

# A Comprehensive Framework for Ensuring Secure Sharing of Electronic Health Records in AWS Environment

MSc Research Project  
Cloud Computing

Harsha Venkata Naga Vardhan Neerukonda  
Student ID: 22173536

School of Computing  
National College of Ireland

Supervisor:     Vikas Sahni

**National College of Ireland**  
**MSc Project Submission Sheet**



**School of Computing**

**Student Name:** Harsha Venkata Naga Vardhan Neerukonda  
**Student ID:** 22173536  
**Programme:** MSC in Cloud Computing **Year:** Jan 2023  
**Module:** Research Project  
**Supervisor:** Vikas Sahni  
**Submission Due Date:** 14/12/2023  
**Project Title:** A Comprehensive Framework for Ensuring Secure Sharing of Electronic Health Records in AWS Environment

**Word Count:** 6222 **Page Count:** 20

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: N.H.V.N.Vardhan

Date: 14/12/2023

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
<b>Attach a Moodle submission receipt of the online project submission</b> , to each project (including multiple copies).	<input type="checkbox"/>
<b>You must ensure that you retain a HARD COPY of the project</b> , both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

<b>Office Use Only</b>	
Signature:	
Date:	
Penalty Applied (if applicable):	

# A Comprehensive Framework for Ensuring Secure Sharing of Electronic Health Records in AWS Environment

Harsha Venkata Naga Vardhan Neerukonda  
22173536

## Abstract

The adoption of cloud servers for storing and sharing electronic health records (EHRs) offers significant benefits but also raises privacy and security concerns. This thesis proposes a comprehensive framework to enable secure EHR sharing in the AWS cloud environment. The framework utilizes Ciphertext-Policy Attribute Based Encryption (CPABE) and Fernet encryption standard to enforce access control and data confidentiality. It allows patients to define access policies to control which healthcare providers can view their records. EHRs are encrypted under these access policies before storing them in the AWS S3 cloud storage. Only users with matching attributes can decrypt the records. A prototype system is implemented to demonstrate the feasibility of the approach. Additionally, deduplication techniques are incorporated to eliminate duplicate EHRs and optimize cloud storage costs. A file-level chunking method is used to detect identical EHR records. The framework was implemented as a web application using Java and JavaScript. The performance evaluation shows the proposed CPABE system achieves faster encryption/decryption speeds compared to the Fernet algorithm, while fernet provided a better compression ratio compared to CPABE. Overall, the proposed approach balances security, access control, and storage efficiency for sensitive health data shared via the cloud. It gives patients control over their records while enabling seamless access for authorized providers. The integration of CPABE, Fernet and deduplication makes it a comprehensive solution tailored for the EHR environment.

## 1 Introduction

The digitalization of health records has transformed the way healthcare is provided, presenting unparalleled possibilities for data-driven analysis and tailored patient treatment. However, this progress is accompanied by difficulties, especially in guaranteeing the security and confidentiality of electronic health information. Major hospitals utilize electronic health records (EHRs) to preserve patient health information for longer durations. The security and privacy of patient health data are crucial concerns in the healthcare industry, particularly when it comes to sharing files or sensitive information on the cloud. EHR has emerged as an exemplar for medical information that prioritizes the needs and preferences of patients ([Ganiga et al.; 2020](#)). EHR offer patients the autonomy to create, alter, and manage their health records from a single location. EHR systems have facilitated the accessibility, storage, and sharing of medical information such that each patient is guaranteed complete protection of their medical records. The utilization of EHRs has expanded due to the significant rise in cloud computing and the patients' inclination towards technology ([Yang et al.; 2015](#)).

Cloud computing provides an economical solution for distributed computing via the Internet, known for its scalability and cost-effectiveness. The storage and management of Electronic Health Record (EHR) data on cloud servers have become an inevitable and widespread practice. Within the EHR system, individuals can easily upload and access their personal information and medication records from these cloud servers. This approach to storing EHR data on cloud servers enhances medical health management, ultimately resulting in resource conservation and reduced hospital costs ([Dhaka et al.; 2021](#)). Approved EHR users, comprising patients, doctors, and nurses, have exclusive access to the data stored in the cloud servers. Using cloud servers for EHR data management comes with various notable advantages, but it also introduces concerns about the security of data ([Chenthara et al.; 2019](#)). If a unauthorized user manages to access the EHR system without authorization and carries out harmful activities like exposing patients data, it not only breaches patients' privacy but also leads to incorrect diagnoses by doctors with severe consequences.

Hence, it's crucial to clearly define the access control requirements for authorized users allowed to access EHR data. The use of CPABE ensures precise access control over EHR data. The EHR owner sets the access policy, specifying individuals authorized to access the data. After encrypting the data, it's then uploaded to cloud servers. Decryption of the ciphertext is possible only if the attributes of the Electronic Health Record (EHR) user align with the access policy established by the EHR owner. ([Satar et al.; 2021](#)).

Owing to the exorbitant expenses associated with constructing and managing expert data centers, a significant portion of medical computing services, including EHRs, are contracted out to external cloud service providers like Microsoft, Amazon, and others. There exist multiple security strategies that can be employed to safeguard privacy in cloud computing. Nevertheless, the current privacy-preserving systems are inadequate in guaranteeing attribute/role-based access control for users of EHRs. Therefore, this study presents a practical framework that aims to promote privacy by employing a combination of role-based policy and cipher-key attribute-based encryption. The patient data is encrypted prior to being transferred to Amazon cloud servers for safe storage. The storage of encrypted data in the cloud restricts access to authorized individuals, who can only decode the data using a key that is generated based on a role-based policy. The framework endeavours to offer a secure, effective, and secure solution for the coordinated exchange of health data by integrating modern encryption strategies, access control mechanisms, and effective deduplication procedures.

## 1.1 Motivation

The rationale for doing this research arises from the necessity to achieve a nuanced equilibrium between the potential advantages of exchanging electronic health data and the necessity to safeguard patient privacy and maintain data integrity. The growing dependence on cloud platforms, like as AWS, has created a demand for a specialized framework that effectively utilizes the benefits of cloud computing while simultaneously addressing the specific issues presented by the healthcare data environment. The objective of this study is to make an academic contribution to the ongoing discussion on the secure sharing of health data. This will be achieved by presenting a comprehensive framework that not only addresses security threats

but also incorporates deduplication methodologies to enhance the efficiency of data storage and transmission.

## **1.2 Research Problem**

A significant vacuum exists in the market for all-encompassing frameworks that concurrently handle privacy, security, and deduplication issues as healthcare businesses move toward cloud-based solutions for transfer of information and storage. The lack of an organized structure leaves sensitive health data vulnerable to potential attacks and undermines the effectiveness of data storage systems. This research will address the existing gap in knowledge by presenting and verifying an innovative framework that is tailored to address the intricate requirements of secure and privacy-preserving exchange of digital health information inside the AWS environment. The framework also places particular emphasis on the implementation of effective deduplication techniques.

## **1.3 Research Question**

Q: How does the CPABE based EHR framework in comparison to fernet encryption ensures the secure sharing of electronic health data in AWS environment, incorporating efficient deduplication strategies to optimize data storage?

## **1.4 Research Objective**

The objective of this work is to develop and execute a thorough framework that tackles the complex difficulties related to the secure storage and access of EHR data for patients on AWS cloud servers. The proposed framework aims to incorporate effective deduplication techniques in order to enhance data storage efficiency and reduce operating costs. This comprehensive approach seeks to address the inherent challenges associated with healthcare data management.

## **1.5 Research Contributions**

1. Developed and executed a web-based framework that ensures the security and privacy of EHR in the AWS environment.
2. Provided a mechanism for streamlined deduplication process into the proposed architecture in order to enhance the efficiency of both data storage and cloud server costs.
3. A comprehensive evaluation of the EHR framework designed and developed using JavaScript with Amazon S3 storage access permissions.
4. The performance was analyzed by comparing the execution times and compression ratios of CPABE with the symmetric fernet encryption standard.

## 2 Related Work

### 2.1 Electronic Health Data Sharing – Overview

[Sun and Fang. \(2009\)](#) introduced a concept for sharing data across different domains in distributed electronic health record (EHR) systems and this method emphasized exchanging and sharing pertinent patient data securely, using cryptographic techniques to safeguard sensitive information and maintain patient privacy. The EHR system they proposed included sophisticated access control features and a mechanism for revoking access when needed, going beyond the basic controls typically used. [\(Kim et al.; 2017\)](#) conducted a study in California on how consumers will share the electronic health information for healthcare and research purposes. They discovered that attitudes towards EHRs, beliefs about the benefits of research, and the desire for individual control significantly impact this willingness. The study found a decrease in willingness to share health data for healthcare as concerns about privacy, security, and quality increased. Conversely, sharing data for research purposes grew among those who saw EHRs as beneficial for research, valued research benefits over privacy concerns, and prioritized control over research benefits. This research highlights the importance of understanding consumer perspectives in effectively using health data in learning healthcare systems.

[Wang. \(2018\)](#) tackled the challenge of designing a data sharing system for medical/health information that would be secure and private, particularly when using public cloud servers. The proposed solution employed a mix of attribute-based, searchable, and symmetric encryption to ensure anonymity and data confidentiality. This approach included detailed security definitions and models, with potential applications in EHR systems. [\(Xu et al.; 2019\)](#) developed a method for sharing patient health information (PHI) that protects privacy and this system allowed healthcare providers to securely access and search PHI files. The technique enables various types of searches on encrypted data while maintaining privacy. Their tests on real and synthetic data demonstrated the system's effectiveness and privacy protection capabilities. [\(Kim et al.; 2019\)](#) proposed a data sharing scheme for collaborative eHealth systems that protected the privacy of health data owners. The method used local differential privacy (LDP) and attribute-based encryption (ABE) to offer different levels of privacy protection, based on the trust between data owners and users.

### 2.2 Security and Privacy Concerns in Healthcare

[Keshta and Odeh. \(2021\)](#) explored the security features of existing EHR systems, delved into the concerns and challenges surrounding the security and privacy of EHRs, and examined incidents of IT security in healthcare settings. [\(Papageorgiou et al.; 2018\)](#) explained the security and privacy aspects of widely used free mobile health apps, uncovering a concerning trend. The study reveals that scrutinized applications deviate from established security and privacy standards, disregarding legal obligations mandated by data protection regulations. Additionally, the analysis revealed a lack of fundamental privacy safeguards in the reviewed

apps, putting users' sensitive personal information at risk. ([Zhang et al.; 2018](#)) proposed Introduced a smart healthcare privacy-conscious access control system named PASH, which employs a partially concealed access policy and an extensive CP-ABE PASH is distinguished by attributes like safeguarding attribute privacy, conducting efficient decryption tests, supporting expressive access policies, and operating within a vast universe. The article provides an intricate overview of the system and its security model.

[Chenthara et al. \(2019\)](#) explored the security and privacy hurdles associated with e-health solutions in cloud computing through an in-depth examination of diverse privacy-preserving strategies. The comprehensive review encompassed various aspects such as EHR security and privacy requirements for e-health data in the cloud, The authors suggested that future research should concentrate on developing efficient and holistic security mechanisms for EHR, along with investigating methods to uphold the integrity and confidentiality. ([Ozkan et al.; 2019](#)) explored the privacy and security concerns of mobile health record systems among Turkish participants. A survey involving 174 participants, nearly half of whom had undergone genetic testing, uncovered that participant placed their trust exclusively in doctors when it came to their health and genetic information. They expressed a preference for restricting even doctors' access to the records. The study highlighted adverse experiences and apprehensions regarding electronic health records, emphasizing the necessity for regulations and robust security measures before adopting any system.

### **2.3 Cloud-based EHR frameworks**

[Yang et al. \(2015\)](#) introduced a hybrid approach to safeguarding the privacy of data shared in the cloud, integrating statistical analysis and cryptography technologies. This innovative solution facilitates diverse various of health data sharing, each offering varying levels of privacy protection. The comprehensive system consists of four essential components: vertical data partitioning for the publication of medical data, merging data to access medical datasets, integrity checking, and a hybrid search that encompasses both plaintext and ciphertext. A functional prototype system was successfully developed for widespread access and sharing of medical data. ([Qian et al.; 2015](#)) suggested a PHR system that safeguards privacy through multi-authority attribute-based encryption (ABE) featuring revocation. The system enables detailed access control, efficient user/attribute revocation, and dynamic policy updates. Security performance was assessed and compared with other multi-authority ABE schemes, confirming the proposed scheme's success in achieving forward secrecy, data confidentiality and fine-grained access control.

[Zhuang et al. \(2020\)](#) Timely exchange of health information among different healthcare systems comes with significant advantages, such as cost reduction, enhanced care quality, and strengthened disease surveillance. Nevertheless, diverse Health Information Exchange (HIE) models present challenges related to data quality, security, privacy concerns, patient engagement, and maintaining patient privacy. The authors have introduced a patient-focused HIE framework utilizing blockchain technology. This framework safeguards data security and patient privacy, ensures data authenticity, and empowers patients with full access to their health

data. Smart contracts are employed to facilitate data segmentation, establishing an "allowed list" for clinicians to access patient data and achieving a patient-centric HIE. The feasibility, stability, security, and robustness of the framework were evaluated through a comprehensive large-scale simulation conducted by the authors. ([Xhafa et al.; 2015](#)) suggested a user-accountable multi-authority ciphertext-policy attribute-based encryption (ABE) scheme for crafting a privacy-conscious system facilitating the sharing of personal health records (PHR) in cloud computing. The devised system enables the tracking of the identity of a PHR user in case of decryption key exposure, ensuring accountability for both authorities and users.

[Deng et al. \(2018\)](#) suggested a groundbreaking CP-OABSC algorithm, designed to alleviate computational burden on PHR users by seamlessly integrating 'signature then encryption' with outsourcing technology for PHR systems. The approach not only ensures verifiable outsourcing designcrypton but has also been validated for correctness and security, showcasing its efficiency in comparison to alternative ABSC schemes. ([Zhang et al.; 2019](#)) suggested a novel encryption technique for Personal Health Records (PHRs), enabling concealed ciphertext policies and rapid decryption. Unlike CP-ABE, which explicitly included access policies with encrypted PHR data, our proposed method achieved comprehensive security in the standard model under static assumptions, thanks to the utilization of the dual system encryption approach. ([Yang et al.; 2020](#)) proposed a secure method for sharing medical data by integrating attribute cryptosystems and blockchain technology. The strategy is a combination of attribute-based encryption and signature techniques to ensure privacy and authenticity. Additionally, the approach outsourced decryption operations to enhance computational efficiency. Upon evaluation, it successfully met confidentiality and unforgeability criteria, demonstrating superior computational performance compared to similar methods.

## **2.4 Deduplication in Cloud Computing**

[Xu et al. \(2019\)](#) designed a framework that includes safe deduplication, access pattern privacy protection, and privacy protecting attribute-based access control into the fundamental element of the revocable CPABE approach. It featured a safe deduplication method built on the suggested access control paradigm, as well as an improved Path-ORAM access protocol to enable write access on encrypted data and privacy-preserving access policy updates. The framework was evaluated and compared the security and performance issues with the existing solutions. ([Ma et al.; 2019](#)) introduced a modified version of an attribute-based encryption scheme designed to facilitate efficient deduplication and attribute revocation within eHealth systems. Leveraging the inherent properties of prime numbers, the scheme aimed to optimize storage space utilization and securely share medical records. Through a comprehensive security analysis, the authors demonstrated that the proposed approach meets the necessary security requirements. Additionally, visual experiment results underscored the outstanding performance of the technique in achieving deduplication and attribute revocation functionalities.

[Mageshkumar et al. \(2023\)](#) implemented a hybrid cloud storage system for secure data deduplication that utilized convergent encryption, block-level deduplication, and the Diffie-Hellman algorithm for end-to-end encryption and data privacy. The proposed system aimed to

improve data security and efficiency in cloud-based document search. ([Malathi and Suganthidevi.; 2021](#)) presented a comparative study of data deduplication techniques for cloud computing storage. The study analyzed the challenges of performing data deduplication on encrypted data and proposed a methodology for secure data deduplication. The proposed methodology focused on encryption-based secured data sharing and key management systems to ensure safe sharing of PHI in the cloud and prevent redundant data. ([Benil and Jasper.; 2023](#)) proposed an approach utilizing blockchain technology to secure the outsourcing of medical data in a cloud environment. The method involved employing the Enhanced Map Chaotic Encryption algorithm for encryption, implementing data deduplication through the Tri-Level Chunk Hashing technique, and ensuring integrity validation through a third-party auditor. Notably, every action related to outsourcing Electronic Health Records (EHRs) was documented as a transaction on the public blockchain. The authenticity of these transactions was guaranteed through registration, and secure access to the data was facilitated using a keyword search mechanism.

### 3 Research Methodology

This section details the research methodology. The primary objective of this project is to enhance the security and confidentiality of e-health solutions operating in the cloud. Ciphertext-Policy Attribute Based Encryption (CPABE) is utilized to enforce data security. CPABE employs authorization attributes and user identification to encrypt sensitive information, thereby limiting access to it. Access to data is limited exclusively to individuals listed in the permissions roster, thereby safeguarding confidential information from external parties. Deduplication techniques are employed to optimize storage capacity. Unique records are archived. Nevertheless, if a file contains repetitive data, it will be ignored, thereby releasing essential storage capacity. The integration of CPABE with deduplication yields a secure and efficient system for protecting patient data. This system ensures both secrecy and privacy, while optimizing the utilization of storage capacity. The healthcare sector greatly benefits from this strategy due to its strong focus on security and efficiency. Members of the medical organization, including doctors, nurses, and pharmacists, initiate a login request to access the system. The system then conducts a thorough access control check, leveraging the Access Broker Unit to verify the users' authenticity. Following any modifications made by the user to a particular field, the system employs Attribute Based Encryption (ABE) Unit to encrypt the updated information within the accessed Electronic Health Record (EHR) fields. This unit extracts the user's characteristic permissions, while the Key Generation Unit provides the necessary encryption keys using the advanced encryption standard (AES).

**A. Access Broker:** This is centered on Attribute Based Access Control (ABAC), with its core components being the Access Broker, which includes the knowledge base, rule-based engine, and policy unit. The knowledge base stores extensive details about entities linked to the medical organization, presented as electronic health data records. Meanwhile, the policy

unit hosts access policies aligned with the organizational confidentiality policy. The rule-based engine employs semantic web rules to enforce confidentiality regulations and make access control decisions. These decisions are based on user and document attributes retrieved from access policy records.

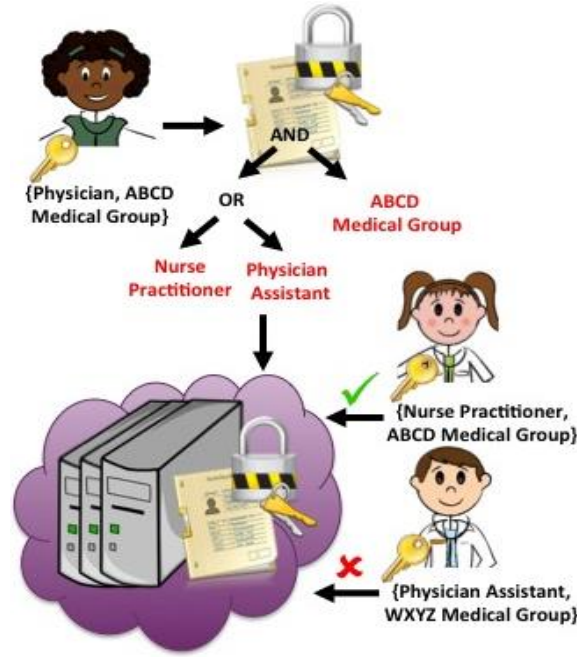
**B. Attribute-based Encryption Unit:** This module is centered on the concept of Attribute-Based Access Control (ABAC). Within the Access Broker, three key sub-modules play integral roles: the knowledge base, the rule-based engine, and the policy unit. The knowledge base stores extensive information on entities linked to the medical organization, preserved as electronic health data records. The policy unit manages access policies derived from the organizational confidentiality policy. Leveraging semantic web rules, the rule-based engine enforces confidentiality regulations to guide access control decisions. These decisions are based on user and document attributes extracted from access policy records.

**C. EHR on Cloud:** The EHR database is a HIPAA-compliant storage system that houses all user and EHR attributes in the form of a knowledge graph. This document provides an analysis about the responsibilities and characteristics of the various personnel inside the medical organization, such as doctors, nurses, and lab technicians. Additionally, it explores the interconnections and dynamics among these individuals. Additionally, it contains the patient's information, medical records, consultations, prescriptions, and drugs. The AWS S3 storage is a publicly accessible cloud storage repository offered by Amazon. The cloud service provider hosting the EHR database receives the encrypted data.

## 4 Design Specifications

### 4.1 CPABE Encryption Implementation

The CP-ABE method enables healthcare providers to utilize a single public key for encryption, eliminating the need for a public key infrastructure (PKI). However, every medical professional possesses a unique secret key for decrypting the patient records. CP-ABE enables the specification of intricate policies that determine which secret keys are capable of decrypting specific ciphertexts. Each secret key belonging to a healthcare provider is assigned a set of attributes, while ciphertexts are linked to access policies. Only a health-care provider whose key's attribute set meets the access policy linked with a ciphertext can decrypt it using their secret key, as depicted in Figure 1. At the ABCD Medical Institution, nurse practitioners have exclusive access to electronic health records (EHRs) that are restricted to physician assistants and nurse practitioners employed by the institution. However, the physician assistant from the WXYZ Medical Group does not have permission to view these records.



**Figure 1. CPABE Encryption Process**

The CPABE process involves four crucial steps: Setup, Encrypt, Key Generation, and Decrypt. The setup algorithm takes the implied security parameter as input and produces public parameters PK and a master key MK. The key generation algorithm, using the master key MK and a set of attributes A, defines the key, resulting in the creation of a private key AK.

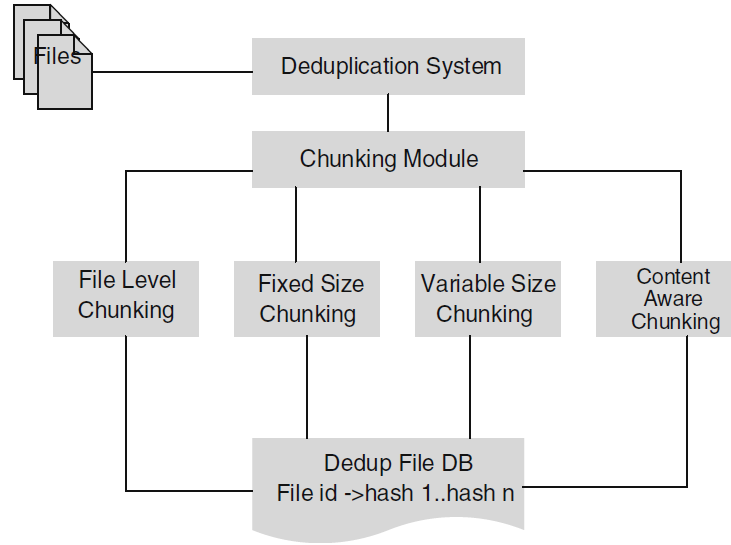
Encryption (PK, M, AP): The encryption process involves using public parameters PK, a message M, and an access policy AP, which is defined based on a set of characteristics. During encryption, the message M is transformed into ciphertext CT. However, only users possessing the specific attributes outlined in the access policy structure will have the ability to decrypt CT.

Decryption (PK, CT, SK): The decryption process involves taking the public key (PK), a ciphertext (CT) associated with an access policy (AP), and a private key (SK) corresponding to a set (A) of attributes. If the attributes within set A fulfill the criteria of the access structure AP, the method proceeds to decrypt the ciphertext, yielding the message (M) as the final output.

In healthcare, CPABE provides a versatile and intricate access control system. It empowers healthcare professionals to retrieve specific Electronic Health Records (EHRs) encrypted with access policies aligned with their key properties. In case of a compromised secret key, only EHRs encrypted with that specific key would be vulnerable, ensuring the security of others.

## 4.2 Deduplication Module

Data deduplication is a nascent technique that aims to decrease storage usage and improve data replication management in cloud storage environments. Deduplication technique involves the fragmentation of data into smaller units known as "chunks," each of which is assigned a distinct hash number. These identifiers are employed for comparing the chunks with previously saved chunks and authenticating their duplication.

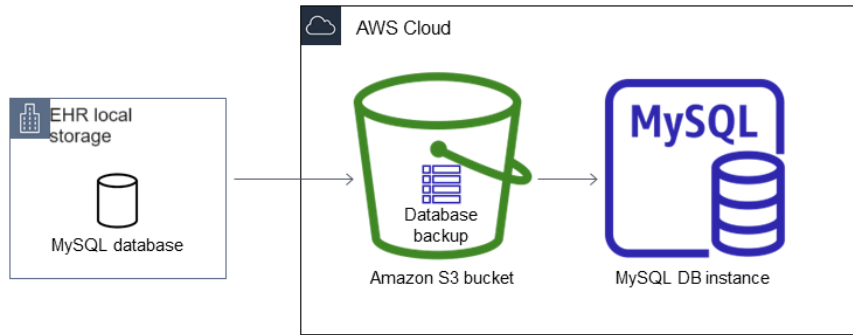


**Figure 2. File-level Chunking Deduplication Module**

This study used file-level chunking, which treats a whole file as a single chunk, instead of dividing files into smaller pieces, as depicted in Figure 2. This method involves the creation of a single index for the entire file, which is then compared to the existing indices of the entire file that have already been stored. This methodology utilizes a single index for the entire file, resulting in a reduced number of index values. Consequently, it conserves space and enables the storage of a greater quantity of index values compared to alternative methods. It minimizes the overhead of looking for metadata and reduces CPU utilization to the utmost extent. Furthermore, it decreases the time required for the index lookup procedure and minimizes the input/output operations for every chunk. Nevertheless, this approach becomes ineffective when only a minor segment of the file is modified. Instead of determining the index specifically for the modified sections, it calculates the index for the entire file and relocates it to the backup location. However, this is not a significant issue for the specific application of an EHR database, as patient records are generated during registration and their information is not routinely altered. The newly generated records from doctor consultations are preserved as distinct entities that are not linked to the existing patient data.

### 4.3 AWS Storage Configuration

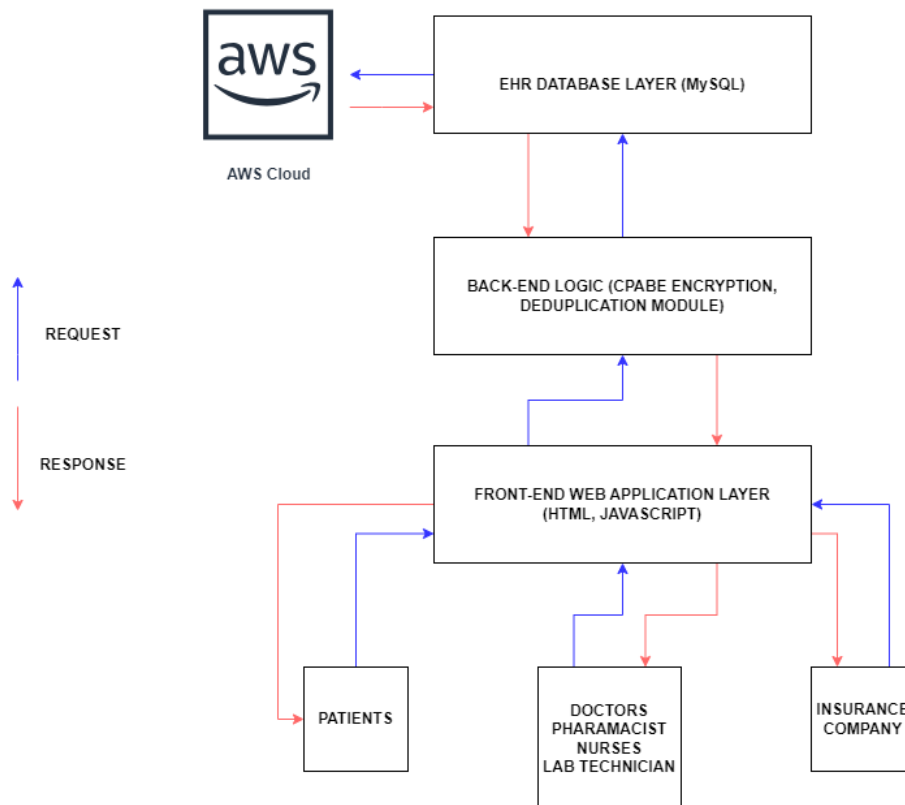
Amazon S3 manages data in an archive that offers durability, high availability, and minimal delay, as well as enhanced durability. In AWS S3, the fundamental components are things organized within buckets. Every object is identified by a distinct key that is supplied by the user. Buckets can be accessed using the AWS S3 console, using the AWS SDK framework. Figure 3 presents the process of storing the locally stored EHR database to the AWS S3 storage bucket where it is stored as a MySQL DB instance. Applications will be authorized by utilizing the access control list associated with each item in the bucket.



**Figure 3. AWS Cloud S3 Storage Access**

## 5 Implementation

The proposed web-based EHR system will consist of three distinct layers as in Figure 4: the application front-end, the backend logic, and the EHR database. The Front-end layer refers to the visually appealing online interface that is accessible to end users through any internet browser. It relies on the HTML5 and JavaScript library. The back-end layer serves as the



**Figure 4. Proposed EHR Implementation**

intermediary between the front-end and database layer. The software was implemented using the Java programming language. The database layer is responsible for storing all the data received from the front-end and implemented using MySQL.

The system is designed for managing Electronic Health Records (EHRs) within a cloud-based framework, accessible via a web portal for stakeholders. The onus of formulating access protocols rooted in the attributes of certified healthcare practitioners, encrypting EHRs as per these policies, and uploading the encrypted data to the cloud rests with the EHR creators. The EHRs are organized in a tiered system with labels, facilitating selective sharing of EHR components, thus adding to the system's adaptability. The framework employs two main cloud services: data storage and processing capabilities. The primary service involves storing the encrypted EHRs, accessible exclusively by healthcare professionals through rigorous authentication processes and access policies that reflect the healthcare providers' comprehensive attributes. The secondary service includes managing the web portal, generating access policies, and conducting other essential computational tasks. Once healthcare professionals are assigned specific access attributes in their accounts, they can sign in using their credentials. At their initial login, a healthcare provider can request access to a secured record. If authorized, they can see a list of patient data they are permitted to view, in accordance with the assigned access policy attributes. For adding new records, the user will seek the necessary attributes and formulate the access policy utilizing the Access Policy Engine. The data will be encrypted at the backend using CPABE, and the encrypted record will be stored in the MySQL database. A deduplication module is incorporated into the backend system to monitor file modifications using the chunking technique, ensuring that no duplicate versions of the same record are stored in the EHR database. The record can be automatically posted to the AWS S3 storage whenever there is a modification in the database. In addition to CPABE, the python implementation of Fernet algorithm for encryption is also presented in this work to make a direct comparison with the CPABE algorithm in terms of speed and compression ratio. With Fernet, the interaction commences by generating a non-standard encryption key, which is subsequently employed to encode the patient data stored as a dictionary. Prior to being uploaded to an Amazon S3 bucket, the encrypted data undergoes compression using the zlib library. The compression ratio and size calculations offer valuable insights into the efficacy of the compression process. The script receives the compressed data from the S3 storage service, decompresses it, and subsequently decrypts it using the identical Fernet key during the download process.

## 6 Experimental Results

### 6.1 User Interface Demo



Figure 5. New User Registration

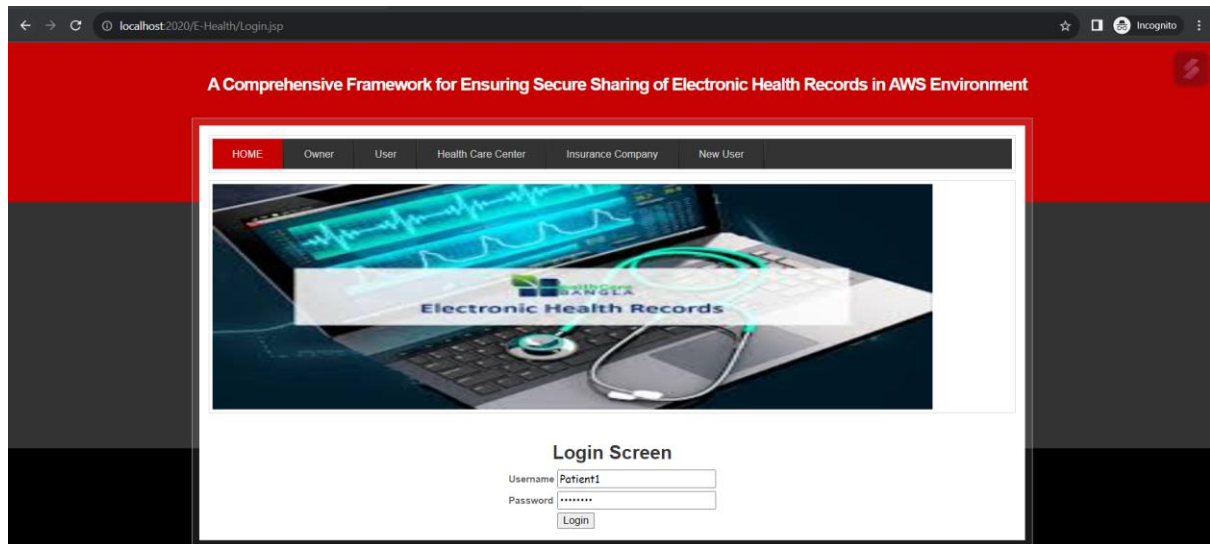


Figure 6. Login Screen

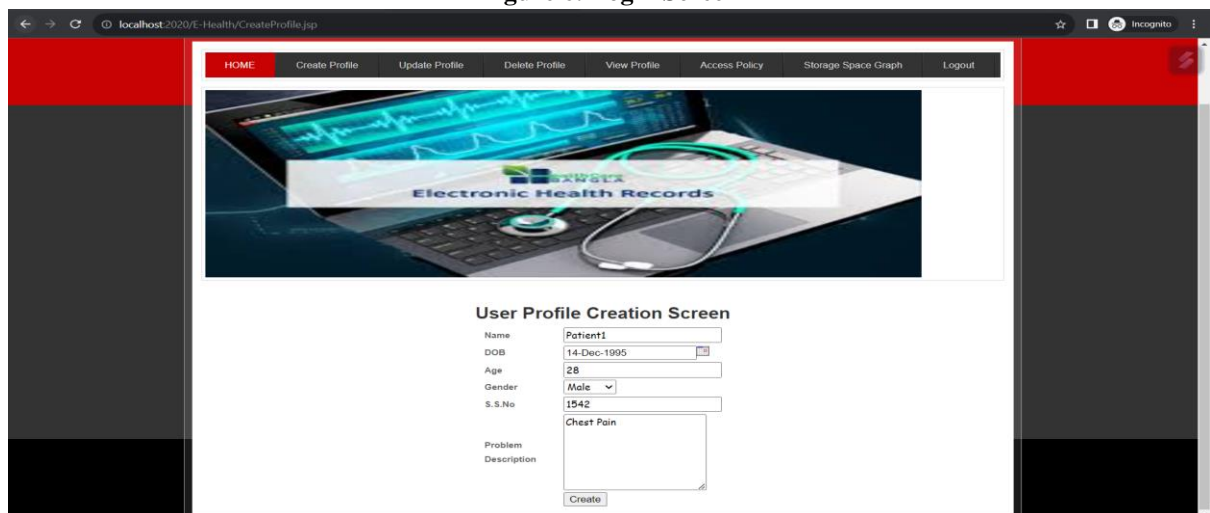


Figure 7. User Profile Creation

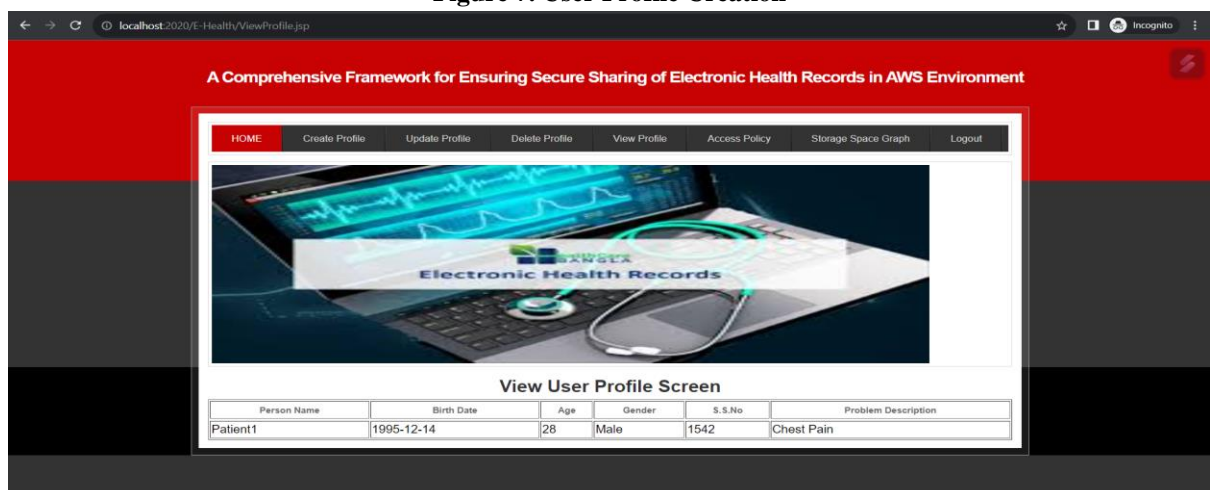


Figure 8. View User Profile

**Access Policy Screen**

Friends Access: friend  
 Access File: Personal Information  
 Physician Access: Doctor  
 Access File: Medical History  
 Nurse Access: Nurse  
 Access File: Medical History  
 Lab Technician Access: lab  
 Access File: Medical History  
 Insurance Company Access: Insurance  
 Access File: Medical History  
 Submit

**Figure 9. Access Policy Creation**

**Login Screen**

Username: Doctor  
 Password: \*\*\*\*\*  
 Login

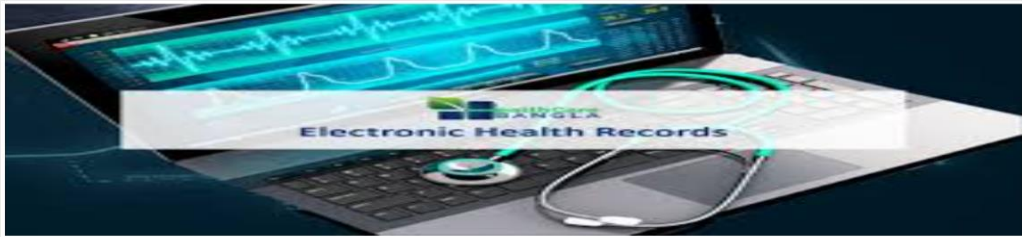
**Figure 10. Login Screen with Access Policy Restrictions (Doctors, Nurses, Lab)**

**View User Profile Screen**

Person Name	Birth Date	Age	Gender	S.S.No	Problem Description	Prescription
Patient1	1995-12-14	28	Male	1542	Chest Pain	Prescription

**Figure 11. Doctor Access – Patient User Profile**

[View Personal Profile](#)
[View Medical Profile](#)
[Logout](#)



### Prescription Screen

Doctor


Patient Name

Physician Name

Prescription

Figure 12. Doctor Access – Prescribe Medicines Screen

[View Personal Profile](#)
[View Medical Profile](#)
[Logout](#)



### View Medical Profile Screen

Patient Name	Physician Name	Prescription Details	Date
Patient1	Doctor	Take Anacin tablet and go for the X-Ray	2023-12-08

Patient Name	Nurse Name	Patient Condition	Date	Blood Pressure	Respiratory Rate	Heart Rate	Pulse Rate
Patient Name	Lab Technician Name	Test Name	Results	Report Name	Date	View Report	

Figure 13. Doctor Access – Medical Profile Screen

[View Personal Profile](#)
[View Medical Profile](#)
[Logout](#)



### Add Patient Condition Screen

Nurse

Patient Name

Nurse Name

Blood Pressure

Respiratory Rate

Heart Rate

Pulse Rate

Patient Condition

Figure 14. Nurse Access – Add Patient Checkup Information

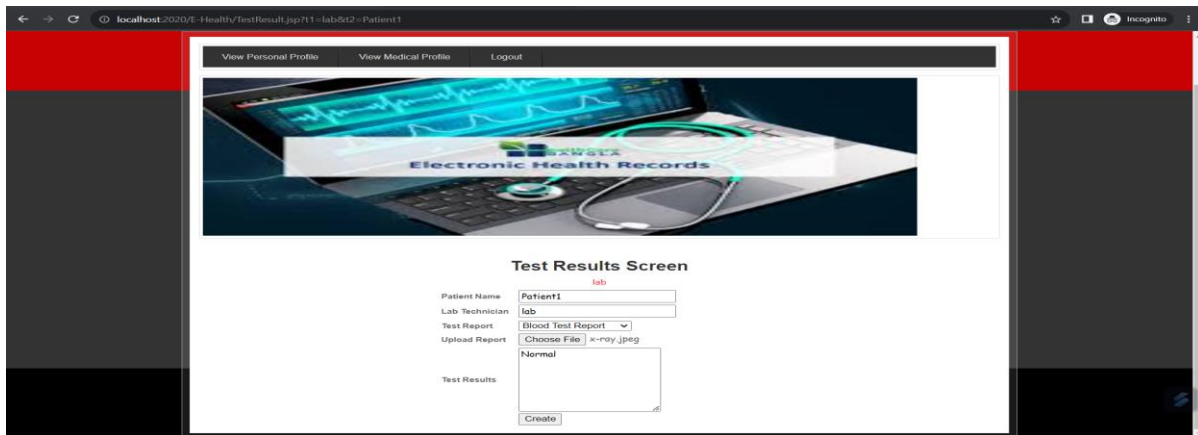


Figure 15. Lab Personnel – Test Reports Upload Screen

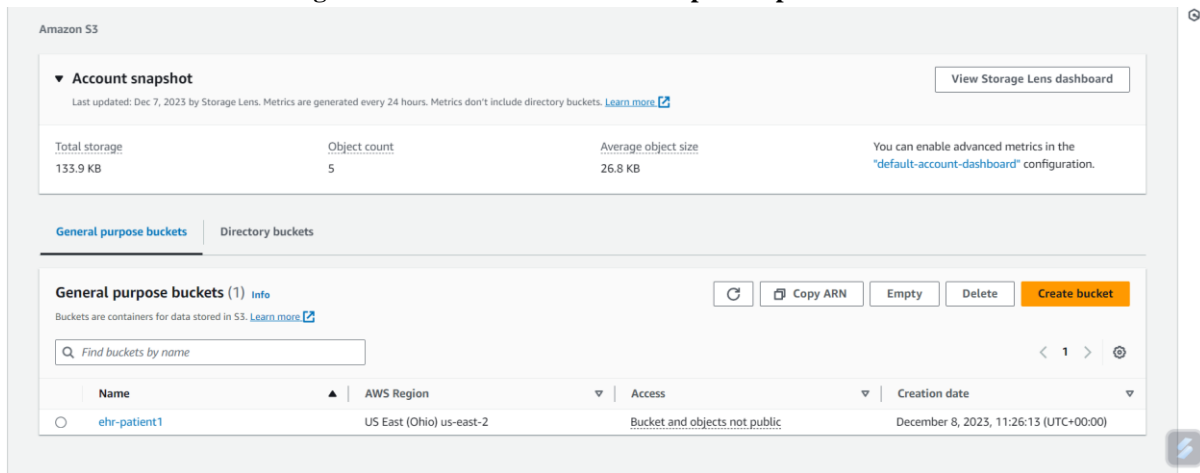


Figure 16. AWS S3 Storage – Bucket Creation

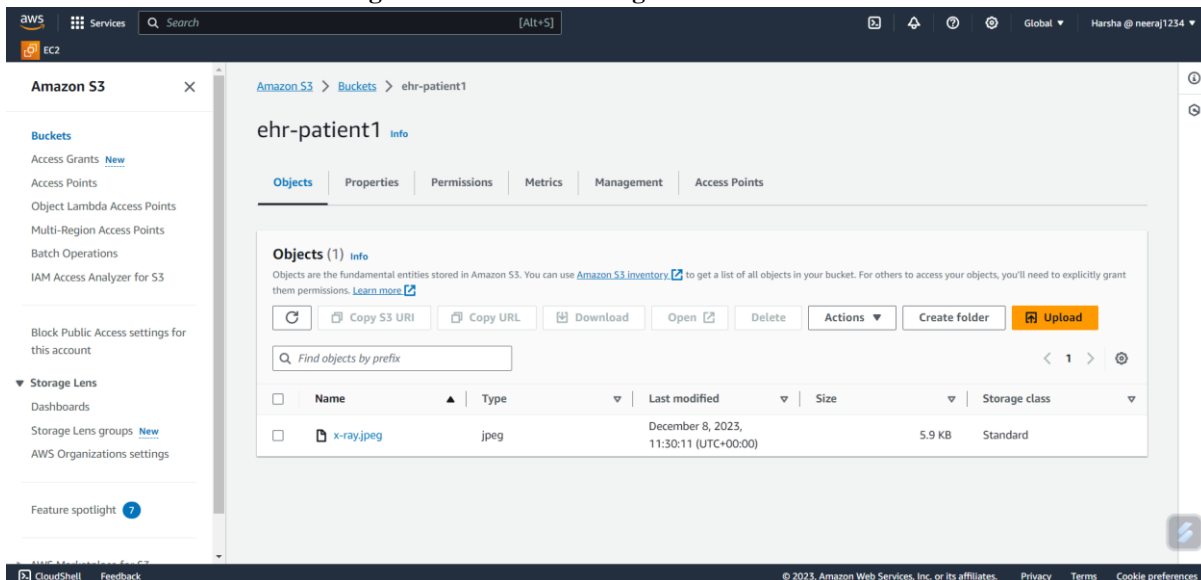


Figure 17. AWS S3 Storage – Files uploaded and stored in bucket

## 6.2 Performance Evaluation

This study utilizes the Fernet algorithm, a robust and efficient symmetric key encryption technique, which is a part of the cryptography package in Python, to evaluate its performance against the proposed CPABE algorithm. Comparison between the proposed CPABE algorithm with Fernet Symmetric encryption algorithm will be presented in terms of execution time and compression ratio. CPABE involves encoding information based on specific attributes, and only users with corresponding attributes can decrypt the information. The arranging stage generates a CPABE event, producing random attributes for the public and private keys. The key age process involves generating client-specific keys by combining random secret values with derived components from public keys, and verifying authenticity by SHA-256 hashing. The encryption process acquires patient information based on a predetermined access method, resulting in the production of ciphertext components. Decryption, conversely, employs the ciphertext and the user's key to reconstruct the original communication.

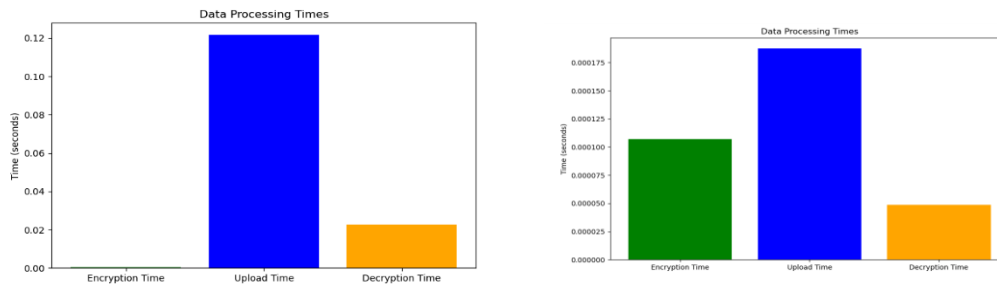


Figure 18. Comparison of encryption, decryption and upload times of Fernet (left) and CPABE (right).

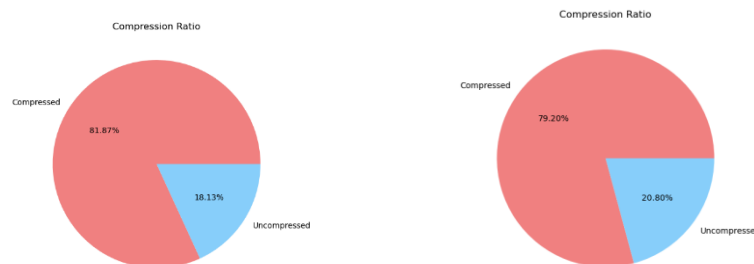


Figure 19. Comparison of compression ratios of Fernet (left) and CPABE (right).

From Figure 18, it can be inferred that the proposed CPABE algorithm upload time is far lesser than Fernet in the order of magnitude 100. The encryption and decryption times of CPABE were also better than Fernet making it the appropriate choice for securing data in the cloud where faster access speeds are important. The compression ratios are compared in Figure 19, with the proposed CPABE providing a slightly lesser compression ratio than Fernet (79.20% vs 81.87%). But this is overcome by the faster encryption and decryption times with a small overhead in terms of storage space size.

## 7 Conclusion

This research signifies a substantial advancement in tackling the crucial obstacles of safe EHR data sharing. The framework showcases a strong solution for protecting EHR by utilizing advanced cryptographic algorithms like CPABE and Fernet on the AWS cloud. Attribute-Based Encryption (CPABE) guarantees precise access control, permitting just authorized

personnel to decode and access certain health records according to established qualities. The web-based application front-end was successfully implemented, showcasing the real-time functionality of the entire EHR platform. The performance of CPABE was also compared to the Fernet algorithm to establish its superiority in terms of encryption-decryption speeds and compression ratio. This system offers a framework for enterprises to improve data security, comply with regulations, and enable safe cooperation in the rapidly growing digital healthcare industry. If this framework is effectively implemented, it has the potential to enhance patient care, foster greater confidence in health systems, and facilitate the smooth sharing of health information among authorized stakeholders.

## References

Benil, T. and Jasper, J., 2023. Blockchain based secure medical data outsourcing with data deduplication in cloud environment. *Computer Communications*, 209, pp.1-13.

Carter, G., Shahriar, H. and Sneha, S., 2019, July. Blockchain-based interoperable electronic health record sharing framework. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)* (Vol. 2, pp. 452-457). IEEE.

Chenthara, S., Ahmed, K., Wang, H. and Whittaker, F., 2019. Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, 7, pp.74361-74382.

Deng, F., Wang, Y., Peng, L., Xiong, H., Geng, J. and Qin, Z., 2018. Ciphertext-policy attribute-based signcryption with verifiable outsourced designcryption for sharing personal health records. *IEEE Access*, 6, pp.39473-39486.

Dhaka, M., Sharma, D.P., Sharma, S.K. and Dixit, A., 2021, December. An Analysis of Electronic Health Record System in Healthcare Services in Cloud: A Review Perspective. In *2021 International Conference on Computational Performance Evaluation (ComPE)* (pp. 886-892). IEEE.

Elghoul, M.K., Bahgat, S.F., Hussein, A.S. and Hamad, S.H., 2023. Management of medical record data with multi-level security on Amazon Web Services. *SN Applied Sciences*, 5(11), p.282.

Ganiga, R., Pai, R.M., MM, M.P. and Sinha, R.K., 2020. Security framework for cloud based electronic health record (EHR) system. *International Journal of Electrical and Computer Engineering*, 10(1), p.455.

Joshi, M., Joshi, K. and Finin, T., 2018, July. Attribute based encryption for secure access to cloud based EHR systems. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)* (pp. 932-935). IEEE.

- Keshta, I. and Odeh, A., 2021. Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, 22(2), pp.177-183.
- Kim, J.W., Edemacu, K. and Jang, B., 2019. MPPDS: multilevel privacy-preserving data sharing in a collaborative eHealth system. *IEEE Access*, 7, pp.109910-109923.
- Kim, K.K., Sankar, P., Wilson, M.D. and Haynes, S.C., 2017. Factors affecting willingness to share electronic health data among California consumers. *BMC medical ethics*, 18, pp.1-10.
- Ma, H., Xie, Y., Wang, J., Tian, G. and Liu, Z., 2019. Revocable attribute-based encryption scheme with efficient deduplication for ehealth systems. *IEEE Access*, 7, pp.89205-89217.
- Mageshkumar, N., Swapna, J., Pandiaraj, A., Rajakumar, R., Krichen, M. and Ravi, V., 2023. Hybrid cloud storage system with enhanced multilayer cryptosystem for secure deduplication in cloud. *International Journal of Intelligent Networks*.
- Malathi, P. and Suganthidevi, S., 2021, September. Comparative study and secure data deduplication techniques for cloud computing storage. In *2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSSES)* (pp. 1-5). IEEE.
- Özkan, Ö., Aydin Son, Y.E.Ş.İ.M. and Aydinoğlu, A.U., 2019. Security and privacy concerns regarding genetic data in mobile health record systems: an empirical study from Turkey. *bioRxiv*, p.678912.
- Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A. and Patsakis, C., 2018. Security and privacy analysis of mobile health applications: the alarming state of practice. *Ieee Access*, 6, pp.9390-9403.
- Qian, H., Li, J., Zhang, Y. and Han, J., 2015. Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation. *International Journal of Information Security*, 14, pp.487-497.
- Satar, S.D.M., Hussin, M., Hanapi, Z.M. and Mohamed, M.A., 2021. Cloud-based secure healthcare framework by using enhanced ciphertext policy attribute-based encryption scheme. *Int. J. Adv. Comput. Sci. Appl*, 12, pp.393-399.
- Sun, J. and Fang, Y., 2009. Cross-domain data sharing in distributed electronic health record systems. *IEEE Transactions on Parallel and Distributed Systems*, 21(6), pp.754-764.
- Wang, H., 2018. Anonymous data sharing scheme in public cloud and its application in e-health record. *IEEE Access*, 6, pp.27818-27826.

Khafa, F., Feng, J., Zhang, Y., Chen, X. and Li, J., 2015. Privacy-aware attribute-based PHR sharing with user accountability in cloud computing. *The Journal of Supercomputing*, 71, pp.1607-1619.

Xu, C., Wang, N., Zhu, L., Sharif, K. and Zhang, C., 2019. Achieving searchable and privacy-preserving data sharing for cloud-assisted e-healthcare system. *IEEE Internet of Things Journal*, 6(5), pp.8345-8356.

Xu, R., Joshi, J. and Krishnamurthy, P., 2019. An integrated privacy preserving attribute-based access control framework supporting secure deduplication. *IEEE Transactions on Dependable and Secure Computing*, 18(2), pp.706-721.

Yang, J.J., Li, J.Q. and Niu, Y., 2015. A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generation computer systems*, 43, pp.74-86.

Yang, X., Li, T., Pei, X., Wen, L. and Wang, C., 2020. Medical data sharing scheme based on attribute cryptosystem and blockchain technology. *IEEE Access*, 8, pp.45468-45476.

Zhang, L., Hu, G., Mu, Y. and Rezaeibagha, F., 2019. Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system. *IEEE Access*, 7, pp.33202-33213.

Zhang, Y., Zheng, D. and Deng, R.H., 2018. Security and privacy in smart health: Efficient policy-hiding attribute-based access control. *IEEE Internet of Things Journal*, 5(3), pp.2130-2145.

Zhuang, Y., Sheets, L.R., Chen, Y.W., Shae, Z.Y., Tsai, J.J. and Shyu, C.R., 2020. A patient-centric health information exchange framework using blockchain technology. *IEEE journal of biomedical and health informatics*, 24(8), pp.2169-2176.