

Attribute-Based Encryption and Key Agreement Protocol for Data Security in EHR Systems

MSc Research Project
Cloud Computing

Murphy Elo
Student ID: x21220263

School of Computing
National College of Ireland

Supervisor: Rashid Mijumbi

National College of Ireland
Project Submission Sheet
School of Computing



Student Name:	Murphy Elo
Student ID:	x21220263
Programme:	Cloud Computing
Year:	2023
Module:	MSc Research Project
Supervisor:	Rashid Mijumbi
Submission Due Date:	14/08/2023
Project Title:	Attribute-Based Encryption and Key Agreement Protocol for Data Security in EHR Systems
Word Count:	6412
Page Count:	17

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:	
Date:	18th September 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission , to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project , 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.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Attribute-Based Encryption and Key Agreement Protocol for Data Security in EHR Systems

Murphy Elo
x21220263

Abstract

Data security in Health Information Exchange (HIE) plays a vital role in ensuring continuous protection and consistency of patient data throughout its lifetime in the system. Specifically, unauthorized access, continuity of data protection, and secure communication for interoperability and interactions between external systems have become challenging problems for Electronic Health Record (EHR) systems. Existing approaches focus on blockchain and attribute-based encryption mechanisms as solutions. While these approaches have succeeded in providing suitable access control mechanisms, they don't fully address the re-encryption of modified data by authorized users in EHR systems. Also, a secure communication channel for interactions with external systems is needed. The proposed algorithms in this research work provide a robust solution that extends the Attribute-Based Encryption (ABE) for continuous encryption of patient data after modification requests. It also leverages the Elliptic Curve Diffie-Hellman (ECDH) for secured communication with external systems or applications. A proof of concept EHR system and mobile application have been developed for evaluation. The result shows the efficiency of the proposed algorithms to provide continuity and secure communication for an attribute-based EHR system.

1 Introduction

The use of Health Information Exchange (HIE) technology has become a crucial part of the sharing of health information electronically among healthcare entities to improve patient care and outcomes HIE (2023). Over the years, we have seen the implementation of HIE systems developed through several system solutions like Electronic Health Records (EHR), Electronic Medical Records (EMR), and Personal Health Records (PHR) systems. While these systems offer diverse and customized solutions to large and small hospitals, unauthorized access to patient data and continuous data protection of modified value have posed significant challenges.

Research has been done to solve these challenges. Some research works such as Joshi et al. (2018), Kaliyaperumal and Sammy (2022), Alabi et al. (2022) have used Attribute-Based Encryption (ABE) techniques where access to patient's data is defined by attributes and access policies in these EHR systems. However, little effort has been made to address the re-encryption of modified patient data when there is a new change. Consider an attribute-based EHR system where attributes have been defined for a doctor user and access given to patient data X. The doctor modifies the patient data, and the system

encrypts it. As the data is updated, the database sees the updated data as plaintext and not as an encrypted continuity value. This will lead to the discontinuation of encryption to achieve data security in the system. Seh et al. (2020). Moreover, the lack of a secure channel for interaction with external systems has had its share of these challenges. Verizon (2022) has reported that 76% of breaches in the healthcare industry were a result of basic web application attacks, miscellaneous errors, and system intrusion when interacting with external services.

To address these gaps, this research proposes to develop a data modification algorithm that extends an attribute-based EHR system to foster continuous data protection. The proposed algorithm uses the Charm framework to perform the Ciphertext - Attribute-Based Encryption (CP-ABE) operations. The algorithm leverages the granular access control and encryption mechanism provided by CP-ABE to re-encrypt patient data after modification.

For secured communication with external systems and applications, a key agreement algorithm is proposed using the Elliptic Curve Diffie-Hellman (ECDH). This will establish secure communication between the mobile application and the EHR system for retrieval of encrypted patient records.

Research Question:

- How can the algorithmic process of a data modification scheme, implemented through Attribute-Based Encryption (ABE), and the integration of the Elliptic Curve Diffie-Hellman (ECDH) protocol enhance data security and provide secured communication in Electronic Health Record (EHR) systems respectively?

The objectives of the research paper include:

- Developing a data modification algorithm using Attribute-Based Encryption (ABE) to enhance data security in EHR systems.
- Developing a key agreement algorithm with the Elliptic Curve Diffie-Hellman (ECDH) to provide secure communication between the mobile app and the EHR system developed.

By leveraging these two protocols, the proposed solution provides an efficient data security solution for attribute-based EHR systems. For evaluation, a prototype EHR system and a mobile app are built to implement the algorithms proposed in this research work.

This paper discusses existing approaches in Section 2. Section 3 describes the research methodology and design specification used in this research. The implementation of the research is detailed in Section 4. Section 5 discusses the evaluation results. Section 6 provides the conclusion and the future work of this research.

2 Related Work

This section aims to examine and critically analyze existing approaches that have been used to tackle the challenges of continuity of data protection and secure communication in EHR systems.

2.1 Attribute-Based Encryption Approach

This research work by Joshi et al. (2018) proposes an Attribute-Based Encryption (ABE) protocol that extracts user field attributes to verify users requesting access to patient data. The proposed methodology includes the organizational knowledge base as an ontology that contains the data of all users, a policy unit that manages the access policies, and the rule-based engine that implements access control decisions based on the policies developed. In their data modification approach, the system encrypts and stores modified values by an authorized user as a new node in the EHR ontology. Storage of modification requests as new nodes is the limitation of this approach. This will create duplication of the same data. This research, Sun et al. (2011) focuses on satisfying the following requirements: privacy, failover, data integrity, access control, accountability, confidentiality, and availability. To do this, they proposed an HCPP (Healthcare system for Patient Privacy) EHR system. This system's approach uses cryptography and wireless network technology to provide satisfaction to their focused requirements. The premise of their method involved restricting access to authorized entities in the proposed system through Identity-based cryptography (IBC), Searchable Symmetric Encryption (SSE), and Searchable Public-Key Encryption (SPKE) schemes. Also, in any case of data breaches or modifications, the involved entity can be traced through the IP address in the associated Local Area Network (LAN) where the entity resides. Shynu and Singh (2017) proposed another application of attribute-based encryption for health systems. A trap function built on attribute-based searchable encryption is developed. The trap function acts as an intermediary key to the original collected by the BAN networks. When the encrypted data is changed, the trap function performs encryption computation on the patient data to prevent unauthorized access to the data. Additionally, a three-factor mutual authentication is developed for authenticating data users. This research Shrestha et al. (2016) proposes a multi-authority attribute-based encryption framework to provide fine-grained access control in a PHR system. A Data Access Requester (DAR) requesting access to data is granted access to decrypt data if only the access policy generated by the patient is satisfied. Access policy responsibility is within the patient entity, which can lead to data insecurity if there is a data breach on the patient's side.

Walid et al. (2021) focused their research work on attribute revocation and data searchability in a cloud-based EHR system. They have proposed a semantic access control scheme that uses Attribute-Based Encryption (ABE) and Semantic Web Technology. Their approach involves developing a robust encryption model to revoke unwanted user attributes and facilitate a faster keyword search of patient data in cloud-based EHR systems with big data. The model is sectioned into two modules: Authentication and Data Processing Module. The first module handles authorization and access control mechanisms. The second module handles revocation, data modification, and searchability functionalities. A proof of concept via an EHR software application is developed to evaluate the proposed EHR framework. Kaliyaperumal and Sammy (2022) proposed a novel multi-attribute-based model using Attribute-Based Encryption (ABE) protocol. In their approach to solving access control, multiple users governed by attributes, can have access to patient health records. The patient records are encrypted before moving them to the servers. The model divides the type of users into two protective domains: Public domain (PUD) and Personal domain (PSD). Each of the domains has a controlling ABE scheme: A novel multi-authority scheme for the PUD; and a revocable key policy attribute for the PSD. Implementation is simulated using CloudSim Simulator. Their

research work reveals that the proposed method is more secure and scalable than previous attribute-based methods. However, the proposed model does not involve a real-time implementation.

To provide data security, this research work by Ganiga et al. (2020) proposes an attribute-based encryption protocol that regenerates access policies when there is a modification. The access policies associated with a patient record are redefined for continuous data security. Elavarasan and Veni (2020) focused on data sharing and attribute revocation for a cloud-based EHR system. They have proposed an enhanced secure data sharing scheme with Efficient Revocation (ESDE) to provide enhanced security. In their evaluation, they compared their proposed scheme with Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Hur's framework scheme. Their results showed that their proposed scheme is more efficient in providing multi-authority access control to cloud-based EHR systems. These researchers Alabi et al. (2022), proposed a multilevel security framework that focuses on privacy and security within local and cloud EHRs. Their approach involves providing encryption to patient data at the local hospital level using the Advanced Encryption Standard (AES) algorithm, and the Elliptic Curve Cryptography (ECC) algorithm for the cloud-based EHR system. Patient health data entering into an on-premise system of a local hospital is first encoded with AES. The key generated from the AES encoding is further encrypted with the ECC encryption when moving the data record to the cloud, thereby achieving multilevel security with both systems. The model is evaluated with existing ECC systems and their results showed high performance in providing privacy for patient data. While this model provides security, it does not provide an access control and data modification mechanism based on who should have access and modify data.

2.2 Blockchain Approach

The approach used in this research paper Liang et al. (2017) focused on achieving health data integrity by incorporating a proof of integrity and validation mechanism within each record inputted into the system. Their approach involves developing a decentralized access control permission management protocol and identity management through blockchain's membership service. When a new data entry is hashed and uploaded to the blockchain network, a proof of integrity and validation mechanism is carried out through identity management. Access is granted from the data owner through a decentralized permission management protocol. Evaluation of the proposed system is done by carrying out integrity-proof generation and validation tests to check for low latency and data processing efficiency. The limitation of this approach is the cost in terms of its scalability. As the number of data records and users increases, the size of the computational resources required by the blockchain also grows significantly.

Ajayi et al. (2020) proposed a shared EHR system with each healthcare provider maintaining their health data on a private Hyperledger Fabric blockchain network platform. These private networks interact with each other to exchange patient health information based on peer and specific requests. The proposed solution detects any inconsistency in all the associated blockchain networks by actively detecting any malicious activities stored and shared. The smart contract acts as the agreement point for all the participants involved to validate transactions and blocks. The result involves detecting malicious attacks by insiders or outsiders within the shared healthcare system. While this approach uses blockchain, each healthcare system in the network maintains its own records centrally,

which can introduce a single point of failure. This research work proposes a Patient-Centric Healthcare Framework (PCH) developed using Hyperledger Fabric blockchain technology Gohar et al. (2022). The method proposed used the blockchain platform to intercept and retrieve the data generated from all entities in the different healthcare systems associated with the framework. It consists of a 5-tier architecture built on the Hyperledger Fabric blockchain platform, with each layer having separate functionalities.

2.3 Blockchain with Other Approaches

Nguyen et al. (2021) proposed an approach that leverages edge-cloud technology and blockchain's smart contract for data offloading and data integrity respectively. A four-layer architectural system within the blockchain network is proposed which consists of an IoT layer, an edge layer responsible for managing IoT devices and processing the health data, and a cloud layer for storing processed health data. The blockchain consensus validation ability is used to provide data synchronization and replication capabilities across the cloud entities for consistency of data. Verification and detection of unauthorized access are done by the validation algorithm. Performance metrics are based on access control, network overheads, and execution time for data offloading. Consensus validation is needed every time the network has to validate access. It is costly to maintain, and it introduces delays, a drawback that can impact real-time decision-making in healthcare. These researchers Wang et al. (2018) proposed a robust framework that combines Interplanetary File System (IPFS), Ethereum blockchain, and attribute-based encryption (ABE) technologies. In their approach, Interplanetary File System (IPFS) is used to provide a decentralized storage model where the nodes in the system do not have to be dependent on each other. The Attribute-based Encryption (ABE) part of the approach provides access control privileges for the Data Owner (DO) over their data, with the choice to choose whom they can distribute secret keys (Data Users). The Ethereum blockchain algorithm provides key management functionalities, enabling data users to retrieve secrets to perform operations on associated data. Although the approach proposed is robust, it can be complex, and ensuring data consistency in the system can require significant effort from data owners and data users.

This research work by Cao et al. (2019) proposed a model to protect outsourced Electronic Health Records (EHRs) systems from unauthorized modifications using blockchain technology. The approach is that every data modification operation performed by an authenticated participant is recorded as a transaction in the blockchain network, and cannot be altered after the transaction is hashed. The system architecture consists of four algorithms: setup, appointment, store, and audit. Every patient's entry is encrypted by the doctor using a treatment key from the patient during the initial appointment. Authentication and validation are done with a corresponding private key when there is a new data modification operation. The operation is recorded as a transaction and cannot be altered after entry to the cloud storage server. The result showed that the average time for confirming a transaction was approximately 3 minutes. For a patient with multiple doctors, the time interval increases. The increase in data transactions in the blockchain can lead to a larger blockchain size and time delay in processing. Mahdy (2021) proposed a semi-centralized cloud-based EHR system implemented on a client-server centralized system and a P2P decentralized system. A central node serves as a message broker to govern and regulate data propagation and user access to the data within the network. Patient consent is achieved through digital signatures via blockchain. To evaluate the

proposed architecture, a proof of concept prototype is developed with a web server acting as the governing node.

2.4 Other Approaches

This research proposed a patient-centered framework giving patients total control of access to their information. The approach consists of two servers for implementation: an authentication server to authenticate credentials, and an access control list(ACL) server for verifying provided credentials. Healthcare entities require permission from patients to access data. For data modification awareness, a notification mechanism is implemented to notify patients of logged-in healthcare entities Vimalachandran et al. (2017).

Rini et al. (2020) focused on achieving data integrity and authorization in cloud-based EHR systems using a QR-code algorithm. An authorized admin uploads patient data to the cloud storage via a mobile application. The data is stored and encrypted in the database with the QR code algorithm. This method provides basic encryption and decryption for associated health data, but the security of the mobile application is not robust enough in the case of preventing unauthorized access. Hanif et al. (2023) research focused on using a genetic-based hashing algorithm for securing and validating health data in a decentralized system. The presented model includes the blockchain system, cryptographic hashing for surveillance of the integrity of patient data in the system, and a Genetic Algorithm (GA) for key generation. The researchers have based their choice of using GA because of its randomness in enhancing the cryptographic hashing process. The random results generated are called chromosomes. The incorporation of GA introduces randomness, making the encryption process more unpredictable and secure. The evaluation is measured against other non-GA blockchain EHR systems in terms of data security, immunity, scalability, and robustness. In multi-systems that involve external interactions between each system, the Elliptic-curve Diffie–Hellman (ECDH) protocol can be used to provide secure communication between systems. This research work leverages ECDH to provide a secured gateway between the patient’s identification and the doctor’s authentication of the patient’s data. A Keyed-Hash Message Authentication Code (HMAC) is introduced to provide confidential communication between patient records and authenticated users Rivero-García et al. (2017).

From the literature review discussed, proposed research works that address data insecurity have been classified into different approaches. The solutions proposed in these approaches focus on providing initial data protection for EHR systems through attribute-based encryptions and blockchain technologies. Little has been done to provide continuous data protection after modification requests have been made. Implementation of a secure channel to provide external communication with third-party services has not been carried out. It is important to address these gaps given that frequent modifications and external interactions are made regularly in an EHR system.

A novel data modification algorithm is proposed to provide continuous data protection for Attribute-Based EHR systems. Furthermore, a key agreement algorithm is proposed to provide secured communication between EHR systems and third-party systems or applications. The proposed algorithms will provide an efficient data security solution for EHR systems.

3 Methodology & Design Specification

A working explanation and workflow of each of the algorithms is discussed in this section. While each of the algorithms works independently in its function, the application of both provides an efficient data security framework for attribute-based EHR systems.

3.1 Data Modification Scheme

A data modification rule for continuous data protection is introduced in an attribute-based EHR system. The rule is based on three parameters: M , T , and D .

Let U be the set of authorized users (doctors) with $U = \{u_1, u_2, \dots, u_n\}$, and attributes as $A = \{u_1, u_2, \dots, u_n\}$,

Let P be the set of patients with $P = \{p_1, p_2, \dots, p_m\}$.

Let F be the original set of EHR fields with $F = \{f_1, f_2, \dots, f_x\}$.

Let M be the set of modified EHR fields in the patient records with $M = \{m_1, m_2, \dots, m_k\}$.

Let T be the set of timestamps for the modifications with $T = \{t_1, t_2, \dots, t_l\}$.

Let CD be the database table for storing the modification details.

- **addModification:** Given authorized user, U with access attribute to patient record, P . For each modification event that occurs in an EHR field, F of a patient, P , the system creates an attribute-value pairing, associating the modified event with a timestamped proof of data, T . The event is encrypted as a modified value in the database. This is expressed mathematically as:

$$D \leftarrow D \cup M\{(u_1, p_1, f_1, t_1)\}$$

- **Enc(ModifiedData):** Before storage takes place in the database the original EHR field, F , is encrypted into a ciphertext as a modified value, $enc(M)$. The process is expressed mathematically as:

$$enc(M) = M\{(u_1, p_1, f_1, t_1)\}$$

Where, $enc(M)$ represents the encrypted ciphertext value of the Modified field, M .

The continuity value of the original EHR field, F at any time is protected and secured as one single entity in the database.

3.1.1 Workflow of the Data Modification Scheme

Figure 1, shows the workflow of the data modification process. Firstly, authentication checks are performed using the access control provided by the attribute-based encryption protocol, in which the system extracts attributes specific to the user to have access to the original data record. In our use case, the doctor is an authorized user, and the username is the attribute specific to the doctor user. Secondly, the original field modified by the

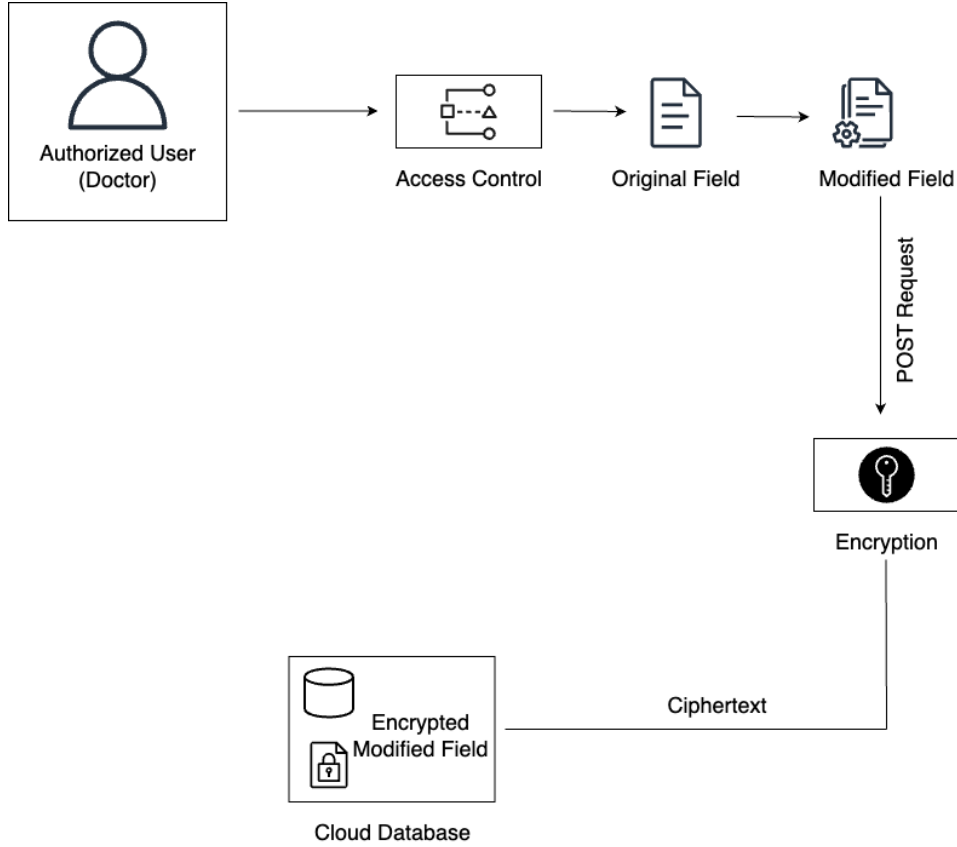


Figure 1: Workflow Process for Data Modification Scheme

authorized user is sent as a JSON payload to the encryption framework which will provide the encryption keys to perform the encryption on the modified EHR field as a ciphertext. Thirdly, the modified encrypted field is stored in the database as a continuity value for the specific patient record. Every modified encrypted EHR field value is made the most recent modification, creating a timestamped proof of any data change.

3.2 Secure Communication Scheme

External communication with a mobile app will require that a secure channel be established to protect the patient's health data. Given two parties, S , and PA , where S is the EHR system, and PA is the mobile app. To protect patients' health data during communication, an ECDH key agreement protocol is used between the systems.

KeyCreate: The initial phase in the protocol is the generation of public keys for the EHR system ($Pub_C S$) and the mobile app ($Pub_P A$). Given an Elliptic Curve E defined over a finite field F_p . The elliptic curve is represented given by a Weierstrass equation Schoof (1985):

$$y^2 = x^3 + ax + b \pmod{p}$$

Where, a and b are constants, and p is a large prime number that defines the finite field.

Setup: Select a base point G on the elliptic curve E , which has a large prime order n . The base point is a fixed point on the curve with a specific order n , meaning that at every point G repeatedly adds itself to n times, the cyclic property of the base point is identified. This is expressed as:

$$n \cdot G = O$$

Where n is prime order of the base point, G , and O is the cyclic property identified

Considering S as *Party A*, and PA as *Party B*, the private key for each of these parties is randomly chosen as a positive integer that is less than the order n of the base point. The private key is represented for Party A as (Pri_S) , and the private key for Party B as (Pri_{PA}) .

Key Exchange: Party A computes $Pub_S = Pri_S * G$. Party B computes $Pub_{PA} = Pri_{PA} * G$. The public keys are points on the elliptic curve obtained by multiplying the base point G with the respective private keys. During this key exchange process, the patient app sends its public key, Pub_{PA} to the cloud server.

Agreement: The EHR system computes the shared secret by multiplying its private key with the received public key from the patient app. The patient app computes the shared secret similarly by multiplying its private key with the received public key from the EHR system. These are expressed as:

$$\begin{aligned} SharedSecretKey &= Pri_S * Pub_{PA} \\ SharedSecretKey1 &= Pri_{PA} * Pub_S \end{aligned}$$

3.2.1 Workflow of the Secure Communication Scheme

Figure 2, shows the workflow of the secure communication process. Firstly, a cryptographic key pair, consisting of a private key and a corresponding public key is generated on the server end using elliptic curve cryptography (ECC) - ECP256R1. The server receives the public key from the mobile app (client) and performs the computation to generate a shared secret. A Key Derivation Function (KDF) is initialized to derive a 32-byte (256-bit) symmetric key from the shared secret provided. The encryption process starts when an Initialization Vector (IV) is initialized which results in the provision of a random value to prevent unauthorized decryption. A cipher object is created using the derived key and the IV (random value provided). An encryptor is created from the cipher object, which will be used for encrypting the data to prevent eavesdroppers from intersecting the data record.

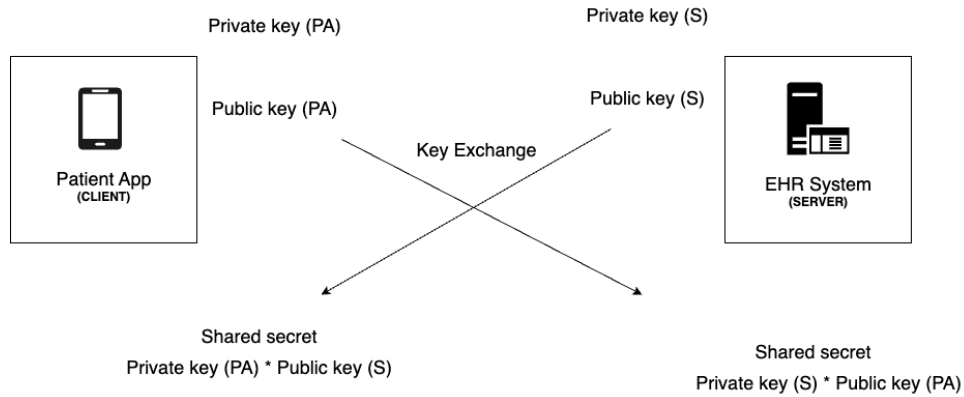


Figure 2: Workflow Process for Data Modification Scheme

On the client's end for decryption, a cryptographic key pair is also generated, comprising a private key and a corresponding public key, using the same elliptic curve used by the server. The mobile app receives the public key of the server. The KDF derives a 32-byte (256-bit) symmetric key from the shared secret. The same Initialization Vector (IV) is used during the encryption. It's crucial that the IV used for decryption matches the IV used for encryption. A Cipher object is created for AES using the derived key and IV. A decryptor is created from the Cipher object, which will be used for decrypting the ciphertext into a human-readable string.

3.3 System Requirements

To carry out this research work, the following system requirements and applications have been used:

- Docker 4.21.1 for running Django and Flask containers
- Python 3.37 to run Charm's framework on Flask for Ciphertext - Attribute-Based Encryption (CP-ABE) protocol.
- Python 3.10 for the EHR system on Django
- Kivy 2.2.1 for developing the mobile app.

4 Implementation

The EHR system and functionalities are built using Python's Django framework, and the proposed attribute-based algorithm is implemented using Python's Flask framework. Both developments are then containerized separately using Docker. By using separate containers for Django and Flask, the Django web app can focus on handling web requests and interactions with the user, while the implemented algorithm on Flask can handle

the encryption operations. The workflow in figure 3 shows the system architecture of the implementation of both algorithms to provide robust data security for EHR systems. As mentioned in 3.1, and shown in algorithm 1, the data modification scheme is implemented through the use of the Charm crypto library, a cryptography library used to perform attribute-based encryption (CP-ABE) operations. When an authorized user makes a modification change to patient data in the EHR system, a POST request in JSON data format is sent to the dockerized ABE framework which contains the modification details, patient data, and doctor’s attribute. The re-encryption operation is performed at the ABE framework and sent back as encrypted modified data to the Django EHR system.

For a secure communication channel with the mobile app acting as a third-party system, the first step involved is the authentication of patients who want to have access to their health records. Credentials are provided via API endpoints from the EHR system. An authentication token is sent to fetch credential information associated with each patient. Secondly, a GET request as a REST API endpoint is sent from the mobile app to retrieve patient data from the EHR system. As mentioned in 3.3, and shown in algorithm 2, the SECP256R1 elliptic curve is used to generate a private key for the server. The function further takes the generated private key for the server and performs the shared secret computation with the associated client’s public key as input, using the key agreement algorithm. Once shared secret computation is processed, the Key Derivation Function (KDF) is initialized to derive a 32-byte (256-bit) symmetric key from the shared secret provided. The derived key and the IV random value are now used to create a cipher object that will encrypt the requested data into a ciphertext. Thirdly, a decryptor is created from the cipher object which is used to decrypt the requested data into plaintext.

This is a successful implementation of the combination of both algorithms to achieve robust data security for EHR systems. The developed algorithms address the gap in the re-encryption of patient data and secure communication between an EHR system and third-party services.

Algorithm 1 Data Modification Algorithm

Input: Changed value to original EHR field

Output: Re-encrypted modified EHR field.

- 1: Let U be the set of authorized users (admins, doctors).
 - 2: Let P be the set of patients.
 - 3: Let M be the set of modified fields in the patient records.
 - 4: Let T be the set of timestamps for the modifications.
 - 5: Let CD be the cloud database table for storing the modification details.
 - 6: **for** each modification event where an authorized user u modifies a field m in a patient record p at time t **do**
 - 7: Re-encrypt the modification details:
 - 8: Replace and store the re-encrypted modified field in the cloud database:
 - 9: $D.add(\text{Modification}(\text{user}=u, \text{patient}=p, \text{field}=m, \text{timestamp}=t))$
 - 10: **end for**
 - 11: **for** each patient p in P **do**
 - 12: Retrieve the latest modified record for patient p from the database:
 - 13: $\text{recent_modification} = D.getRecentModification(\text{patient}=p)$
 - 14: **end for**
-

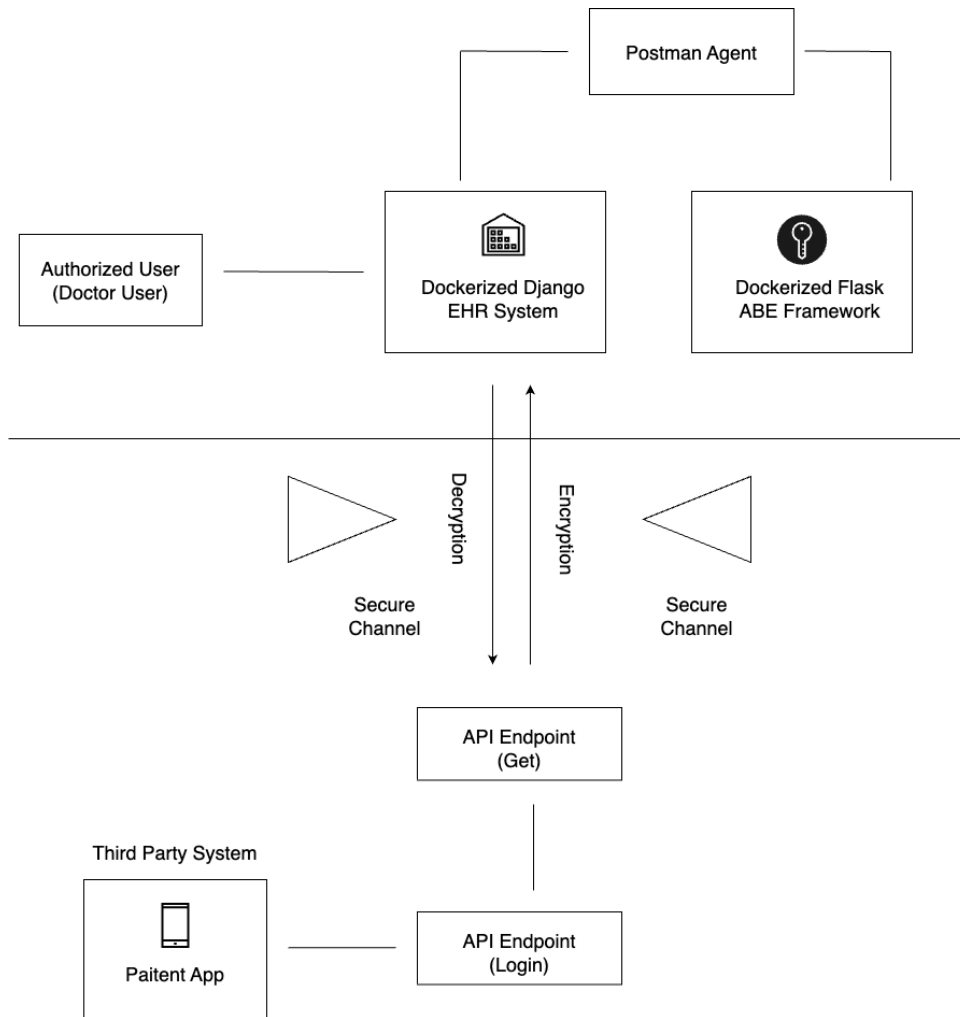


Figure 3: System Architecture of Combined Algorithms

Algorithm 2 Secure Communication Algorithm

Input: Request from patient’s app (client)

Output: Retrieved health record through secure channel

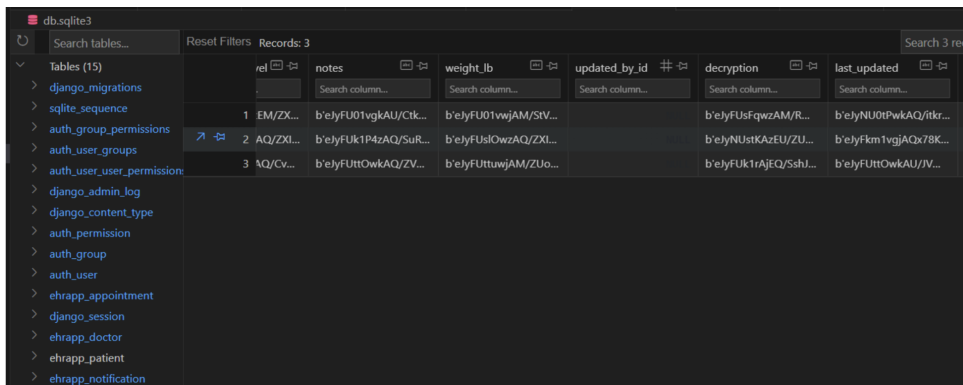
- 1: Generate server’s private key (Pri_S), and public key (Pub_S) using SECP256R1 elliptic curve
 - 2: Initialize derived key using the KDF
 - 3: Create a cipher object from the derived key and IV
 - 4: **return** an encryptor created from the cipher object
 - 5: Generate mobile app’s private key (Pri_{PA}), and public key (Pub_{PA}) using SECP256R1 elliptic curve
 - 6: Initialize derived key using the KDF from the encryption phase
 - 7: Create a cipher object from the derived key and IV
 - 8: **return** a decryptor created from the cipher object
-

5 Evaluation

This section evaluates the implemented solution of enhancing the data security capabilities of an attribute-based Electronic Health Record (EHR) system. The evaluation is based on its objectives to provide an efficient data security solution for health data within and outside of an EHR system through an attribute-based and key agreement protocol.

5.1 Achieving Encryption Continuity in Modified EHR Fields

To test for continuity of modified health data, several modification requests between the Django container and the Flask container were carried out, each containing the modification details of the EHR field, patient data, and doctor’s username as the associated attribute. As shown in Figure 4, the data modification algorithm successfully re-encrypted the modified data and returned it to the database of the EHR system as a continuity value. This ensures continuity in data protection and integrity through the lifetime cycle of a patient record in an EHR system.



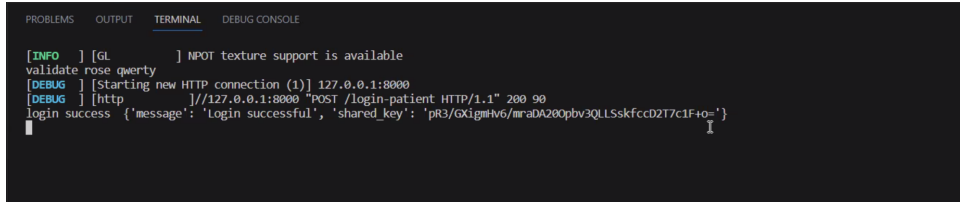
The screenshot shows a database interface with a table containing three rows of data. The columns are: id, ref, notes, weight_lb, updated_by_id, decryption, and last_updated. The data in the rows is as follows:

id	ref	notes	weight_lb	updated_by_id	decryption	last_updated
1	EM/ZK...	b'elyFU01vgkAU/Ctk...	b'elyFU01vwjAM/SV...		b'elyFUsFqwZAM/R...	b'elyNU0tPwAQ/itkr...
2	AQ/ZXl...	b'elyFUk1P4zAQ/SuR...	b'elyFUslOwzAQ/ZXl...		b'elyNUstKzEU/ZU...	b'elyFkm1vgjAOx78K...
3	lQ/CV...	b'elyFUttOwkAQ/ZV...	b'elyFUttuwjAM/ZUo...		b'elyFUk1rAjEQ/SshJ...	b'elyFUttOwkAU/IV...

Figure 4: Continuity of Modified EHR Field

5.2 Retrieving Record in Secured Environment

Several authentications and GET retrieval requests were made from the mobile app built with Kivy to the EHR system. As shown in figure 5, and figure 6, the generation of private keys and shared key computations were processed to perform encryption and decryption operations between both systems.



```
PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE
[INFO ] [GL      ] NPOT texture support is available
validate rose qwerty
[DEBUG ] [Starting new HTTP connection (1)] 127.0.0.1:8000
[DEBUG ] [http      ] //127.0.0.1:8000 "POST /login-patient HTTP/1.1" 200 90
login success {'message': 'Login successful', 'shared_key': 'pR3/GXigmHv6/mraDA20pbv3QLLSskfccD2T7c1F+o='}
```

Figure 5: Shared Secret Key Computation on Terminal

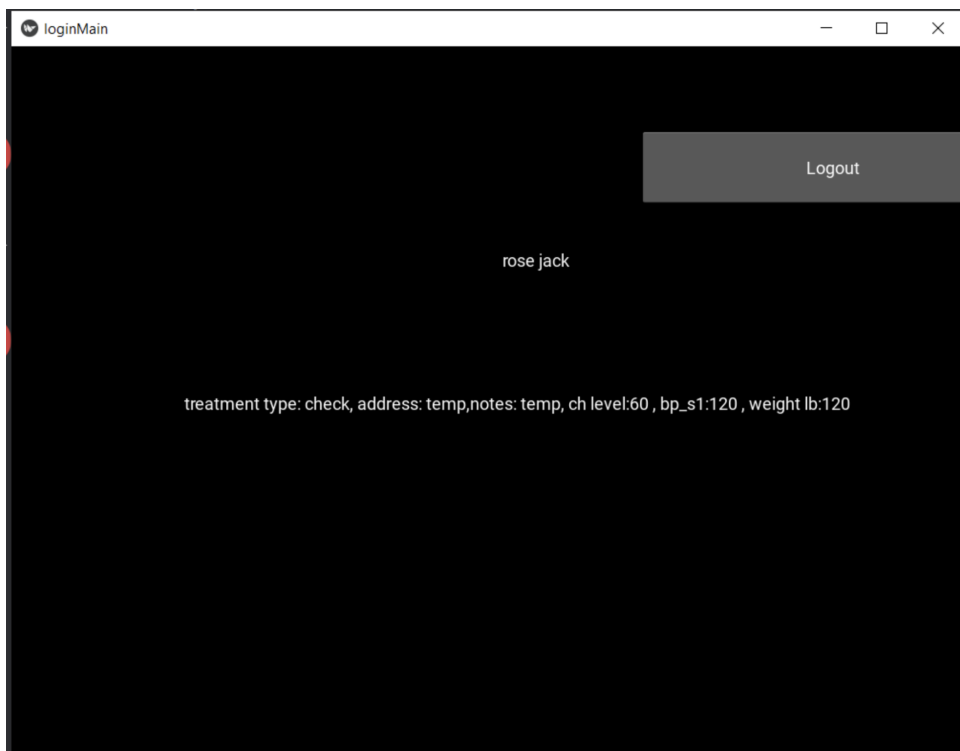


Figure 6: Mobile App Retrieval Interface

5.3 Discussion

The implementation of the Attribute-Based Encryption (ABE) system caused some number of challenges. The major part of the challenge was to solve the disparity between Python version 3.10 which was used in the EHR system, and Python 3.3 which was used for the encryption framework in Flask. The Charm library used was only compatible with Python version 3.3. Hence, the use of Docker to provide an isolated environment for

both applications to run separately, and an API endpoint to communicate with both applications. Overall, this research contributes to the existing literature on attribute-based encryption EHR systems, and how it can be extended to include data modification and secure communication with third-party systems or applications.

6 Conclusion and Future Work

In this research work, a combination of data modification and secure communication algorithms was developed. The implemented solution explores two vital needs for an attribute-based EHR system - enhance data security through encryption continuity when an EHR field is modified, and improve secure communication for data interactions and transmissions with external systems. To achieve encryption continuity, the Charm framework is utilized to extend the capabilities of an attribute-based EHR system. Also, ECDH is implored to provide a secure channel for data interaction and transmission. For implementation, docker is used to provide isolated environments for each application to run successfully. Initialization of re-encryption is ignited when there is an updated change in a patient's EHR field, ensuring that there is a single encrypted continuity of value stored in the database. This will ensure that there is consistency and continuous security in patient health data. Additionally, the implementation of an ECDH protocol ensures that there is always a secure and encrypted channel when interoperability and transmission of data with external systems take place. The overall results show the efficiency of the system in providing continuity of encrypted patient data whenever modification requests are made. Overall, the implementation of the research successfully tackles the research questions and objectives of the research paper.

While this research tackles data security in attribute-based EHR systems, optimization techniques can be explored in scenarios when there is a high volume of patient data and categorized users (Doctors, pharmacists, nurses, etc). Techniques such as caching mechanisms can be explored to provide fast responses to data modification requests. Additionally, an exploration of migrating the EHR systems' database to a cloud-based relational database can be implemented. The system will benefit from the scalability and availability of cloud data storage.

References

- Ajayi, O., Abouali, M. and Saadawi, T. (2020). Secure architecture for inter-healthcare electronic health records exchange, *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, pp. 1–6.
- Alabi, O., Gabriel, A. J., Thompson, A. and Alese, B. K. (2022). Privacy and trust models for cloud-based ehRs using multilevel cryptography and artificial intelligence, *Internet of Things* p. 91–113.
- Cao, S., Zhang, G., Liu, P., Zhang, X. and Neri, F. (2019). Cloud-assisted secure ehealth systems for tamper-proofing ehr via blockchain, *Information Sciences* **485**: 427–440.
- Elavarasan, G. and Veni, S. (2020). Data sharing attribute-based secure with efficient revocation in cloud computing, *2020 International Conference on Computing and Information Technology (ICCI-1441)*, pp. 1–6.

- Ganiga, R., Pai, R. M. and Sinha, R. K. (2020). Security framework for cloud based electronic health record (ehr) system, *International Journal of Electrical and Computer Engineering* **10**(1): 455.
- Gohar, A. N., Abdelmawgoud, S. A. and Farhan, M. S. (2022). A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and iot, *IEEE Access* **10**: 92137–92157.
- Hanif, F., Waheed, U., Shams, R. and Shareef, A. (2023). Gahbt: Genetic based hashing algorithm for managing and validating health data integrity in blockchain technology, *Blockchain in Healthcare Today* **6**(2).
- HIE (2023). What is health information exchange?, Available at: <https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie>. [Accessed April 16, 2023].
- Joshi, M., Joshi, K. and Finin, T. (2018). Attribute based encryption for secure access to cloud based ehr systems, *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp. 932–935.
- Kaliyaperumal, K. and Sammy, F. (2022). An efficient key generation scheme for secure sharing of patients health records using attribute based encryption, *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, pp. 1–6.
- Liang, X., Zhao, J., Shetty, S., Liu, J. and Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications, *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–5.
- Mahdy, M. M. (2021). Semi-centralized blockchain based distributed system for secure and private sharing of electronic health records, *2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, pp. 1–4.
- Nguyen, D. C., Pathirana, P. N., Ding, M. and Seneviratne, A. (2021). A cooperative architecture of data offloading and sharing for smart healthcare with blockchain, *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, pp. 1–8.
- Rini, R. C., Priyadharsini, R., Parasakthi, A. and Mahalakshmi, D. (2020).
URL: https://ijresm.com/Vol.3_2020/Vol3_Iss3_March20/IJRESM_V3_I3_140.pdf
- Rivero-García, A., Santos-González, I., Hernández-Goya, C., Caballero-Gil, P. and Yung, M. (2017). Patients’ data management system protected by identity-based authentication and key exchange, *Sensors* **17**(4): 733.
- Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots mod p, *Mathematics of Computation* **44**(170): 483.
- Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R. and Ahmad Khan, R. (2020). Healthcare data breaches: Insights and implications, *Healthcare* **8**(2): 133.

- Shrestha, N. M., Alsadoon, A., Prasad, P., Hourany, L. and Elchouemi, A. (2016). Enhanced e-health framework for security and privacy in healthcare system, *2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC)*, pp. 75–79.
- Shynu, P. G. and Singh, K. J. (2017). An enhanced abe based secure access control scheme for e-health clouds., *International Journal of Intelligent Engineering & Systems* **10**(5).
- Sun, J., Zhu, X., Zhang, C. and Fang, Y. (2011). Hcpp: Cryptography based secure ehr system for patient privacy and emergency healthcare, *2011 31st International Conference on Distributed Computing Systems*, pp. 373–382.
- Verizon (2022). 2022 data breach investigations report (dbir), Available at: <https://www.verizon.com/business/resources/T408/reports/dbir/2022-data-breach-investigations-report-dbir.pdf>. [Accessed April 16, 2023].
- Vimalachandran, P., Wang, H., Zhang, Y., Heyward, B. and Zhao, Y. (2017). Preserving patient-centred controls in electronic health record systems: A reliance-based model implication, *2017 International Conference on Orange Technologies (ICOT)*, pp. 37–44.
- Walid, R., Joshi, K. P. and Choi, S. G. (2021). Secure cloud ehr with semantic access control, searchable encryption and attribute revocation, *2021 IEEE International Conference on Digital Health (ICDH)*, pp. 38–47.
- Wang, S., Zhang, Y. and Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems, *IEEE Access* **6**: 38437–38450.