International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I4P123

Volume 72 Issue 4, 216-225, April 2024
© 2024 Seventh Sense Research Group®

Original Article

SRMDS: Hybrid Cryptography with Block Chain for Secure and Reliable Medical Data Sharing in E-Health Systems

M. Madhavi[1], T. Sasirooba[2], G. Kranthi Kumar[3]

[1,2]Department of Computer Science and Engineering, Annamalai University, Tamil Nadu, India.
[3]Department of Computer Science and Engineering, Velagapudi Ramakrishna Siddhartha Engineering College, Andhra Pradesh, India.

[1]Corresponding Author : madhavi.macharapu@gmail.com

Received: 16 December 2023 Revised: 01 April 2024 Accepted: 09 April 2024 Published: 24 April 2024

Abstract *- Medical data sharing can increase diagnosis precision in an e-health system where security and privacy are essential objectives. Blockchain (BC) has been proposed as a potential way of improving the exchange of Personal Health Information (PHI) due to its unchangeability. However, there is still a need for improvement in terms of patient privacy protection and PHI-sharing security. Thus, this study presents a Secure and Reliable Medical Data Sharing (SRMDS) system. This system consists of Consortium BC (CBC), private BC (PBC), and hybrid cryptography. Every patient's PHI has been encrypted employing Advanced Encryption Standards (AES) to improve privacy preservation, and Adaptive Elliptic Curve Cryptography (AECC) is employed to conduct the AES key's encryption. The AES key and PHI ciphertexts are kept in a block on the hospital's private BC. Additionally, PHI's keyword is sent to the CBC. By looking up the relevant PHI keyword, the physician can retrieve a patient's PHI from the PBC. Simulation results demonstrate that the suggested SRMDS-based electronic health (e-health) system reduces storage overhead, encryption, and decryption, enhancing patient confidentiality and safety preservation.*

Keywords *- Medical data sharing, BC, CBC, AES, AECC.*

1. Introduction

The phrase "e-Health" refers to the provision of healthcare services via digital technology. In the modern world, e-health is regarded as the most promising application [1-3]. Applications for e-health provide the ability to monitor multiple diseases for a large number of patients at any time and from any location [4-6].

When patients choose to share their medical information with others, like hospitals or research organizations, the traditional healthcare system requires them to go through a time-consuming manual consent process that can be highly difficult for healthcare providers to organize [7]. Therefore, in order to prevent those drawbacks, most modern hospitals are willing to take advantage of numerous newly developed e-health information systems. These electronic health information technologies have made it possible for patients to conveniently access smart medical services, including online registration and diagnostic appointments. A patient typically has access to a variety of healthcare experts, such as therapists, specialists, and primary care doctors [8]. In order to offer patients with high-quality care, these service providers make it easier for healthcare professionals (such as physicians, hospitals, and researchers) to remotely share and access patient medical data (such as images, videos, audio, text, etc.). The most recent health status of the patient, patient details, lab results, medical scans, clinical notes, billing data, sensor data, medical history, medication, charts, graphs, insurance information, MRI, Computed Tomography (CT), X-ray, ECG images, and other related information from participating healthcare associations medical data are among the various types of medical multimedia content that are stored in e-Health systems. Patients can go to a number of hospitals under e-Health systems, and every institution is responsible for managing its own database. With the Telecare Medicine Information System (TMIS), physicians can communicate with other medical specialists about patients' conditions and important details while seated in various remote places.

As a result, the sharing and exchange of health records is receiving more attention from researchers and industry communities, where data security and privacy protection are important subjects. These kinds of applications deal with sensitive data, and any unnecessary change or alteration to a person's private information may result in unintended actions [9-11]. It is crucial to guarantee that the data in e-health applications can only be viewed, accessed, and modified by authorized individuals [12-14]. Sharing the patient's medical information with the wanted physician so they can get the relevant information for better diagnosis is a promising solution to this issue. Suppose the person has seen another physician inside the same hospital or healthcare center, and that institution has created the relevant medical file. In that case, the doctor may view the patient's file straightaway over the local internet with the patient's permission**.**

1.1. Problem Statement and Contributions

To meet the expanding demands of the medical industry, numerous researchers are suggesting privacy-preserving sharing data approaches. Traditional access control methods for sharing Electronic Health Records (EHRs) [15–17] make the assumption that cloud servers have full confidence from data owners, granting them the authority to handle every aspect of data consumption-related access control and authorization. It is worth noting that traditional access control methods are mostly dependent on a predetermined point of access, such as a centralized cloud server, which may result in the central point of failure for electronic health networks. Still, it is a difficult challenge to securely share health information between individuals and healthcare professionals. Blockchain-based PHI-sharing platforms should enable the safe distribution of medical records. Blockchain technology offers creative solutions to speed up the delivery of healthcare, reviving the industry [18-20].

Nonetheless, patient privacy protection and the security of sharing medical data still need to be improved. These efforts offer viable ways to implement PHI sharing between healthcare facilities in e-health systems, where privacy preservation and security are major issues. The following contributions are made in this paper in order to achieve these goals.

- Hybrid cryptography is first used to encrypt each patient's PHI at a hospital. Specifically, the Advanced Encryption Standard (AES) technique is used to first encrypt the PHI. Next, the AECC encrypts the AES secret key.
- The AES secret key and encrypted patient health information can be kept in the PBC, and the CBC will maintain data on the PHI's indexes of securities.
- A patient's medical records are only accessible to licensed physicians, preventing future record retrieval.

The following sections comprise the organization of the paper: Section 2 reviews recent works based on secure medical data sharing. In Section 3, the use of hybrid cryptography with BC for secure and reliable medical information sharing in electronic healthcare systems has been suggested. The performance of the SRMDS is analyzed in section 4. Section 5 presents the conclusion of the research work.

2. Related Works

Data-level and schema-level mappings were generalized by Mehedi Masud et al. [21] as a means of achieving data interoperability across heterogeneous data sources. By solving the heterogeneity problems, the approach offered a way for the sources to share data with one another. Additionally, they developed a framework for managing metadata for multimedia content related to medicine, such as X-ray, ECG, MRI, and ultrasound images.

To find relevant multimedia resources for user searches, a distributed query processing system based on agents was employed. With the use of a suitable structure, the framework effectively creates metadata for the resources. According to the evaluation's findings, this approach worked well in terms of query execution costs and accuracy. To improve this work, it did not cover distributed management of resources and processing queries in a cloud computing context.

A strengthened key management method was presented by Salman Iqbal et al. [22] with the goal of identifying the difficulties associated with the security and privacy concerns of patients' sensitive information through strong encryption management. Another goal of this architecture was to offer a simple, well-organized key management system.

The goal of the healthcare key management (HCKM) framework, a secure and private key management strategy for electronic health systems, was therefore achieved by using various keys to decrypt the same plain text's ciphertext. According to the findings, the HCKM was a reliable and secure system. Additionally, the HCKM framework has demonstrated its resistance to frequent security breaches. This framework was not implemented since it was not created as a prototype or tested in an actual setting.

A BC-based safe and privacy-preserving PHI sharing (BSPP) method was proposed by Aiqing Zhang et al. [23] to enhance diagnosis in e-health systems. In order to achieve health record sharing, two blockchains—a PBC and a CBC—were first presented and incorporated into the framework. The PHI's secure indexes were maintained on the CBC, but the private blockchain was responsible for storing the PHI.

In addition, to incorporate fresh blocks into the BC, the block generators had to prove their compliance, which ensured system availability. In addition, they used JUICE to test this strategy and assess its performance. According to security analysis, this protocol accomplished safe searching, time-controlled annulment, confidentiality maintenance, and data protection. For the e-Health blockchains, they did not create a unique miner and verifier election algorithm. An Identity-based Authorized Searchable Encryption method (IBASE) was presented by Xiaojun Zhang and Sheng Cao et al. [24] that does not require significant certificate administration expenses. By combining identity-based encryption using keyword searches, IBASE allowed a physician to delegate authority to a physician assistant to manage the complex encrypted testing records exchanged with patients via cloud-assisted electronic health information platforms.

This significantly reduces the doctor's workload. Therefore, by submitting a request with the relevant keyword, any patient might obtain his or her diagnostic reports in a private manner. The comparison of performance showed that IBASE was feasible for cloud-assisted mobile electronic health information platforms. They didn't provide a reversible identity-based proxy re-encryption with a keyword search strategy to more protect confidential information against assistance.

A blockchain-based EHR sharing mechanism that preserves privacy and security was proposed by Salman Shamshad et al. [25] in order to increase diagnosis and treatment efficiency in TMIS. First, the consensus, data structures, and processes supporting the two different types of blockchains—the consortium blockchain and the private blockchain—were developed.

The blockchain-based EHR system employed public-key encryption with relevant keyword searches. After obtaining the patient's permission, the physician was authorized to view the intended EHRs for improved diagnosis and treatment. As a result, the increased security and improved performance demonstrated this protocol's overall strength. This protocol's security evaluation showed that it effectively prevented numerous major and small security assaults while achieving the safety of information, search, time-controlled revocation, and confidentiality protection.

A BC-based permissioned medical information transfer platform, as proposed by Khaled Shuaib et al. [26], integrates BC technology with a threshold signature and decentralized file structure to solve security issues like one point of inability and Denial-of-service (DoS) assaults that are common in traditional database systems.

The Interplanetary File System (IPFS) and the Istanbul Byzantine Fault Tolerant (IBFT) consensus mechanism served as the foundation for this system. They used Hyperledger Besu, an enterprise Ethereum blockchain, to construct this system. A certain number of transactions and Variable network sizes were used in the experiments. As demonstrated by the experimental results, this system offered improved data security and integrity. It outperformed other blockchain-based systems in the majority of circumstances and across a variety of network sizes.[28]

A BC and decentralized Interplanetary File System (IPFS) on a mobile cloud platform were coupled in a framework for exchanging Electronic Health Records (EHRs), as proposed by Dinh C. Nguyen et al. [27]. Specifically, the authors created a trustworthy access control framework that utilizes Smart Contracts (SC) to facilitate the safe exchange of electronic health records between various patients and healthcare professionals. They demonstrated a working prototype that used the Ethereum blockchain in a mobile app that leveraged Amazon cloud computing to share actual data.

The experimental results showed this technology provided an effective means of ensuring secure data transfers on mobile clouds while protecting confidential medical records from harm. The system assessment and security evaluation also showed improvements in performance in lightweight access control design, minimum network delay, and enhanced safety and confidentiality of information levels when compared to existing information exchange approaches.

A reliable access control system that made use of smart contracts was presented by Mudassir Khan et al. [29] in order to increase security when exchanging electronic health records between different patients and medical professionals. They employed a blockchain in conjunction with a peer-to-peer review process to integrate seamless storage options and achieve safe information management and sharing. To test the efficacy of this approach, they merely deployed an Ethereum blockchain on the AWS cloud.

By effectively identifying and preventing unauthorized access to e-health systems, an access control system might protect computer security and patient privacy. The framework valuation and protection technique found that considerable degrees of security and data concealment, low network expectation, and lightweight access control architecture were more practicable when evaluating the current data-sharing models.

3. Proposed Methodology

3.1. Overview

The suggested scheme's process is depicted in Figure 1. Under this method, every hospital patient's PHI is electronically recorded and preserved in a hospital server. A doctor extracts the PHI's keyword and saves it on a server along with the PHI. PHI for every patient is encrypted to improve patient privacy protection. In this method, hybrid cryptography is introduced. Specifically, the AES standard is offered to encrypt the PHI, and the AES key is encrypted using AECC. Next, the server places the encrypted PHI report in the associated PBC along with the AES block, and it stores the PHI keyword in the CBC.

Physicians obtain the PHI of a patient associated with the keyword from the PBC through the CBC through verifying the identity of the data generator. They are able to obtain the patient's PHI ciphertext by gaining access to the PBC. Subsequently, they use the AES key to decode both the AES key and the PHI ciphertext.

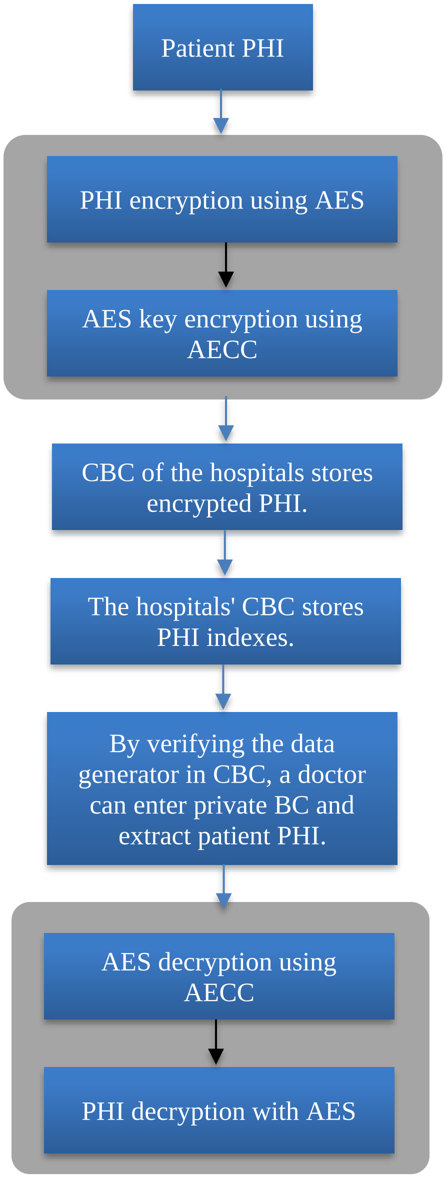
Patient PHI
PHI encryption using AES
AES key encryption using AECC
CBC of the hospitals stores encrypted PHI.
The hospitals' CBC stores PHI indexes.
By verifying the data generator in CBC, a doctor can enter private BC and extract patient PHI.
AES decryption using AECC
PHI decryption with AES

Fig. 1 The proposed scheme's workflow

3.2. System Architecture

Figure 2 shows the system architecture for the suggested health information exchange. Medical centers, or Medical Service Providers (MSPs), consumers, or patients, and system managers are the three main entities in the paradigm, as shown in the image below.

3.2.1. System Manager (SM)

It oversees the entire structure. Every doctor and patient registers their information with this SM. Additionally, it produces the CBC consensus vector (a).

3.2.2. MSPs

It also serve as a representative for hospitals. Each hospital has a certain number of computer clients and servers, as shown in Figure 2.

The doctor enters each patient's PHI using the computer client. These clients, after that, create blocks for the recorded PHI of the patients and send them to the hospital's PBC. The patient and doctor registration is kept up to date by the server. Additionally, it provides access to patient PHI for doctors who are not in the PBC by verifying their identity. It also confirms fresh blocks for CBC.

3.2.3. Patients

Patients seeking medical care in hospitals. Prior to seeing a physician, patients have to register with the hospital server. The token is given by a server to each patient upon registration. When the patient visits the hospital, they must show the token to the doctor, keeping it private. Beacons enable the creation of PHI for patients by serving as evidence of the patient-doctor relationship. The PHI will, after that be stored in the hospital's PBC. Additionally, the CBC obtains the keywords of the blocks in the PBC from the hospitals.

3.3. Hybrid Cryptography for Encrypting PHI

Using computer clients, the doctor enters the patient's PHI after the patient visits the hospital. These patients send the file to the hospital's PBC in the form of a block. The PHI is encrypted using hybrid cryptography to improve the patient's privacy protection. It specifically presents the combination using AECC for encryption. This method encrypts the patient's PHI using the AES algorithm, and the AES secret key is encrypted using the AECC algorithm. The following is an explanation of how encryption performs:

3.3.1. AES

The PHI data is fed into the AES algorithm first. Round keys are produced for this algorithm based on the original encryption key (the AES secret key) employing a random number generator (RNG). Though this algorithm operates with many key sizes, 128 bits with 10 rounds is the key size used in this study. Additionally, the block's size and key length are the same. Following the completion of ten rounds, the input voted data is encrypted. There are four main operations in each round.

3.3.2. SubBytes

In this procedure, a new byte is used to replace each byte in the block. This process will be carried out by using the lookup table, also called the S-box.
Row Shift: This process involves shifting each row a certain number of times.

3.3.3. Mix Column

To alter each byte's position in a column, a certain matrix is multiplied by each column in the block. In the previous round, this step was not taken into account.

3.3.4. Round Key

In this phase, the outcome from the prior step and the associated round key are XORed.

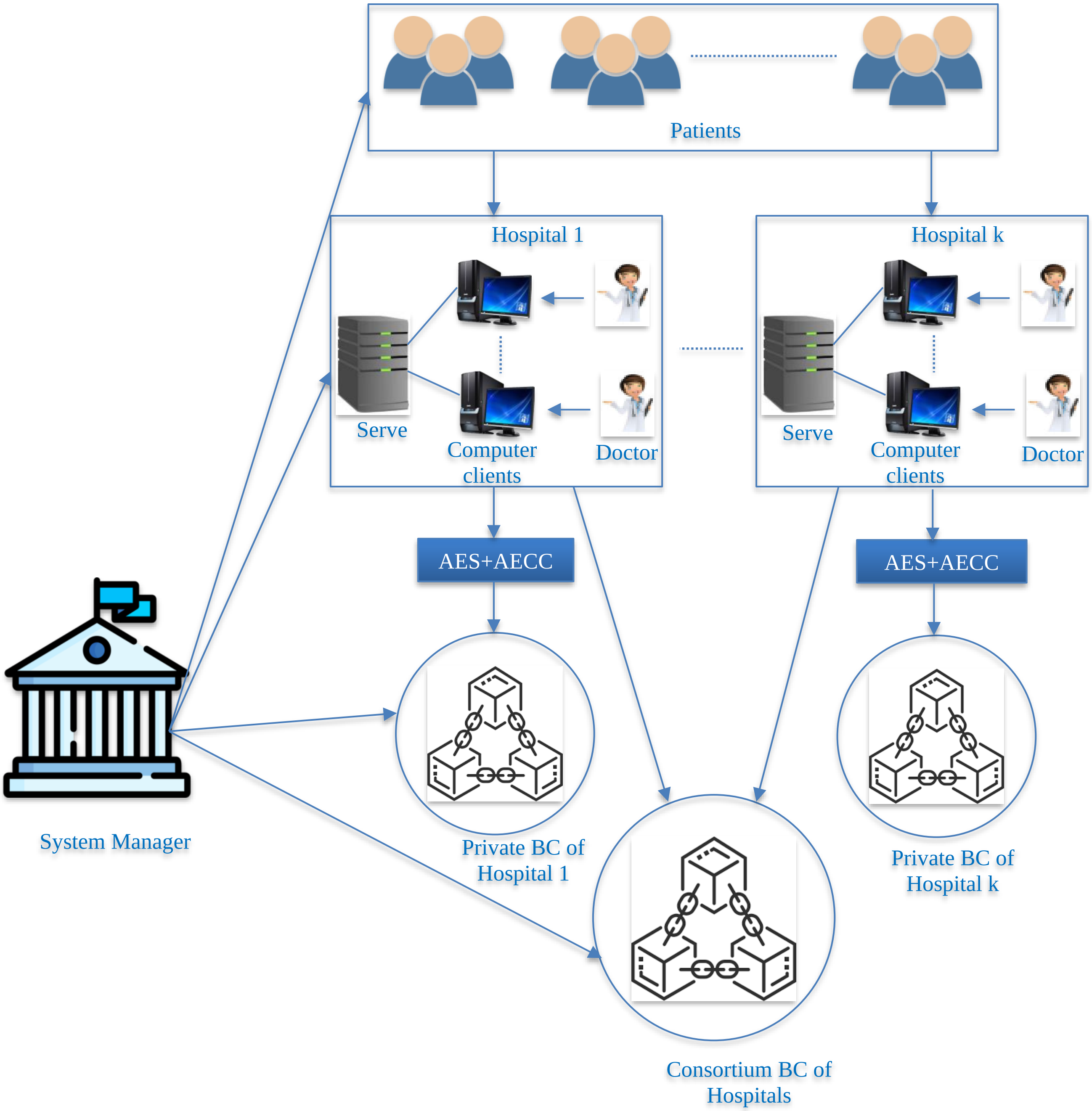

Fig. 2 System architecture

After finishing each of these rounds, the output is 128-bit encrypted voting data. Until all voting data is obtained in encrypted form, the same procedure is repeated. Furthermore, the security strength of PHI transactions is enhanced through encrypting the AES secret key with a suggested AECC. The performance of the IECC algorithm is explained in the section that follows.

3.3.5. AECC

The ECC algorithm is an unequal or public key cryptography algorithm. In order to encrypt and decrypt data, this algorithm produces a couple of keys: a public and a private key. The ECC method raises the possibility of implementation errors even though it can boost security with less processing resources. Therefore, an updated ECC method is described in order to raise the system's security level. Specifically, a secret key can be produced together with both of the keys. Using the prime number operations, the AECC algorithm is utilized as a maximal limit and is centered on a curve that has certain base points. The mathematical representation of ECC is described as follows:

$$p^2 = q^3 + uq + v \tag{1}$$

In this case, u and v stand in for the random numbers.

3.3.6. Key Generation

The AECC generates three different sorts of keys: public key (η_m), private key (μ_m), and secret key (ε_m). The server η_m creates the input data, which is initially encrypted. Secondly, μ_m is produced by the server to decrypt the relevant information. Lastly, $\varepsilon_m$is produced based on the η_m, $\mu_m$and curve point (P). ε_m Is incorporated into the data during encryption and deducted from the cipher data when AECC is used to decrypt the data. In addition, $\mu_m$is selected at random from the set of n prime numbers. Next, the following is η_m produced based on a μ_m and P:

$$\eta_m = \mu_m \times P \tag{2}$$

Subsequently, η_m , is produced by adding, η_k , $\varepsilon_k$and G, that is,

$$\varepsilon_m = \eta_m + \mu_m + P \tag{3}$$

3.3.7. Encryption

In this stage, an affine point on the curve is created using the AES secret key (AESsk). Additionally, the obtained AESsk is encrypted. There are two cipher texts in the encrypted data, and they are as follows:

$$C_1 = \varepsilon_m + \left((K * P)\right) \tag{4}$$

$$C_2 = \varepsilon_m \ + \left(AES_{sk} + (K * \eta_m)\right) \tag{5}$$

The cipher texts are represented by, and K shows the random integer that falls inside the interval [1, n-1].

3.4. Encrypted PHI Sharing Using Consortium and Private Blockchains

The PHI and AES key ciphertexts are transferred as blocks by the clients to the PBC. These clients additionally provide the CBC with the keywords linked to the PHI blocks. The following describes the performance of CBC and private BC:

3.4.1. Private BC

The block structure of a hospital's private BC is shown in Figure 3. This block structure includes the block header, contributor's signatures, timestamps and payload. The prior block's hash, block ID, and block size are all included in the block header. Payment payload contains AES key, hash of encrypted PHI, PHI keyword and IDs of PHI owner or patient, creator or doctor. The block creator can be located by using the contributor's signature. A timestamp represents the block creation time.

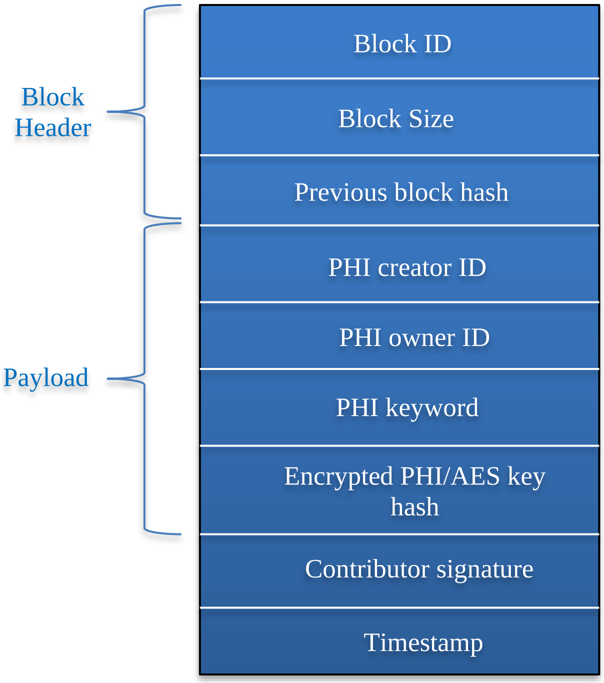

Fig. 3 The PBC block structure of the hospital

A consensus mechanism determines the validation of a fresh block in PBC. Proof of conformity is regarded in this method as the PBC and CBC consensus mechanism. The block's validation is established using the proof of conformance. Once the person has registered with the hospital, they may obtain a secure token that will enable them to participate in this consensus mechanism. The user gives their token to a physician upon visiting. A physician is able to employ a safe token to create a user ID. Other consumers verify that a physician has the right to create patient records upon obtaining a newly made transaction from this consumer. The latest transaction is recognized as the latest authorization block in the PBC if more than two or three clients approve it.

3.4.2. CBC

The block structure of CBC is depicted in Figure 4. CBC includes the block header, payload, timestamp and contributors' signatures, similar to those in private BC. Secure indexes and the block creator ID are included in this block's payload. The secure index is made up of n transactions, which are represented by $Ty_1, Ty_2, \ldots, Ty_{1n}$ here. Additionally, every transaction provides a safe index to the patient's PHI, which is made up of the PHI keyword, the block ID, and the PHI owner's ID. Since users are able to perform keyword searches in the CBC, keywords in the BC must be consistent. Because keywords explain a patient's symptoms or diagnosis, they are correlated in the system with standard medical descriptions. In order for users to search for keywords on the BC, keywords are usually tied to a predefined set. The keywords selected from the predetermined list of keywords shown *Ω* are verified by the consensus mechanism.

For CBC proof of conformity, the framework creates a polynomial based on keywords.

Consider $\Omega = \{k_1, k_2, \ldots\ldots, k_l\}$ where l represents the size of Ω. The following is a description of the polynomial building process:

Find $H_1(k_1), H_1(k_2), \ldots\ldots\ldots, H_1(k_l)$ and create a polynomial f(y) that satisfies

$$f(H_1(k_i)) = 0, \quad i \in [1, 2, \ldots\ldots, l]$$

with order l. The definition of a polynomial is

$$f(y) = (y - H_1(k_1))(y - H_1(k_2))\ldots\ldots(y - H_1(k_n)) \tag{6}$$

Equation (6) is expressed as

$$f(y) = y^l + b_{l-1} y^{l-1} + \ldots\ldots\ldots + b_1 y + b_0 \tag{7}$$

The polynomial coefficients are indicated here by $[1, b_{l-1}, b_{l-2}, \ldots\ldots, b_0]$. Through function substitution f (y) = 0,

$$f(y) = y^l + b_{l-1} y^{l-1} + \ldots\ldots\ldots + b_1 y + b_0 \tag{8}$$

After dividing Equation (8) by $-b_0$, we get

$$\frac{-1}{b_0} y^l + \frac{-b_{l-1}}{b_0} y^{l-1} + \ldots\ldots\ldots + \frac{-b_1}{b_0} y = 1 \tag{9}$$

Equation (9) is expressed as

$$g(y) = a_l y^l + a_{l-1} y^{l-1} + \ldots\ldots\ldots + a_1 y \tag{10}$$

Formula, it can be inferred that $g(H_1(k_i)) = 1$, here $k_i \in \Omega$. The following is a description of the vectors a and h:

$$a = [a_1, a_2, \ldots\ldots, a_{l-1}, a_l] \tag{11}$$

$$h_i = [H_1(k_i), H_1(k_i)^2, \ldots\ldots\ldots, H_1(k_i)^{l-1}, H_1(k_i)^l] \tag{12}$$

a and h_i is $a \cdot h_i = 1$ the inner product of vectors. In this case, the consensus vector a is utilized to confirm that the secure indexes in newly arrived CBC blocks are valid. If a maximum of two or three consumers authorizes a fresh transaction, it is saved in the CBC as a fresh authorization block.

The physician resolves this in order to retrieve the patient's PHI linked to a keyword that indicates the PHI owner, the PHI creator's ID, the PHI ciphertexts, and the AES key in this instance. By confirming, the physician can gain entry to the hospital's private BC to get ciphertexts. After that, the physician decrypts the AES key's ciphertext to retrieve the patient's PHI.

3.5. The Hybrid Cryptography Decryption Phase

The contributor's signature is known to the doctor; therefore, they rehash the server's blocks. From the blocks, they obtain the encrypted AESsk and the cipher text (PHI).

AESsk must first be decrypted in order to decode the cipher text. The same AECC technique is used to decode the AESsk. The following is the definition of the decryption function in AECC:

$$AES_{sk} = (((C_2 - \mu_m) * C_1) - \varepsilon_m) \tag{13}$$

€$_m$ is subtracted from the cipher texts to obtain an initial AESsk, as per (13).

Invert mix columns, shift rows, invert subbytes, and add round keys are the steps in the sequence that are used to decode the encrypted PHI using the obtained AESsk. A physician obtains a patient's original PHI once all rounds have been completed.

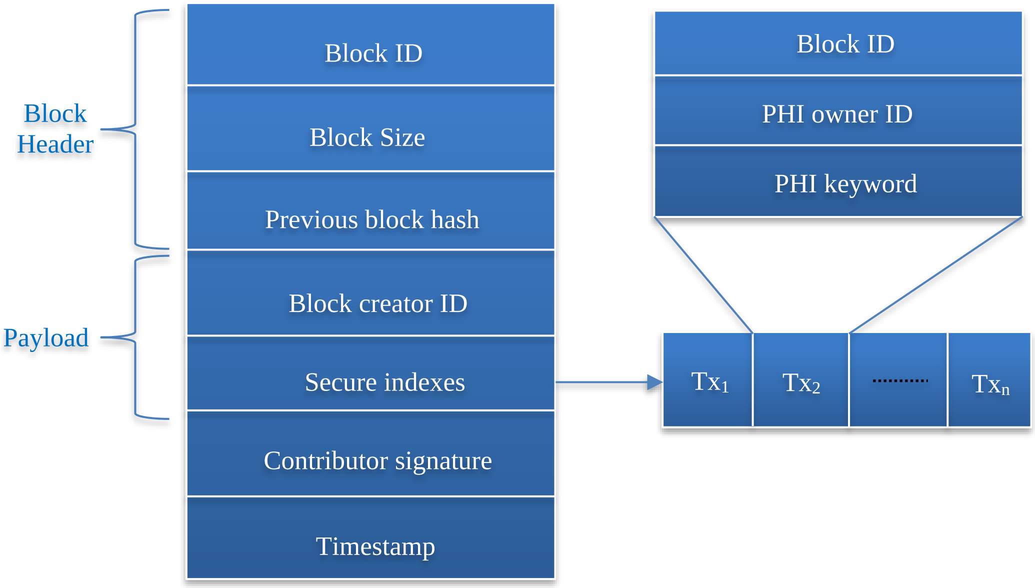

Fig. 4 The block structure of CBC

4. Results and Discussion

This system works with a Windows 10 operating system on an Intel Core i5 processor that has 6GB of RAM. The proposed approach is simulated and implemented in Python.

4.1. Performance Analysis

The encryption and decryption time, memory consumption during encryption and decryption, and degree of security of a suggested AES-AECC with a blockchain-based healthcare system are all analyzed. The performance of a suggested scheme is contrasted with both AES-ECC as well as DES-ECC algorithms. The PBC and CBC are used by every cryptographic algorithm in their implementation. Figure 5 and Table 1 show the BC-based hybrid cryptographic methods' encryption times. The figure shows that AES-ECC has a 25% shorter encryption time than DES-ECC.

Nonetheless, contrasted with AES-ECC as well as DES-ECC, the encryption time of the suggested scheme is decreased to 31% and 49%, respectively. The blockchain decryption times for many hybrid cryptographic algorithms are displayed in Figure 6 and Table 2. The suggested scheme's decryption time is reduced to 33% and 47%, respectively, compared to AES-ECC and DES-ECC, as the figure illustrates. As can be seen in Figure 7 and Table 3, the suggested approach uses 13% and 20% less RAM for encryption than AES-ECC and DES-ECC. Figure 8 and Table 4 display the memory utilization of various decryption techniques. The suggested technique reduces memory use during decryption to 8% and 19%, respectively, in comparison to AES-ECC and DES-ECC. Figure 9 and Table 5 illustrate the various techniques' security levels. Because the security effectiveness of ECC is strengthened by including a secret key in addition to the pair keys, the security level of AECC-AES is raised to 3% and 5% higher than that of AES-ECC and DES-ECC, accordingly.

Table 1. Different hybrid cryptographies' encryption times with BC

Methods	Encryption time (ms)
DES-ECC	1984
AES-ECC	1457
Proposed	986

Table 2. Different hybrid cryptographies' decryption times with BC

Methods	Decryption time (ms)
DES-ECC	1898
AES-ECC	1486
Proposed	976

Table 3. Memory utilization for various hybrid cryptography encryptions using BC

Methods	Memory usage on encryption (kilobytes)
DES-ECC	968544784
AES-ECC	887441265
Proposed	763325488

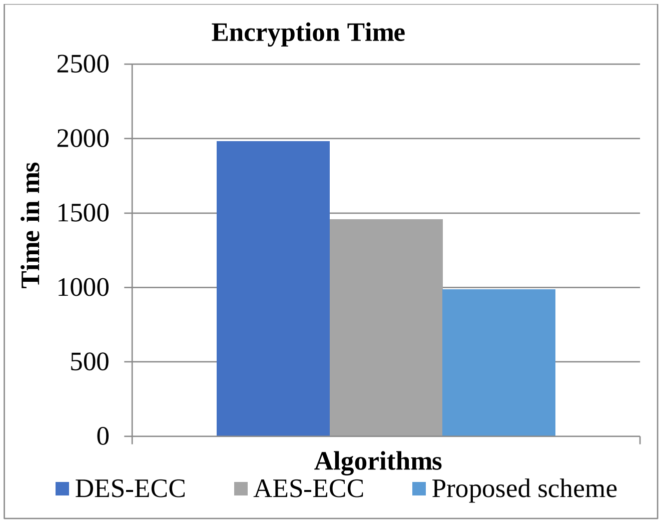

Fig. 5 Different hybrid cryptographies' encryption times with BC

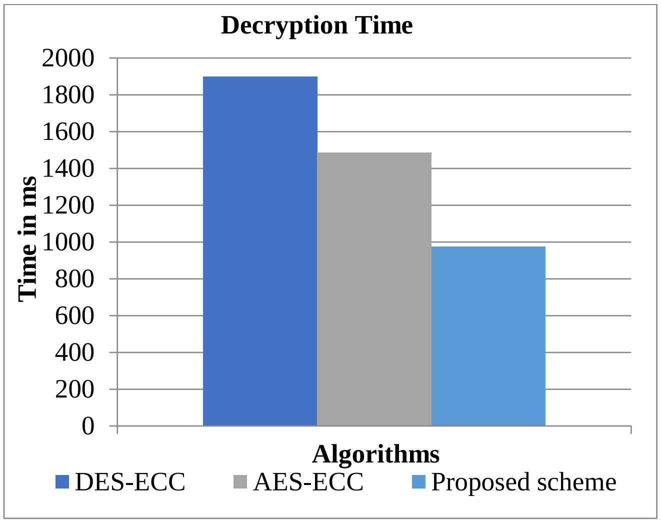

Fig. 6 Different hybrid cryptographies' decryption times with BC

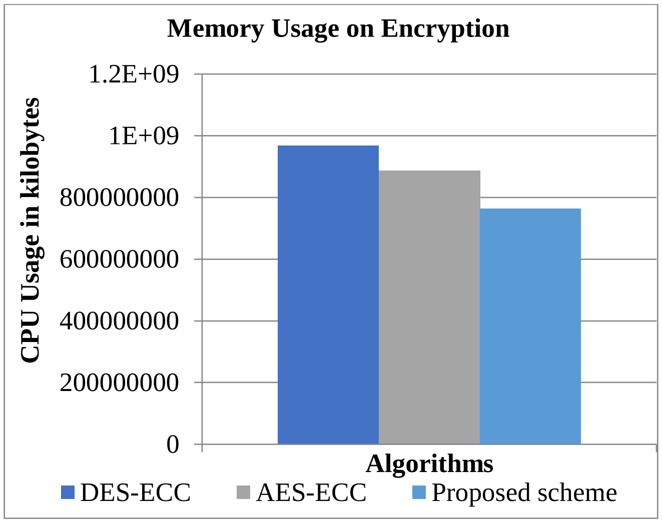

Fig. 7 Memory utilization for various hybrid cryptography encryptions using BC

Table 4. Memory used for decrypting various hybrid cryptographies with BC

Methods	Memory usage on decryption (kilobytes)
DES-ECC	978455474
AES-ECC	863355448
Proposed	784588756

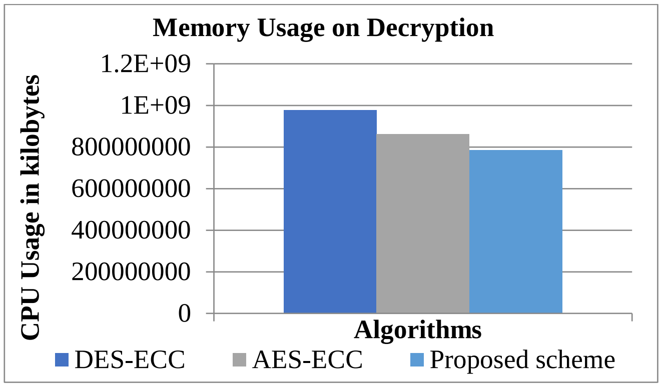

Fig. 8 Memory used for decrypting various hybrid cryptographies with BC

Table 5. Various hybrid cryptography security levels with BC

Methods	Security level (%)
DES-ECC	93
AES-ECC	95
Proposed	97

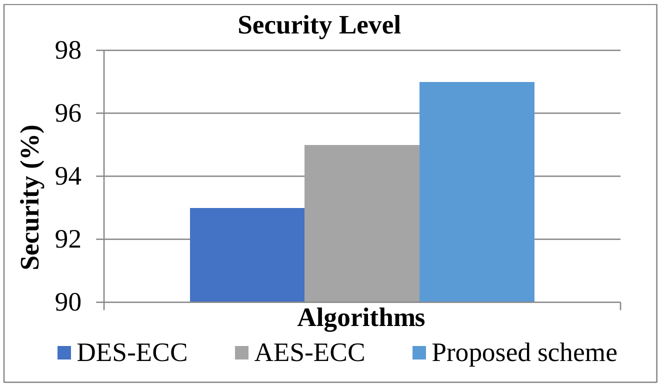

Fig. 9 Various hybrid cryptography security levels with BC

5. Conclusion

To improve the privacy and security preservation of every patient's PHI in a method of medical data exchange, an SRMDS-based e-health system was developed in this study. Every hospital patient's PHI is encrypted in this system using the AES algorithms. Next, AECC algorithms are used to encrypt the AES key. The hospital server stored the PHI and AES key ciphertexts as a block on a PBC, and a keyword associated with that PHI has been stored on a CBC.

The physicians had the ability to obtain a patient's PHI linked to the keyword in a PBC by comparing a data generator's ID with the CBC. They were able to obtain the patient's PHI ciphertext by gaining access to the private BC. Subsequently, they used the AES key to decrypt the PHI ciphertext and successfully decrypted the AES key.

Performances of AES-AECC with BC, AES-ECC and DES-ECC have been contrasted. Furthermore, a suggested AES-AECC e-Health system built on BC reduced the encryption and decryption times to 49% and 47%, respectively. Additionally, storage overhead has dropped to 19–20%.

Funding Statement

The Authors received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] R. Canetti et al., “Multicast Security: A Taxonomy and Some Efficient Constructions,” *IEEE INFOCOM '99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, New York, USA, vol. 2, pp. 708-716, 1999. [CrossRef] [Google Scholar] [Publisher Link]

[2] H. Harney, and C. Muckenhirn, “Group Key Management Protocol (GKMP) Architecture,” *Network Working Group*, pp. 1-22, 1997. [Google Scholar] [Publisher Link]

[3] O.S. Albahri et al., “Systematic Review of Real-Time Remote Health Monitoring System in Triage and Priority-Based Sensor Technology: Taxonomy, Open Challenges, Motivation and Recommendations,” *Journal of Medical Systems*, vol. 42, pp. 1-27, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[4] A.S. Albahri et al., “Real-Time Fault-Tolerant mHealth System: Comprehensive Review of Healthcare Services, Opens Issues, Challenges and Methodological Aspects,” *Journal of Medical Systems*, vol. 42, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[5] A.A. Zaidan et al., “A Review on Smartphone Skin Cancer Diagnosis Apps in Evaluation and Benchmarking: Coherent Taxonomy, Open Issues and Recommendation Pathway Solution,” *Health and Technology*, vol. 8, pp. 223-238, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] M.A. Alsalem et al., “A Review of the Automated Detection and Classification of Acute Leukaemia: Coherent Taxonomy, Datasets, Validation and Performance Measurements, Motivation, Open Challenges and Recommendations,” *Computer Methods and Programs in Biomedicine*, vol. 158, pp. 93-112, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[7] Alevtina Dubovitskaya et al., “Secure and Trustable Electronic Medical Records Sharing Using Blockchain, *AMIA Annual Symposium Proceedings*, pp. 650-659, 2017. [Google Scholar] [Publisher Link]

[8] Assad Abbas, and Samee U. Khan, “A Review on the State-of-Theart Privacy-Preserving Approaches in the e-Health Clouds,” *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 4, pp. 1431-1441, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[9] Muzammil Hussain et al., “Conceptual Framework for the Security of Mobile Health Applications on Android Platform,” *Telematics and Informatics*, vol. 35, no. 5, pp. 1335-1354, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[10] A.A. Zaidan et al., “Evaluation and Selection of Open-Source EMR Software Packages Based on Integrated AHP and TOPSIS,” *Journal of Biomedical Informatics*, vol. 53, pp. 390-404, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[11] M.L. Mat Kiah et al., “An Enhanced Security Solution for Electronic Medical Records Based on AES Hybrid Technique with SOAP/XML and SHA-1,” *Journal of Medical Systems*, vol. 37, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[12] Chun Zhang et al., “Comparison of Inter-Area Rekeying Algorithms for Secure Wireless Group Communications,” *Performance Evaluation*, vol. 49, no. 1-4, pp. 1-20, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[13] M.L.M. Kiah et al., “Open Source EMR Software: Profiling, Insights and Hands-On Analysis,” *Computer Methods and Programs in Biomedicine*, vol. 117, no. 2, pp. 360-382, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[14] A.A. Zaidan et al., “Multi-Criteria Analysis for OS-EMR Software Selection Problem: A Comparative Study,” *Decision Support Systems*, vol. 78, pp. 15-27, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[15] Ruoyu Wu, Gail-Joon Ahn, and Hongxin Hu, “Secure Sharing of Electronic Health Records in Clouds,” *8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, Pittsburgh, PA, USA, pp. 711-718, 2012. [Google Scholar] [Publisher Link]

[16] Ahmed Ibrahim, Baban Mahmood, and Mukesh Singhal, “A Secure Framework for Sharing Electronic Health Records Over Clouds,” *2016 IEEE International Conference on Serious Games and Applications for Health (SeGAH)*, Orlando, FL, USA, pp. 1-8, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[17] Zuobin Ying et al., “A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud,” *IEEE Access*, vol. 6, pp. 53698-53708, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[18] Hira Fariha Anjum et al., “Mapping Research Trends of Blockchain Technology in Healthcare,” *IEEE Access*, vol. 8, pp. 174244-174254, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Cornelius C. Agbo, Qusay H. Mahmoud, and J. Mikael Eklund, “Blockchain Technology in Healthcare: A Systematic Review,” *Healthcare*, vol. 7, no. 2, pp. 1-30, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[20] Israa Abu-Elezz et al., “The Benefits and Threats of Blockchain Technology in Healthcare: A Scoping Review,” *International Journal of Medical Informatics*, vol. 142, pp. 1-9, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] Mehedi Masud, M. Shamim Hossain, and Atif Alamri, “Data Interoperability and Multimedia Content Management in e-Health Systems,” *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1015-1023, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[22] Salman Iqbal et al., “Real-Time-Based E-Health Systems: Design and Implementation of a Lightweight Key Management Protocol for Securing Sensitive Information of Patients,” *Health and Technology*, vol. 9, pp. 93-111, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[23] Aiqing Zhang, and Xiaodong Lin, “Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain,” *Journal of Medical Systems*, vol. 42, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[24] Xiaojun Zhang et al., “Enabling Identity-based Authorized Encrypted Diagnostic Data Sharing for Cloud-Assisted E-Health Information Systems,” *Journal of Information Security and Applications*, vol. 54, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] Salman Shamshad et al., “A Secure Blockchain-based e-Health Records Storage and Sharing Scheme,” *Journal of Information Security and Applications*, vol. 55, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[26] Khaled Shuaib et al., “Secure Decentralized Electronic Health Records Sharing System Based on Blockchains,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5045-5058, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] Dinh C. Nguyen et al., “Blockchain for Secure EHRs Sharing of Mobile Cloud-Based E-Health Systems,” *IEEE Access*, vol. 7, pp. 66792-66806, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[28] Sherali Zeadally, Jesús Téllez Isaac, and Zubair Baig, “Security Attacks and Solutions in Electronic Health (E-health) Systems,” *Journal of Medical Systems*, vol. 40, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[29] P. Chinnasamy et al., “Smart Contract-Enabled Secure Sharing of Health Data for a Mobile Cloud-Based E-Health System,” *Applied Sciences*, vol. 13, no. 6, pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]