to decrypt the data and convert it back into plaintext. The algorithm4 demonstrates how the data is decrypted.

Algorithm 4: DBD

Input:

Ctxt is Cyphertext

SK_h is hashed secret key

h is hashing

j is counter

N_r number of rounds

Output: Encrypted data

1: **Get** SK_h

```
2: state(Ctxt) ← state
3: AddKey(state, SKh(0))
4: for j=1 to Nr-1 do
5:   InvShiftRows(state)
6:   InvSubBytes(state)
7:   InvMixColumns(state)
8:   AddKey(state, SKh(j))
9: End
10: InvShiftRows(state)
11: InvSubBytes(state)
12: AddKey(state, SKNr-1)
13: h(Ptxth) ← Ptxt
14: Generate Ptxt
```

CHAPTER FOUR: EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Introduction

Security and privacy issues are considered essential obstacles in the healthcare-based cloud service systems. Therefore, user access control is a crucial step in ensuring security and accessing data in the E-healthcare system with the minimum of delay. In a previous contribution (Chapter three), a robust and secure access control system is described based on the proposed algorithms in the E-healthcare system. Also, by using our algorithms, the time of legitimate user access could be decreased and keep these data private and away from unauthorized access. The performance analysis results indicate an important balance between security and performance. This chapter shows the performance of the proposed model and its computational cost compared with previous works.

4.2 Mechanism of E-Healthcare Design

The mechanism of using supported tools to design E-Healthcare consists of four steps:

4.2.1 Webpage Design

It means designing the structure of a web page, such as (tables, forms, input fields, text areas, etc.) using the Hypertext Markup Language (HTML5) programming language. HTML5 is the latest version of the HTML used to create web pages and applications. It is an improvement over previous versions, offering better support for multimedia elements, improved performance, and enhanced accessibility on mobile devices. HTML5 is also designed to be backward compatible, making it easier for developers to upgrade their existing web pages to the latest version.

4.2.2 Webpage Effects

Using the CSS programming language, jQuery, and Bootstrap classes, webpage effects depict the style of HTML components such as (colors, hovers, font size, position, animation, etc.).

- CSS (Cascading Style Sheets) is a language used to style and format web pages. It is used alongside HTML and JavaScript to create visually appealing and dynamic web pages. CSS allows to control the layout, typography, color, and other visual aspects of a web page.
- jQuery is a popular JavaScript library that simplifies the process of manipulating HTML documents and handling events in web pages. It provides a wide range of tools and features that make it easier to work with HTML, CSS, and JavaScript.
- Bootstrap classes can be used to apply various styling to any web page, like font style, text color, background color, flex, grid system, etc.

4.2.3 Data Processing

During this stage, the inputted data is verified to ensure it is accurate and meets specific requirements. Then, using tools like PHP, jQuery, and JavaScript, the necessary computations are performed to generate the desired output.

- PHP is a server-side scripting language that is used to develop dynamic web pages and web applications. PHP code is executed on the server-side, and the output is sent to the client-side as HTML, CSS, and JavaScript.
- JavaScript is a programming language that is used to create dynamic and interactive web pages. It is a client-side scripting language that runs in the browser and interacts with the CSS to dynamically update web

pages. JavaScript is commonly used to add functionality such as form validation, interactive menus, and animations to web pages.

4.2.4 Saving and Retrieving

Saving means storing entered data in the database, while retrieving is the opposite of saving and involves restoring data from the database. Heroku Cloud Database is a cloud-based database service that allows to store and manage data in the cloud. It is a fully managed service that provides high availability and scalability for applications that require a database. Heroku offers a variety of plans to meet different business needs. The Premium 3 plan on Heroku provides businesses with high availability and heavy workload capabilities. The cloud plan that has been used is outlined in Table 4.1 and includes specific details regarding its specifications.

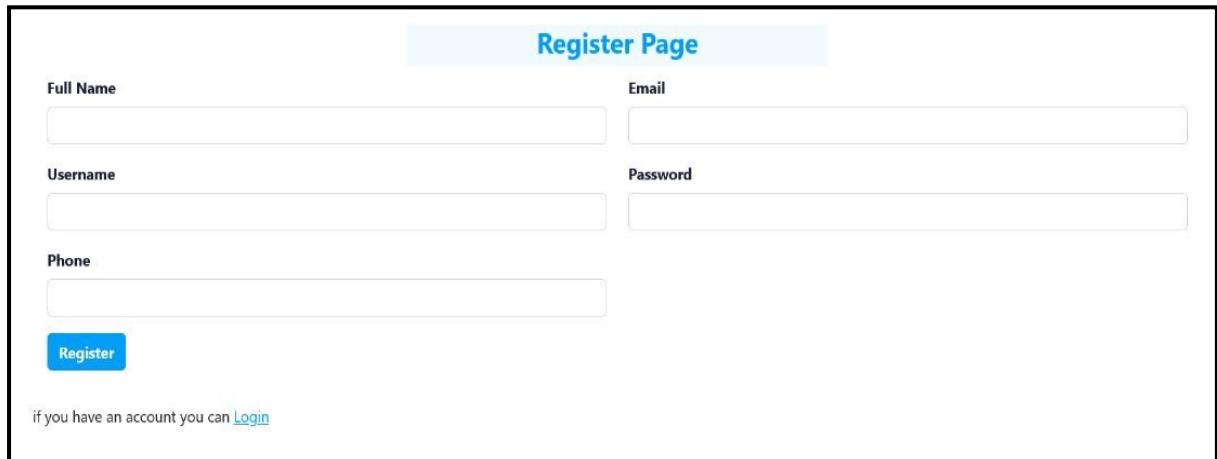
Table 4. 1 Specifications of the used cloud

Specifications	Details
Plan	Premium 3
RAM	15GB
Storage	512GB
Resources	Dedicated
Vertical scaling	Automatic
Horizontal scaling	Automatic
Availability	High

4.3 Implementation of the proposed algorithm

Registration page shown in Fig 4.1 typically serves as the initial interface for patients to create an account and establish their electronic health record. This page requires the user to enter personal information such as name, contact details such as email and phone number along with additional medical history and

demographic data. This data is then stored in the E-healthcare system and used to create a patient profile that can be accessed by healthcare providers to provide more effective and efficient care.

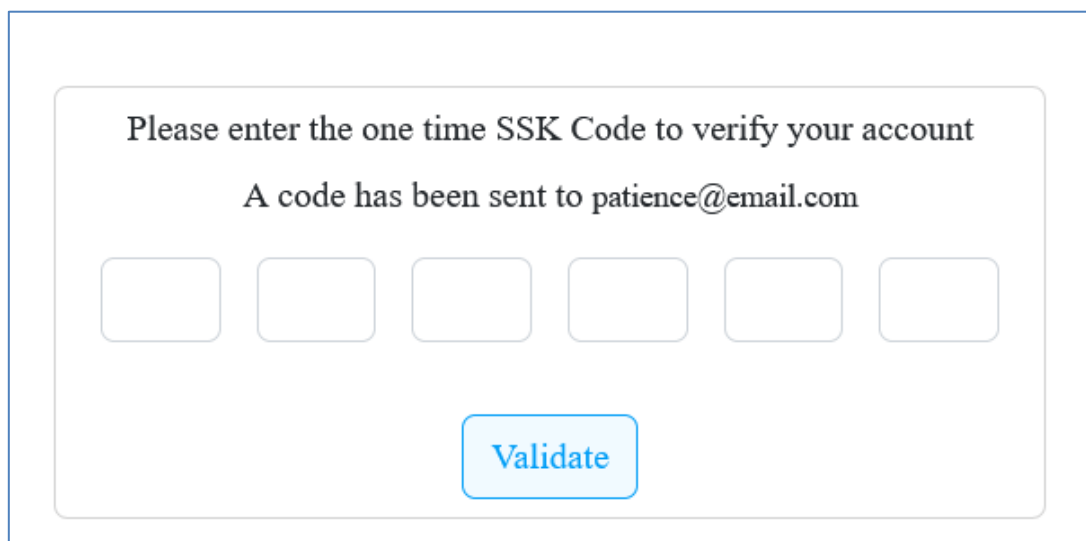


The image shows a registration form titled "Register Page". It includes the following fields and elements:

- Full Name**: A text input field.
- Email**: A text input field.
- Username**: A text input field.
- Password**: A text input field.
- Phone**: A text input field.
- Register**: A blue button.
- Footer**: A link that says "if you have an account you can [Login](#)".

Fig. 4. 1 Registration page

The page used for registering patients also has a system in place to confirm their identity and maintain the confidentiality of their medical information. Once the user has filled out the registration form, they will need to enter a unique code called the SSK as presented in fig 4.2 that has been sent to them in order to finalize the registration process. This additional step is taken to ensure the security and accuracy of the registration information, and to prevent unauthorized access to the patient's personal health data.



Please enter the one time SSK Code to verify your account

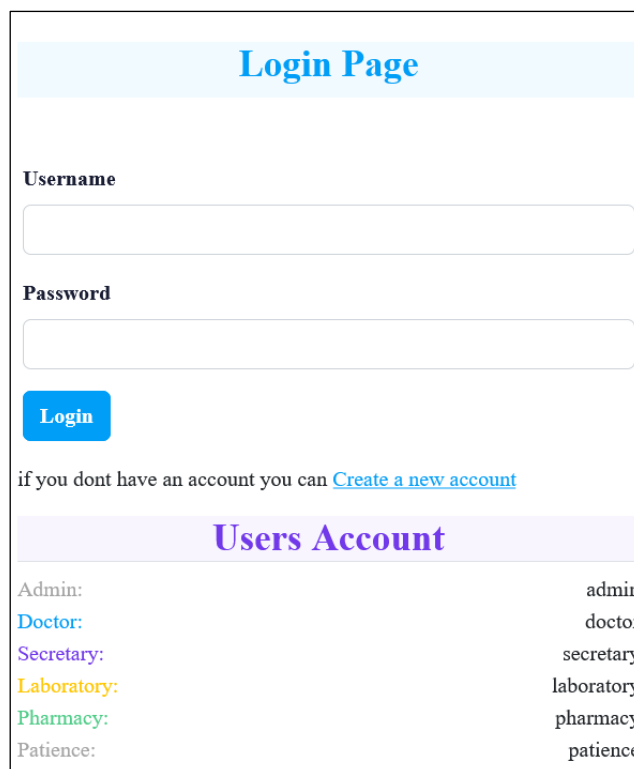
A code has been sent to patience@email.com

□ □ □ □ □ □

[Validate](#)

Fig. 4. 2 Verifying the identity of users before they register

The login page as shown in Fig 4.3 is a primary interface that authorized users use to access health records. To access the E-healthcare system, the user is typically required to enter a username and password, which is then authenticated by the system before granting access to the user's account.



Login Page

Username

Password

[Login](#)

if you dont have an account you can [Create a new account](#)

Users Account

Admin:	admin
Doctor:	doctor
Secretary:	secretary
Laboratory:	laboratory
Pharmacy:	pharmacy
Patience:	patience

Fig. 4. 3 Login page

The login page also requires SSK that is sent to his email as shown in fig 4.4, to ensure the confidentiality, integrity, and availability of the sensitive health data stored within the system.

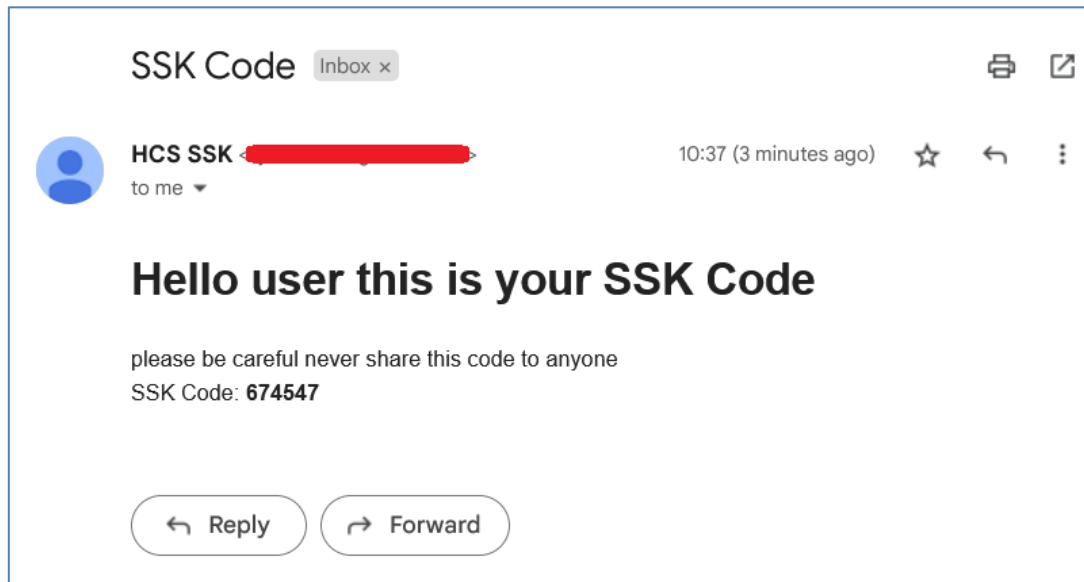


Fig. 4. 4 The sent SSK via E-mail

Fig 4.5 illustrates that the login process necessitates the user to provide an SSK before accessing the system

A screenshot of a verification page. At the top, a green box says "SSK Code Send successfully.". Below that, a white box contains the text: "Please enter the one time SSK Code to verify your account" and "A code has been sent to patience@email.com". There are six input fields for the code, and a blue "Validate" button at the bottom.

Fig. 4. 5 Verifying the identity of users before they register

Upon successful login, the user is granted access to the patient health records that they are authorized to view, edit, or manage. Fig 4.6 contains all the roles that have access to the system. Each user role has specific access levels and permissions within the E-healthcare system, which are designed to ensure that patient information is protected and accessed only by authorized individuals.

#	Name	Role
1	Pharmacy	pharmacy
2	laboratory	laboratory
3	Secretary	Secretary
4	Doctor	Doctor
5	Admin	Admin

Fig. 4. 6 User roles

Fig. 4.7 illustrates that the secretary has the ability to either authorize or decline the patient's request to visit the doctor. The secretary also has the authority to cancel or reschedule the appointment.

#	Doctor	Patient	Appointment	Visit	Time	Action
1	Doctor	Halgurd	Confirmed	With doctor	🕒 / 19	Confirmed
2	Doctor	Halgurd	Confirmed	Comming	🕒 / 18	👤 ✖
3	Doctor	Halgurd	Pending	Comming	🕒 / 17	👤 ✖

Fig. 4. 7 Arrangement of today appointment

The "Today Appointment" page which shown in Fig 4.8 is a feature that allows healthcare providers and administrative staff to view all of the appointments that are scheduled for the current day.

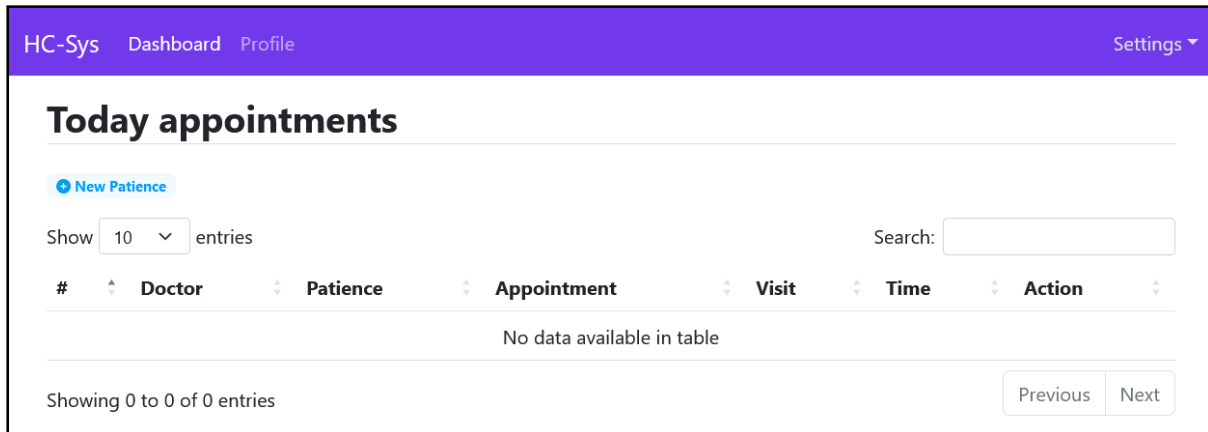


Fig. 4.8 Current day appointment

The doctor secretary can add new patient after filling the patient's information. This will be the alert notification for success adding record to the database. As shown in Fig 4.9 After adding information about a patient to the database the secretary can add an appointment for the patient. the data is stored and can be retrieved by secretary any time needed.

The screenshot shows a web interface for a healthcare system. At the top, there is a purple navigation bar with 'HC-Sys', 'Dashboard', 'Profile', and 'Settings' (with a dropdown arrow). Below the navigation bar, the main content area is divided into two sections. The first section, titled 'Patience Data', displays patient information: Name: Halgurd, Phone: 07501234567, Address: Erbil, Near qalat 30m road, and Gender: Male. The second section, titled 'New Appointment', contains a form with three dropdown menus for 'Doctor', 'Appointment', and 'Visit', each with a 'Choose...' option. Below these are input fields for 'Date' (format: mm/dd/yyyy) and 'Time' (dropdown: Select time). A blue '+ Add' button is located at the bottom left of the form.

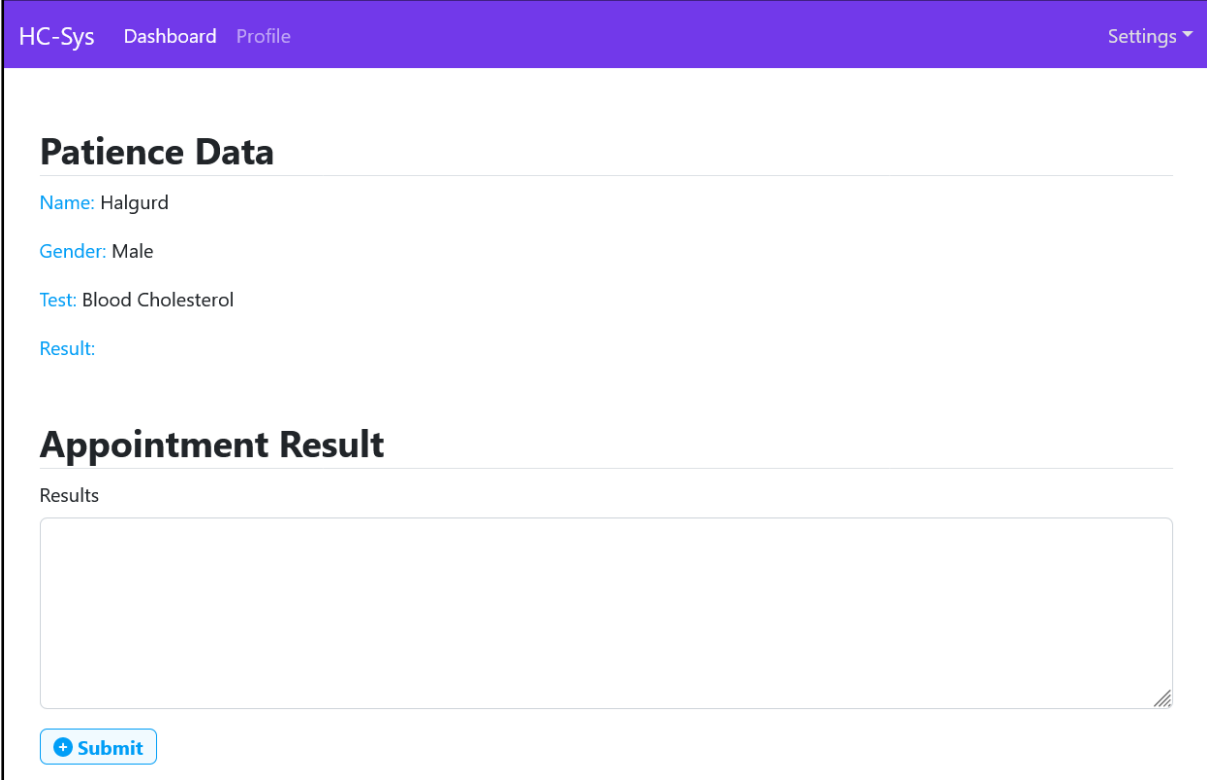
Fig. 4.9 Adding new patient

After the patient is examined by a doctor, the doctor can prescribe tests or drugs for the patient's medical treatment that shown in Fig 4.10.

The screenshot shows the same web interface as Fig 4.9, but with different content. The 'Patience Data' section is identical, showing Name: Halgurd, Gender: Male, and empty fields for Test, Result, and Drugs. The second section, titled 'Doctor Request', contains two large empty rectangular boxes for 'Tests' and 'Drugs'. Below each box is a corresponding button: a purple '+ Tests' button and a yellow '+ Drugs' button.

Fig. 4.10 Doctor view patient data

After the doctor requests a test for a patient in the E-healthcare system, laboratory users will be notified of the test request and perform the necessary tests on the patient. Once the test results are ready, the laboratory users will then send the results to the doctor for review and analysis as shown in Fig 4.11.



The screenshot shows a web interface for a laboratory system. At the top, there is a purple navigation bar with the text "HC-Sys" on the left, "Dashboard Profile" in the center, and "Settings" with a dropdown arrow on the right. Below the navigation bar, the main content area is white. It features a section titled "Patience Data" (note the typo) in bold black text. Underneath this title, there are four lines of text: "Name: Halgurd", "Gender: Male", "Test: Blood Cholesterol", and "Result:". Below the "Patience Data" section is another section titled "Appointment Result" in bold black text. Underneath this title, the word "Results" is displayed above a large, empty rectangular box with a light gray border. At the bottom left of the main content area, there is a blue button with a white plus sign and the text "Submit".

Fig. 4.11 laboratory view a patient's test requests

If the doctor accepts the test results and determines that medication is necessary for the patient's treatment, they may write a prescription for the appropriate medication. The prescription will typically include the name of the medication, the dose, and instructions for how to take it that is shown in Fig 4.12.

The screenshot shows a web interface for a patient's medical data. At the top, there is a navigation bar with 'HC-Sys', 'Dashboard', 'Profile', and 'Settings'. The main content is divided into two sections: 'Patience Data' and 'Doctor Request'. The 'Patience Data' section includes fields for Name (Halgurd), Gender (Male), Test (Blood Cholesterol), and Result (LDL: less than 100 mg/dL, HDL: 40 to 60 mg/dL, Total cholesterol: less than 200 mg/dL, Triglycerides: less than 150 mg/dL, VLDL levels: under 30 mg/dL). The 'Doctor Request' section has two input fields labeled 'Tests' and 'Drugs', each with a corresponding '+ Tests' and '+ Drugs' button below it.

Fig. 4.12 drug request by doctor

The patient can then take the prescription to a pharmacy to have it filled. The pharmacist will review the prescription, prepare the medication, and provide instructions on how to take it shown in Fig 4.13. The patient will need to provide their insurance information or pay for the medication out-of-pocket, depending on their insurance coverage.

The screenshot shows the 'Patience Data' section of the HC-Sys interface. The patient's name is Halgurd and gender is Male. The 'Drugs' section lists two prescriptions: Atrovastatin (Lipitor) and Fluvastatin (Lescol). The 'Finish' status is marked with a green checkmark, indicating the patient has taken the drugs.

Fig. 4.13 Patient took the drugs

After obtaining the medication, the patient may need to schedule a follow-up appointment with the doctor to monitor their response to the treatment and adjust the medication if necessary.

The results displayed in fig 4.14 depict the outcome of employing an encryption methodology designed to enhance database security by protecting against potential security breaches by hackers. In the event that unauthorized access is obtained, the encrypted records stored within the database are rendered unreadable, thereby preventing hackers from obtaining any useful information. The use of this encryption technique is aimed at ensuring that user privacy is safeguarded, even in the event of a security breach even it is impossible by using the proposed accessing method.

id	username	password	name	role
1	NWFSbE91dTlIbKxRZmx5eXgwUXk1UT09	NWFSbE91dTlIbKxRZmx5eXgwUXk1UT09	WVczdHNXWkQURSYldPTkNyeUhgQT09	L01WM0VFZFMUnVCZUVIAnFuTxhXUT09
2	TzNFZTJMaUIPcGFqQI9Ta2Juem1PUT09	TzNFZTJMaUIPcGFqQI9Ta2Juem1PUT09	MDZIS3R1Y1F1dUNBWUdjblh4UKE4UT09	MEM1djjKRWPNUXJZKzdOMisyODdMQT09
3	eTR4ZnNCSDN0S2J3NEVHcStMS1Fkdz09	eTR4ZnNCSDN0S2J3NEVHcStMS1Fkdz09	dDFiSjdljZmN0JiNjBLU0RWb1BXUT09	SGx6QmVsb2JjNGRhWTJucTICendIzZ09
4	ZDFmYmVFNjE5blF4TDZKcWRFWniEUT09	ZDFmYmVFNjE5blF4TDZKcWRFWniEUT09	ZDFmYmVFNjE5blF4TDZKcWRFWniEUT09	TnJtbiZUT2piUGFzSXhVN096ZWZqUT09
5	dHVxQmd0bUdzV25XK3BwNkFuTnlrZz09	dHVxQmd0bUdzV25XK3BwNkFuTnlrZz09	NURZKzExd28xN2k1aExqcdpVGJ4QT09	Z0kvRjlsK1Q1eIRIUgxrK2RrT3ZQQT09

Fig. 4.14 Encrypted data in the database

4.4 Experimental Results and Analysis

The proposed system model is simulated to evaluate its performance and confirm its theoretical background. The simulated findings of the model are shown and discussed.

4.4.1 Simulation Environment

Apache JMeter has been an open-source platform for assessing the performance of systems. To test the effectiveness of the suggested secure access control in an E-healthcare-based cloud system, the algorithms mentioned earlier

were implemented using the JMeter Simulator. The system consists of five operations ($T_{\oplus}, T_h, T_{Enc}, T_{Dec}, T_{||}$) that have been tested with varying levels of load and different numbers of users (n) ranging from ten to two hundred. And requested data size determined.

The system used in this project is detailed in table 4.2 that highlights key specifications. The laptop's high-speed memory, solid-state drive, and powerful CPU and GPU provided the necessary tools to analyze and process the data.

Table 4. 2 specification of the system

Specifications	Details
OS	Win 10
RAM	16GB – 2933MHz
Hard	M.2 NVMe 512GB
CPU	Intel core i7-10750H
GPU	NVIDIA GeForce GTX 1660 Ti

4.4.2 Performance Evaluation

To evaluate the performance of the proposed method according to the system model design. The time cost evaluation is used to determine how much time it takes to authenticate users. When the users send login requests, the system checks if they are valid or not. For this purpose, after checking the U_{ID} and U_{PW} , a SSK is created and sent to the users for proof of user validation. Table 4.3 shows the simulation results of our algorithm. The authenticated users then view the data cloud according to their roles.

Table 4.3 The authentication phase

Number of users (n)	Time (second)
10	20

20	30
30	40
40	50
50	60
60	80
70	100
80	120
90	150
100	180
110	210
120	240
130	270
140	290
150	310
160	330
170	350
180	380
190	410
200	440

The time delay cost for ten to two hundred participants is simulated, and 10 users per simulation are added, as shown in Fig 4.15. First, the least number of users, which are ten users ($n = 10$) is simulated, and the time delay for authentication in our model is 20 milliseconds in the authentication phase. The time delay is gradually increasing as the number of users increases. Because the queuing and processing load on the system also increase, leading to a time delay. If one hundred users ($n = 100$) want to authenticate, the time delay is 180 milliseconds. The difference in time is 160 milliseconds between login requests

from ten users and one hundred users, so the proposed model has good efficiency and high performance.

When there are more users sending login requests, the system performance should not be affected significantly. When 110 users send login requests at the same time, and the proposed system wants 120 milliseconds. The time spent authenticating 150 users is 310 milliseconds, and for 180 users, 380 milliseconds are needed. Only 440 milliseconds are spent for every 200 users. The time difference between $n = 200$ and $n = 110$ is 230 milliseconds, indicating that the proposed secure model requires very little time to obtain authentication. So, the proposed algorithm is lightweight to reduce the overhead on the system and ensure that it can handle high volumes of requests.

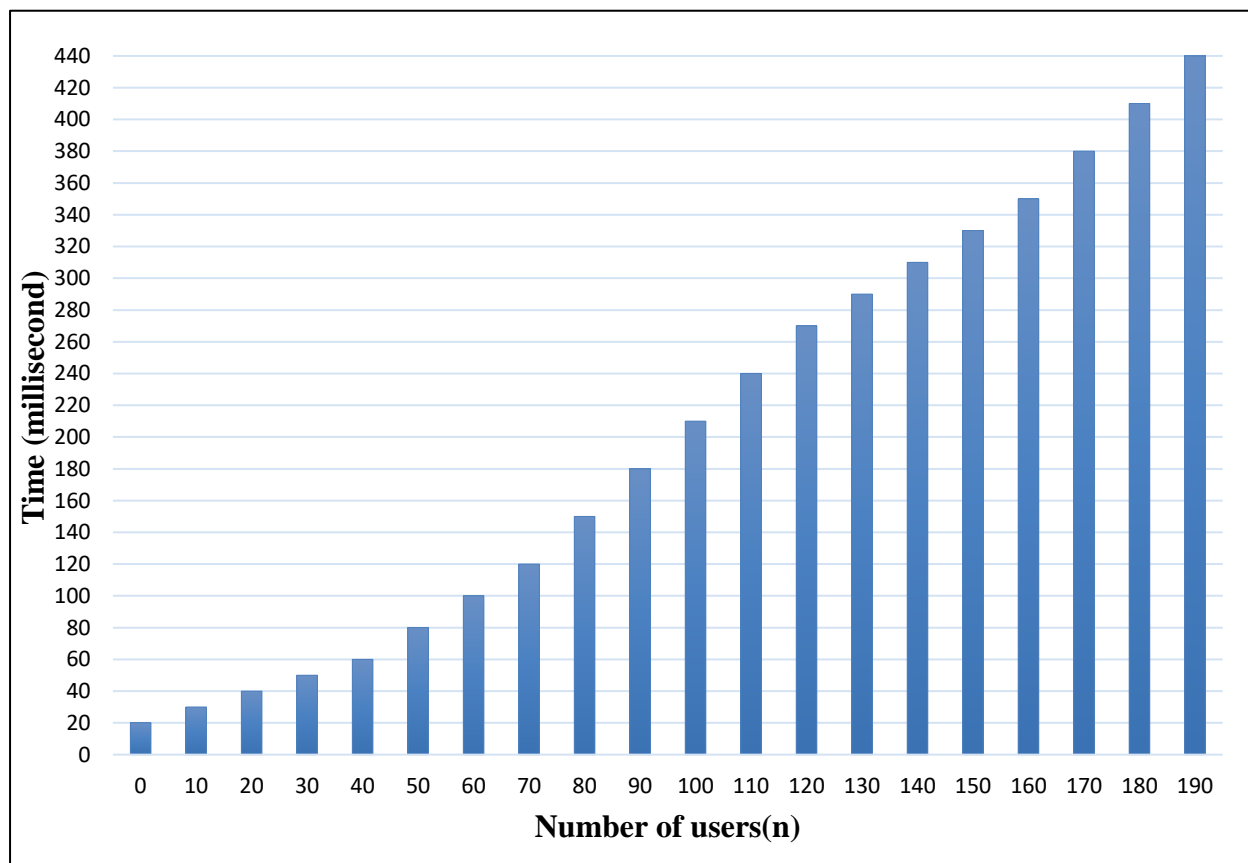


Fig. 4.15 Authentication phase (2)

To evaluate the performance of our system response time for multiple users. The total time for data response time for multiple users is shown Table 4.4. The results of the experiment show that our system is capable of responding to a lot of users in a reasonable response time as shown in Fig 4.16.

Table 4. 4 Data response time

Number of users (n)	Time (millisecond)
10	10
20	20
30	30
40	40
50	50
60	70
70	90
80	110
90	130
100	150

There are one hundred users $n=10$ users requesting 153 bytes of data from data cloud at the same time the response time delay is 10 milliseconds, the data response time is gradually increases because the need to process more requests sequentially. When the number of users $n=60$, 70 milliseconds are needed for requesting and responding the data. Also, we obtain the response time for 100 participants request access data, the time delay is 150 milliseconds.

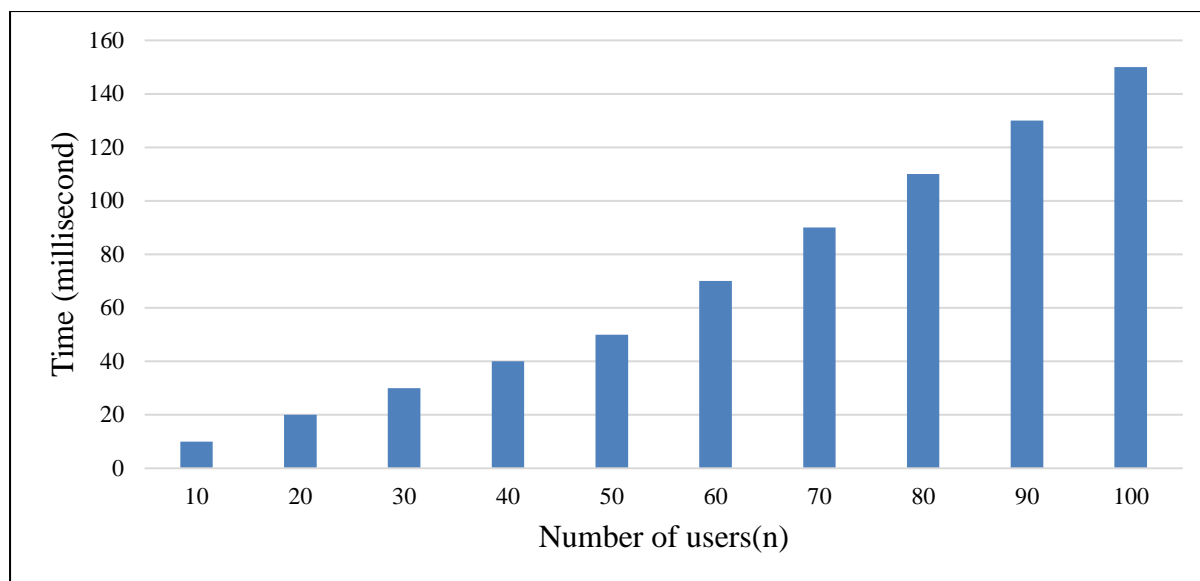


Fig. 4.16: Data response time

4.5 Comparison with other works

The computational time cost refers to the amount of time it takes to execute an algorithm or a set of operations. In order to assess performance of the proposed algorithms, the computational time cost for all the registration, login, and authentication phases are compared with other methods. The outcomes of the computational comparisons between the suggested algorithms and the associated algorithms are shown in Table 4.5.

Table 4.5 Comparison of computational time costs with other related works

Reference	D_R	D_A	D_T
(Yassin et al., 2016)	$5T_h + 2T_{\oplus} + 1T_{\parallel}$	$13T_h + 12T_{\oplus} + 6T_{\parallel} + 2T_{Dec} + 2T_{Enc}$	$18T_h + 14T_{\oplus} + 7T_{\parallel} + 2T_{Dec} + 2T_{Enc} \approx 0.0598$
(Zhang et al., 2017)	$4T_h + 5T_{\oplus} + 5T_{\parallel}$	$18T_h + 27T_{\oplus} + 19T_{\parallel}$	$22T_h + 32T_{\oplus} + 24T_{\parallel} \approx 0.0506$

(Kaul et al., 2020)	$6T_h + 6T_{\oplus}$ $+ 6T_{\parallel} + 1T_{Dec}$ $+ 1T_{Enc}$	$10T_h + 20T_{\oplus}$ $+ 10T_{\parallel}$	$16T_h + 26T_{\oplus}$ $+ 16T_{\parallel} + 1T_{Dec}$ $+ 1T_{Enc} \approx 0.046$
Our system model	$2T_h + 2T_{\parallel}$	$5T_h + 5T_{\parallel}$ $+ 2T_{Enc} + 1T_{Dec}$ $+ 2T_{\oplus}$	$7T_h + 7T_{\parallel} + 2T_{Enc}$ $+ 1T_{Dec} + 2T_{\oplus}$ ≈ 0.035

The process of registering a user in the system only needs to be carried out once for that particular user. After registration, the user's account information and identity are stored in the system for future reference. On the other hand, the login and authentication phases are required to be performed every time the user intends to access healthcare services. These phases are necessary to verify the user's identity and authorization, ensuring that only legitimate users gain access to the system. The proposed algorithms in the comparisons has a great advantage in terms of computational costs (0.035 milliseconds). That is because SSK was created with a very small delay and is not included in any phase, and time for other operations in all phases is very small if compared with other systems as shown in fig 4.17. We see that the suggested system has a fair mix of speed, performance, and security aspects.

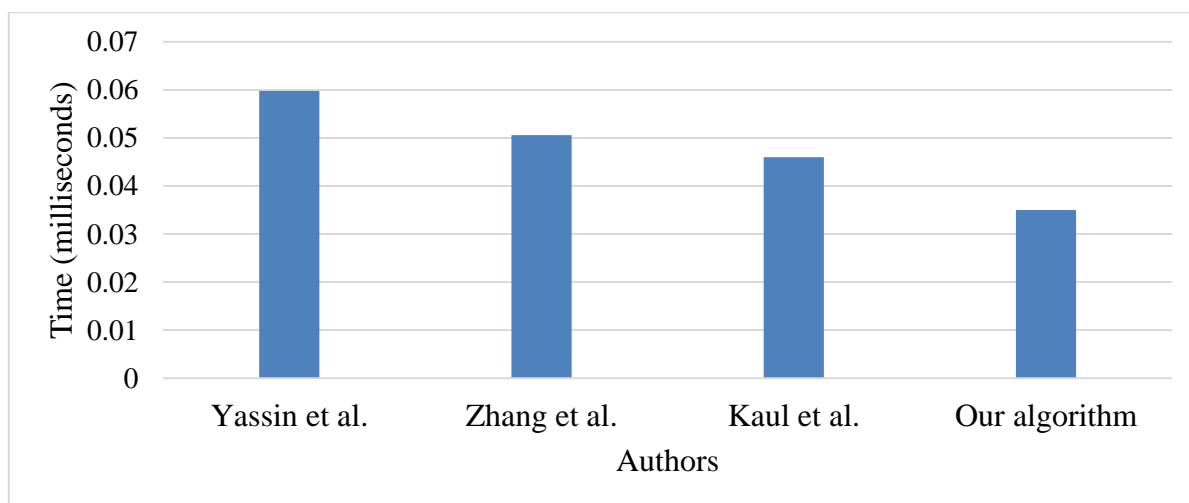


Fig. 4.17: Computation time Cost Comparison

CHAPTER FIVE: CONCLUSION AND FUTURE WORKS

5.1 Introduction

This chapter ends the thesis and summarizes the most significant contributions and discoveries. The first section is the summary of the thesis, while the later section discusses the constraints of the study and presents a list of potential possibilities for further research.

5.2 Conclusion

To ensure the security of E-healthcare based cloud systems, several security measures can be implemented. These include access controls that are used to ensure that only authorized users have access to E-healthcare data. Proposing new algorithm for data access in an E-healthcare based cloud is an important step towards improving the quality and efficiency of healthcare delivery. By reducing delays in accessing patient data, healthcare providers can provide better care and ultimately help to improve the overall health of the population.

We identified that the primary aim of E-healthcare based cloud is security. Therefore, A Generate Access Key (GAK) algorithm is proposed to produce a Security Secret Key (SSK). The GAK would work by providing users with a unique SSK that would be used to allow them when they attempt to access data in the E-healthcare system with the minimum of delay. Users are also given flexible access rights based on their role and rights according to User Access Rights (UAR) algorithm. To protect the privacy of users, the data is encrypted using the Database Encryption (DBE) algorithm before being stored in the database. To read the data in the system by the users the data is decrypted based on Database Decryption (DBD) algorithm.

The algorithms are capable of handling security requirements for allowing valid users to access with a minimum of delay compared with other works. The

design of the system is showed with the use of the proposed algorithms. The performance of our algorithms is simulated, the simulation results show that the delay of authenticate two hundred users is 440 milliseconds, and the data response time is 150 milliseconds for 200 participants requesting data simultaneously. The computational cost was compared with other related works and found that in our algorithms, 0.035 milliseconds were needed for the registration, login, and authentication stages.

5.3 Future Works

E-healthcare systems have become increasingly popular due to their ability to improve patient care and optimize healthcare services. However, there were a number of unresolved concerns that need further investigation in the future. Only the most promising one is highlighted from our perspective. Future research can investigate how the proposed algorithm can be integrated with other emerging technologies, such as blockchain, machine learning and artificial intelligence, to enhance the security and performance of E-healthcare-based cloud systems. These technologies have the potential to improve the overall security and performance of E-healthcare -based cloud systems and can be integrated with the proposed algorithm to achieve even better results.

Research in this field is increasing as lifestyles change and learn towards the fast large and unlimited transfer of data. Searching for new E-healthcare-based cloud theories and algorithms to maintain security and privacy is extremely demanding for production technology companies to be partners, and the future remains open in this area.

REFERENCES

- ABDULMALIK, H. A., YASSIN, A. A. J. B. O. E. E. & INFORMATICS 2023. Secure two-factor mutual authentication scheme using shared image in medical healthcare environment. 12, 2474-2483.
- AGHILI, S. F., MALA, H., SHOJAFAR, M. & PERIS-LOPEZ, P. J. F. G. C. S. 2019. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. 96, 410-424.
- ALZHRANI, A. G. M., ALENEZI, A., MERSHED, A., ATLAM, H., MOUSA, F. & WILLS, G. 2020. A framework for data sharing between healthcare providers using blockchain.
- ARIKUMAR, K., PRATHIBA, S. B., ALAZAB, M., GADEKALLU, T. R., PANDYA, S., KHAN, J. M. & MOORTHY, R. S. J. S. 2022. FL-PMI: federated learning-based person movement identification through wearable devices in smart healthcare systems. 22, 1377.
- AZEEZ, N. A. & VAN DER VYVER, C. J. E. I. J. 2019. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. 20, 97-108.
- CELESTI, A., FAZIO, M., GALÁN MÁRQUEZ, F., GLIKSON, A., MAUWA, H., BAGULA, A., CELESTI, F., VILLARI, M. J. J. O. S. & NETWORKS, A. 2019. How to develop IoT cloud e-health systems based on FIWARE: a lesson learnt. 8, 7.
- CHUMBLER, N. R., KOBBER, R., HARRIS, L., RICHARDSON, L. C., DARKINS, A., SBERNA, M., DIXIT, N., RYAN, P., DONALDSON, M. & KREPS, G. L. J. T. J. O. A. C. M. 2007. Healthcare utilization among veterans undergoing chemotherapy: the impact of a cancer care coordination/home-telehealth program. 30, 308-317.
- CRESSWELL, K., DOMÍNGUEZ HERNÁNDEZ, A., WILLIAMS, R. & SHEIKH, A. J. J. H. F. 2022. Key challenges and opportunities for cloud technology in health care: Semistructured interview study. 9, e31246.

- ESMAEILZADEH, P. & SAMBASIVAN, M. J. J. O. B. I. 2016. Health Information Exchange (HIE): A literature review, assimilation pattern and a proposed classification for a new policy approach. 64, 74-86.
- ESPOSITO, C., DE SANTIS, A., TORTORA, G., CHANG, H. & CHOO, K.-K. R. J. I. C. C. 2018. Blockchain: A panacea for healthcare cloud-based data security and privacy? 5, 31-37.
- FLAUMENHAFT, Y. & BEN-ASSULI, O. J. H. P. 2018. Personal health records, global policy and regulation review. 122, 815-826.
- GUPTA, M., THIRUMALAISAMY, M., SHAMSHER, S., PANDEY, A., MUTHIAH, D. & SUVARNA, N. Patient health monitoring using feed forward neural network with cloud based internet of things. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022. IEEE, 924-931.
- HUANG, Q., YUE, W., HE, Y. & YANG, Y. 2018. Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing. *IEEE Access*, 6, 36584-36594.
- IDOGA, P. E., AGOYI, M., COKER-FARRELL, E. Y. & EKEOMA, O. L. Review of security issues in e-Healthcare and solutions. 2016 HONET-ICT, 2016. IEEE, 118-121.
- JAVAID, M., HALEEM, A., SINGH, R. P., RAB, S., SUMAN, R. & KHAN, I. H. J. I. J. O. C. C. I. E. 2022. Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers. 3, 124-135.
- KAUL, S. D., MURTY, V. K. & HATZINAKOS, D. Secure and privacy preserving biometric based user authentication with data access control system in the healthcare environment. 2020 International Conference on Cyberworlds (CW), 2020. IEEE, 249-256.
- KHAN, F. A., ALI, A., ABBAS, H. & HALDAR, N. A. H. J. P. C. S. 2014. A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. 34, 511-517.

- KHAN, S. & HOQUE, A. J. C. S. J. O. M. 2016. Digital health data: a comprehensive review of privacy and security risks and some recommendations. 71, 273-292.
- KHEZR, S., MONIRUZZAMAN, M., YASSINE, A. & BENLAMRI, R. 2019. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. 9, 1736.
- KIM, E., RUBINSTEIN, S. M., NEAD, K. T., WOJCIESZYNSKI, A. P., GABRIEL, P. E. & WARNER, J. L. The evolving use of electronic health records (EHR) for research. Seminars in radiation oncology, 2019. Elsevier, 354-361.
- KURDI, H., ALSALAMAH, S., ALATAWI, A., ALFARAJ, S., ALTOAIMY, L. & AHMED, S. H. 2019. HealthyBroker: A Trustworthy Blockchain-Based Multi-Cloud Broker for Patient-Centered eHealth Services. 8, 602.
- KUTE, S. S., TYAGI, A. K. & ASWATHY, S. J. I. I. M. S. F. E.-H. A. 2022. Industry 4.0 Challenges in e-Healthcare Applications and Emerging Technologies. 265-290.
- LI, H., YANG, Y., DAI, Y., YU, S. & XIANG, Y. 2020. Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data. *IEEE Transactions on Cloud Computing*, 8, 484-494.
- LIN, H.-Y. & JIANG, Y.-R. 2021. A Multi-User Ciphertext Policy Attribute-Based Encryption Scheme with Keyword Search for Medical Cloud System. 11, 63.
- LÖHR, H., SADEGHI, A.-R. & WINANDY, M. Securing the e-health cloud. Proceedings of the 1st acm international health informatics symposium, 2010. 220-229.
- MAHMOOD, Z. Cloud computing: Characteristics and deployment approaches. 2011 IEEE 11th International Conference on Computer and Information Technology, 2011. IEEE, 121-126.

- MANIKANDAN, N., MUTHAIAH, R., TEEKARAMAN, Y., KUPPUSAMY, R., RADHAKRISHNAN, A. J. S. & NETWORKS, C. 2021. A Novel Random Error Approximate Adder-Based Lightweight Medical Image Encryption Scheme for Secure Remote Monitoring of Health Data. 2021, 1-14.
- MOGHADDAM, F. F., ROHANI, M. B., AHMADI, M., KHODADADI, T. & MADADIPOUYA, K. Cloud computing: Vision, architecture and Characteristics. 2015 IEEE 6th control and system graduate research colloquium (ICSGRC), 2015. IEEE, 1-6.
- MOHAMED, N., AL-JAROODI, J. & ABUKHOUSA, E. 2022. Enabling Healthcare 4.0 applications development through a middleware platform. *Digital Innovation for Healthcare in COVID-19 Pandemic*. Elsevier.
- MOSA, A. S. M., YOO, I., SHEETS, L. J. B. M. I. & MAKING, D. 2012. A systematic review of healthcare applications for smartphones. 12, 1-31.
- NIGAM, D., PATEL, S. N., RAJ VINCENT, P., SRINIVASAN, K. & ARUNMOZHI, S. J. J. O. H. E. 2022. Biometric authentication for intelligent and privacy-preserving healthcare systems. 2022.
- OJO, S., OLUGBARA, O., DITSA, G., ADIGUN, M. & XULU, S. Formal model for e-healthcare readiness assessment in developing country context. 2007 Innovations in Information Technologies (IIT), 2007. IEEE, 41-45.
- OMARY, Z., LUPIANA, D., MTENZI, F. & WU, B. Challenges to E-healthcare adoption in developing countries: A case study of Tanzania. 2009 First International Conference on Networked Digital Technologies, 2009. IEEE, 201-209.
- PELEKOUDAS-OIKONOMOU, F., ZACHOS, G., PAPAIOANNOU, M., DE REE, M., RIBEIRO, J. C., MANTAS, G. & RODRIGUEZ, J. J. S. 2022. Blockchain-based security mechanisms for IoMT Edge networks in IoMT-based healthcare monitoring systems. 22, 2449.

- PENG, Y., CHEN, K., WANG, G., BAI, W., MA, Z. & GU, L. Hadoopwatch: A first step towards comprehensive traffic forecasting in cloud computing. *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, 2014. IEEE, 19-27.
- PINO, C. & DI SALVO, R. A survey of cloud computing architecture and applications in health. *Conference of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)*, 2013. Atlantis Press, 1649-1653.
- SALJI, M. R., UDZIR, N. I., NINGGAL, M. I. H., SANI, N. F. M., IBRAHIM, H. J. I. J. O. A. C. S. & APPLICATIONS 2022. Trust-based Access Control Model with Quantification Method for Protecting Sensitive Attributes. 13.
- SCHIZA, E. C., KYPRIANOU, T. C., PETKOV, N. & SCHIZAS, C. N. 2019. Proposal for an eHealth Based Ecosystem Serving National Healthcare. *IEEE Journal of Biomedical and Health Informatics*, 23, 1346-1357.
- SENGAN, S., KHALAF, O. I., SHARMA, D. K., HAMAD, A. A. J. I. J. O. R. & E-HEALTHCARE, Q. 2022. Secured and privacy-based IDS for healthcare systems on E-medical data using machine learning approach. 11, 1-11.
- SEOL, K., KIM, Y.-G., LEE, E., SEO, Y.-D. & BAIK, D.-K. J. I. A. 2018. Privacy-preserving attribute-based access control model for XML-based electronic health record system. 6, 9114-9128.
- SHAW-SALIBA, K., HANSOTI, B., BURKOM, H., MARTINEZ, D. A., DUVAL, A., LEE, B., CHAU, P., MCBRIDE, B., HSIEH, Y.-H. & SATHANANTHAN, V. J. W. J. O. E. M. 2022. Cloud-Based Influenza Surveillance System in Emergency Departments Using Molecular-Based Testing: Advances and Challenges. 23, 115.

- SUBASHINI, S. & KAVITHA, V. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34, 1-11.
- SUN, Y., ZHANG, J., XIONG, Y. & ZHU, G. J. I. J. O. D. S. N. 2014. Data security and privacy in cloud computing. 10, 190903.
- SUSANTO, H., CHEN, C. K. J. I. O. T. & HEALTHCARE, B. D. T. F. N. G. 2017. Information and communication emerging technology: making sense of healthcare innovation. 229-250.
- TAHER, B. H., WEI, L. H. & YASSIN, A. A. Flexible and efficient authentication of iot cloud scheme using crypto hash function. Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence, 2018. 487-494.
- TAHIR, A., CHEN, F., KHAN, H. U., MING, Z., AHMAD, A., NAZIR, S. & SHAFIQ, M. J. S. 2020. A systematic review on cloud storage mechanisms concerning e-healthcare systems. 20, 5392.
- TARI, Z., YI, X., PREMARATHNE, U. S., BERTOK, P. & KHALIL, I. J. I. C. C. 2015. Security and privacy in cloud computing: vision, trends, and challenges. 2, 30-38.
- TAWALBEH, M., QUWAIDER, M. & LO'AI, A. T. Authorization model for IoT healthcare systems: case study. 2020 11th International Conference on Information and Communication Systems (ICICS), 2020. IEEE, 337-342.
- WEHDE, M. J. I. E. M. R. 2019. Healthcare 4.0. 47, 24-28.
- XIAO, Z., XIAO, Y. J. I. C. S. & TUTORIALS 2012. Security and privacy in cloud computing. 15, 843-859.
- YASSIN, A. A., YAO, J. & HAN, S. J. C. 2016. Strong authentication scheme based on hand geometry and smart card factors. 5, 15.

ZHANG, L., ZHANG, Y., TANG, S. & LUO, H. J. I. T. O. I. E. 2017. Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement. 65, 2795-2805.



Title of Paper:

Authentication and Access Control Model for Healthcare based Cloud Services

Published in:

Journal of Engineering (uobaghdad.edu.iq)

Date of Acceptance: 29 January 2023

Date of publication: 1 March 2023

P-ISSN: 1726-4073

E-ISSN: 2520-3339

Issue: Vol. 29 No. 3

Publisher: Journal of Engineering

Journal Location: Baghdad, Iraq

Paper Link: An Authentication and Access Control Model for Healthcare based Cloud Services | Journal of Engineering (uobaghdad.edu.iq)



Date: 29 / 01 /2023
NO.: 24

**Dear \ Glena Aziz Qadir
Bzar Khidir hussan**

Based on the reviewers' recommendations, I am delighted to inform you that your manuscript entitled:

An Authentication and Access Control Model for Healthcare based Cloud Services

has been accepted for the publication in the Journal of Engineering. It will be published in the upcoming issues.

Your plagiarism percent using Turnitin was (17%)

Thank you for submitting your article to the Journal of Engineering. From all of us at Journal of Engineering, I wish you great success.

We are looking forward to receive more articles in the future.

Best Regards

**Prof. Dr. Karima E. Amori
Editor-in-Chief**

www.joe.uobaghdad.edu.iq
Email: joengbag@uobaghdad.edu.iq
Tel.: 07714076860



An Authentication and Access Control Model for Healthcare based Cloud Services

Glena Aziz Qadir*

MSc. student
Dept. of Information System Engr.
Technical Engineering college
Erbil Polytechnic Univ.
Glena.mei20@epu.edu.iq

Bzar Khidir Hussan

Assist Prof., Ph.D.
Dept. of Information System Engr.
Technical Engineering college
Erbil Polytechnic Univ.
bzar.hussan@epu.edu.iq

ABSTRACT

Electronic Health Record (EHR) systems are used as an efficient and effective method of exchanging patients' health information with doctors and other key stakeholders in the health sector to obtain improved patient treatment decisions and diagnoses. As a result, questions regarding the security of sensitive user data are highlighted. To encourage people to move their sensitive health records to cloud networks, a secure authentication and access control mechanism that protects users' data should be established. Furthermore, authentication and access control schemes are essential in the protection of health data, as numerous responsibilities exist to ensure security and privacy in a network. So, the main goal of our suggested solution is to maintain a secure authentication and access control mechanism for health cloud data. Thus, in this work, Security Secret Key Provider (SSKP) phase is proposed for the E-healthcare-based cloud that consists of two parts. The first is an authentication scheme that is Security Secret Key (SSK) and the second is a modular access control mechanism. We explain the methodology of the proposed approach through appropriate evaluation results, which improves system security and performance by minimizing the time spent to get authentication and access the data. Simulation results indicate that our approach is significantly more effective than existing research.

Keywords: Cloud, Data security, privacy, Authentication, Access control, E-healthcare.

*Corresponding author

Peer review under the responsibility of University of Baghdad.

<https://doi.org/10.31026/j.eng.2023.03.02>

This is an open access article under the CC BY 4 license (<http://creativecommons.org/licenses/by/4.0/>).

Article received: 08/11/2022

Article accepted: 29/01/2023

Article published: 01/03/2023

پوخته

چاودیری تهنروسستی ئهلیکترۆنی وهشانیکی دیجیتالییه له میژووی پزیشکی نهخۆش، که زانیاری ده‌باره‌ی بارودۆخی پزیشکی و چاره‌سه‌ر و ده‌رمانه‌کانیان له‌خۆده‌گریت. چاودیری تهنروسستی ئهلیکترۆنی به‌شیوه‌یه‌کی گشتی له‌لایهن دابینه‌کرانی چاودیری تهنروسستیوه به‌کارده‌هینریت بۆ باشترکردنی کوالیتی چاودیری نهخۆش. سیسته‌می چاودیری تهنروسستی ئهلیکترۆنی نامرازیکی سه‌ره‌کییه که زانیاری هه‌ستیا‌ری نهخۆش له‌خۆده‌گریت و کهوتوته ژیر ریس‌ا تونده‌کانی پاراستنی نه‌ینی و ئاسایشه‌وه. له‌دوای سه‌ر هه‌لدانی کلاود زۆریک له‌دابینه‌کرانی چاودیری تهنروسستی ئیستا زانیارییه‌کانی چاودیری تهنروسستی ئهلیکترۆنی خۆیان له‌سه‌ر سیسته‌می بنهما کلاود هه‌لده‌گرن. گواسته‌وه‌ی داتا‌کانی چاودیری تهنروسستی ئهلیکترۆنی بۆ کلاود ده‌توانیت چه‌ندین ته‌حه‌دای نه‌می بخاته‌روو که ده‌بیت به‌وردی له‌به‌رچاو بگه‌ریت و به‌ریوه‌به‌ریت. به‌کیک له‌نیگه‌رانییه سه‌ره‌کییه نه‌مییه‌کان له‌کاتی گواسته‌وه‌ی داتا‌کانی چاودیری تهنروسستی ئهلیکترۆنی بۆ کلاود، مه‌ترسی ده‌ستر اگه‌شتن به‌زانیارییه‌کانی نه‌خۆشه‌به‌ی مۆله‌ت. کۆنترۆلی ده‌ستر اگه‌شتن پیکه‌ته‌یه‌کی گرنگی سیسته‌می چاودیری تهنروسستی ئهلیکترۆنییه، و دلنیا‌بوون له‌ده‌ستر اگه‌شتن به‌زانیارییه‌کانی نه‌خۆش به‌شیوه‌یه‌کی پارێزراو و گونجاو بۆ پاراستنی ئاسایش زۆر گرنگه. هه‌روه‌ها پاراستنی نه‌ینی بۆ په‌کپارچه‌یی سیسته‌می چاودیری تهنروسستی به‌کۆکردنی داتا‌کان له‌کاتی هه‌لگرنتی له‌کلاود دا. کۆنترۆلی ده‌ستر اگه‌شتن ته‌نها رینگه به‌به‌کاره‌ینه‌رانی رینگه‌پێدراو ده‌دات ده‌ستیان به‌داتا‌کانی تهنروسستی ئهلیکترۆنی بگات. له‌چاودیری تهنروسستی، ده‌ستر اگه‌شتن به‌زانیارییه‌کانی نه‌خۆش له‌کاتی خۆیدا زۆر گرنگه بۆ پێشکه‌شکردنی چاودیری کاریگه‌ر. دواکه‌وتنی کات له‌ده‌ستر اگه‌شتن به‌زانیارییه‌کان ده‌توانیت ببێته‌هۆی ده‌رئه‌نجامی چاوهروانه‌کراو بۆ چاودیری نه‌خۆش که بریتین له‌دواکه‌وتنی ده‌ستنی‌شانکردن و چاره‌سه‌ری نه‌گونجاو. هه‌ر له‌به‌ر نه‌م هۆکاره، دواکه‌وتنی کاتی ده‌ستر اگه‌شتن به‌به‌کاره‌ینه‌ر کهم ده‌بیته‌وه به‌به‌کاره‌ینه‌رانی ئه‌لگۆریتمه‌پێشنیار کراوه‌کان.

له‌م تیزه‌دا ئه‌لگۆریتمی Generate Access Key (GAK) پێشنیار کراوه له‌سه‌ر بنهما‌ی Message Authentication Code (MAC) و ته‌کنیکه‌کانی Hashing بۆ به‌رهمه‌ینه‌نی Security Secret Key (SSK) که کارده‌کات بۆ دابینه‌کردنی SSK بۆ به‌کاره‌ینه‌ران که به‌کارده‌هینریت بۆ ئه‌وه‌ی رینگه‌یان پێدات ده‌ستیان به‌داتا‌کان بگات له‌سیسته‌می کلاودی بنهما‌ی چاودیری تهنروسستی ئهلیکترۆنی به‌که‌مترین دواکه‌وتن. هه‌روه‌ها به‌کاره‌ینه‌ران مافی ده‌ستر اگه‌شتن پێده‌دریت به‌پشتبه‌ستن به‌رۆل و مافه‌کانیان به‌پێی ئه‌لگۆریتمی User Access Rights (UAR). بۆ پاراستنی نه‌ینی به‌کاره‌ینه‌ران، داتا‌کان به‌به‌کاره‌ینه‌رانی ئه‌لگۆریتمه‌ی Database (DBE)

Encryption كۆد دهكرين پيش ئهوهى له داتا بايسه كه دا ههلبگيرين و بو خويندنهوهى له لايهن بهكار هينه رانهوه داتاكانى ناو سيستمه كه دهبيت به پشتبهستن به ئه لگور يتمى (DBD) Database Decryption كۆد بكر يتهوه . ئه نجامى تا قير د نه وهى ئه لگور يتمه كان نيشان ده دن كه دوا كه وتن بو ره سه نايه تى دوو سه د به كار هينه ر ۴۴۰ ميلى چركه ، و كاتى وه لامدانه وهى داتاكان ۱۵۰ ميلى چركه بو ۲۰۰ به شدار بوو كه له يهك كاتدا داواى داتا ده كن . كاتيك بهر اور د ده كريت له گه ل چند تويزينه وه يه كى پيشوو ، كاتى پيوست بو هه موو قوناغه كانى تومار كردن ، و چوونه ژوور موه و قوناغى سه لماندى ياسايى به كار هينه ر كه م ده كاته وه بو ۰،۰۳۵ ميلى چركه .



حكومهتی هه‌ریمی كوردستان – عێراق
سه‌رۆكایه‌تی نه‌نجومه‌نی وه‌زیران
وه‌زاره‌تی خویندنی با‌لا و تو‌یژینه‌وه‌ی زانستی
زانكۆی پۆلیته‌كنیكی هه‌ولێر
كۆلیژی ته‌كنیكی نه‌ندازیاری
به‌شی نه‌ندازیاری سیسته‌می زانیاری

پلانیکی چوونه ژوره‌وه‌ی پته‌و و پارێزراو بو خزمه‌تگوزاریه‌کانی چاودێری ته‌ندروستی له‌ کلاود

پیشکەشی نه‌نجومه‌نی كۆلیژی ته‌كنیكی نه‌ندازیاری كراوه له زانكۆی پۆلیته‌كنیكی هه‌ولێر وه‌كو
به‌شێك له پێداویسته‌یه‌كانی به‌ده‌ست هینانی پله‌ی ماسته‌ر له نه‌ندازیاری سیسته‌می زانیاری

له‌لایه‌ن

گ‌لینه‌ عزیز قادر

به‌كالۆریۆس له نه‌ندازیاری سیسته‌می زانیاری

به‌سه‌ر په‌رشتیاری

ی.پ.د. بژار خ‌ضر حسین

هه‌ولێر- كوردستان

٢٠٢٣ به‌فرانبار