International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.2 (2025) pp. 1616-1631
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Algorithms for Enhanced Security and Data Sharing in Blockchain-Driven Healthcare Systems

G. Jithender Reddy[1,2]*, T. Uma Devi[3]

[1]Research Scholar Department of Computer Science GITAM School of Science, Visakhapatnam, India
[2]Assistant Professor St. Peter's Engineering College Hyderabad, India
* **Corresponding Author Email:** 121962504002@gitam.in - **ORCID:** 0009-0006-4506-0025

[3]Professor Department of Computer Science GITAM School of Science Visakhapatnam, India
Email: utatavar@gitam.edu - **ORCID:** 0000-0003-4560-3270

Article Info:

DOI: 10.22399/ijcesen.1162
Received : 11 December 2024
Accepted : 20 February 2025

Keywords :

Healthcare,
Blockchain,
Data Security,
Encryption,
Decryption,
Secure Data Sharing.

Abstract:

In the era of blockchain-driven healthcare systems, sharing and storing secure data has emerged as one of the pivotal challenges. The framework employs Advanced Encryption Standard with Galois/Counter Mode (AES-GCM) to securely encrypt data, including customer and product information, to ensure confidentiality and integrity. Utilizing a new method for Diffie-Hellman key exchange and ring signatures, it is possible to share encryption keys alongside an option anon securely, which are significantly improved to 2.3 and 1.8 seconds, respectively. The blockchain implements Proof-of-Authority (PoA), which allows for high throughput and a low latency response suitable for time-sensitive healthcare applications. A comprehensive real-world dataset of electronic health records (the MIMIC-III Clinical Database) was utilized to evaluate the framework's performance. Compared to state-of-the-art methods, the encryption and decryption times for 50 MB of data have significantly improved to 2.3 seconds and 1.8 seconds, respectively. It is also scalable, which means it scales up as the volume of work increases, and the privacy/security standards can be sustained as the workload increases. This framework covers areas of the regulatory requirements for efficient, secure healthcare data handling, including anonymity, non-repudiation, and data resistance to tampering. Compared with traditional models, it achieves better results regarding execution time, scalability, and data-sharing privacy.

1. Introduction

The number of patients is skyrocketing in many nations, and it's getting harder for people to see primary care physicians or other providers. Through remote patient monitoring (RPM), the emergence of wearable technology and the Internet of Things has enhanced patient quality of care in recent years [1]. It also makes it possible for doctors to treat more patients. Patients are monitored and cared for using RPM while they are not in a traditional clinical setting—for instance, at home. The main components of an RPM system may consist of an internet-connected smartphone, an RPM application, a monitoring device, and smart contracts for blockchain integration [2]. IoT and wearable technology are key components of RPM and the ongoing endeavor to establish Smart Cities. Technology gathers health information from patients and sends the same to service providers to help with diagnosis, treatment, and health monitoring. As a result of all the patient data being shared and evaluated, the development of a big data scenario is evident 3]. Such infrastructure requires secure data sharing in order to manage such patient data with other organizations. Blockchain technology may hold the key to addressing data security and privacy issues in IoT scenarios. Blockchain technology, which was first postulated by Satoshi Nakamoto, offers resilience versus data and failure disclosure. The miners, who are in charge of generating blocks, are always attempting to solve hash computations, which are cryptographic riddles known as Proof of Work (PoW). For healthcare applications in blockchain, there is a need for improving security and provision for data sharing across healthcare units. In the literature, numerous endeavors are documented

aimed at enhancing the security of healthcare applications utilizing blockchain technology. Reference [4] discusses a secure blockchain-based framework for storing and sharing electronic health records (EHRs), emphasizing data integrity, confidentiality, and patient privacy through cryptographic mechanisms and decentralized access control. This innovative system not only guarantees the privacy and security of electronic health data but also enhances the overall effectiveness of healthcare practices. Omar et al. [5] focused on using blockchain technology to decentralize healthcare data security in the cloud while keeping the patient in mind. In the study documented in reference [6], an in-depth analysis is conducted to explore the privacy and security aspects of the healthcare blockchain. This examination encompasses an investigation into potential risks (dangers), the identified requirements (needs), and proposed solutions associated with the exchange of electronic medical data.

This innovative method is designed to ensure the private and secure exchange of E-healthcare data, addressing critical confidentiality and security concerns within the healthcare blockchain domain. The research indicates that a thorough security plan is necessary, one that not only protects healthcare data but also provides the required provision for secure data sharing across healthcare units.

The following are the contributions to this publication.

1. A comprehensive security framework integrating various algorithms to achieve secure data storage in blockchain and facilitate secure sharing among authorized users.
2. Proposal of essential algorithms, including Encrypt, Decrypt, Key Sharing, and Verify, crucial for implementing and operationalizing the aforementioned security framework. (rewrite as below- Proposal of essential algorithms, including Encrypt, Decrypt, Key Sharing, and Verify, that are crucial for the implementation and operation of the aforementioned security framework.)
3. Evaluation of the utility, performance, and security of the proposed framework and underlying algorithms to assess their overall effectiveness.

The literature on current security protocols related to blockchain technology and medical applications is reviewed in Section 2. The suggested security structure and algorithms are presented in Section 3. The experimental results are presented in Section 4, and a discussion of the proposed work and its limitations is included in Section 5. The work is concluded, and future work opportunities are outlined in Section 6.

2. Related Work.

This section examines the research done on existing techniques used for protecting application data in blockchain. Niu et al. [1] suggested a permissioned blockchain-based attribute encryption and ciphertext-based medical data exchange strategy for safe, effective, and privacy-preserving electronic health record access and sharing across medical facilities. Pournaghi et al. [2] displayed "MedSBA," a blockchain-based attribute-based encryption system for safe and effective medical data sharing. Mamta et al. [3] in order to provide resilience, a blockchain is used in the proposed decentralized ABSE scheme for healthcare Cyber-Physical Systems (CCPS) to handle computational operations effectively and remove a single point of failure. Shamshad et al. [4] presented an EHR sharing system that is blockchain-based and guarantees privacy and security for effective healthcare. Security study verifies the system's resistance to assaults, and performance analysis shows that it has less overhead than other protocols. The methodology makes EHR exchange in the TMIS safe and effective, which improves healthcare. The platform performs well in a blockchain context, and future work will focus on interoperability and solving important problems associated with it.

Zhang et al. [6] examined the privacy and security elements of healthcare blockchains, examining the dangers, needs, and solutions associated with the sharing of digital health information. The intention of the survey is to give developers and healthcare experts some insights. Tao and Ling [7] presented a blockchain-based medical file-sharing system that supports multi-person choices and dynamic updates and has decentralized attribute-based encryption for privacy. Andola et al. [8] through the use of the Ethereum blockchain, SHEMB offers a safe healthcare management solution that guarantees patient autonomy, privacy, and quick access. Its usefulness is confirmed by experiments. Itnal et al. [9] focused on employing blockchain technology to secure patient data in the healthcare industry while maintaining confidentiality, security, and trust. Ghazal et al. [10] with 0.93 training and 0.91 validation accuracy, a blockchain-based encryption framework that makes use of computational intelligence improves security in E-health monitoring systems.

Islam and Shin [11] suggested "BHEALTH," a safe healthcare program that makes use of body sensors, UAVs, and blockchain. Its benefits and viability are supported by performance and security assessments. Lin et al. [12] suggested an invisible proxy re-encryption technique based on blockchain

guarantees the private and secure exchange of e-healthcare data. The plan keeps situations under wraps, ensures precise outcomes, and shows that it is practically feasible. Zou et al. [13] displayed SPChain is an Ethereum-based electronic health system that tackles EMR sharing issues. It demonstrates viability and efficacy by guaranteeing privacy, fast throughput, and resilience to threats. Liu et al. [14] decentralized, tamper-resistant, and private elements of the proposed hospital's blockchain-based private plan improve EHR. Matching symptoms to patients enables safe patient communication. Chen et al. [15] offered a blockchain-based medical information system that ensures the secure collection, archiving, and sharing of SHR and EMR data. The solution satisfies realistic criteria for medical manufacturing and is built on Hyperledger Fabric.

Swetha et al. [16] provided decentralized healthcare solutions and is well-known for protecting sensitive data. Permission control, efficiency, and secure EHRs are guaranteed. Xu et al. [17] described Healthchain, a system built on a blockchain foundation that protects sensitive health data, provides smart healthcare systems with individual-level access control, and prevents corruption. Xu et al. [17] introduced Healthchain, a blockchain-based system designed to protect sensitive health data, provide individual-level access control for smart healthcare systems, and prevent data corruption. Madine et al. [18] addressed current problems with PHR management solutions by introducing Ethereum blockchain-based smart contracts for decentralized, traceable, and safe control of patient medical records. Sharma et al. [19] demonstrate that Blockchain-based Electronic Health Records (EHRs) offer private and secure solutions that ensure data management and accessibility, thereby advancing medical research. Sharma et al. [19] proposed blockchain-based Electronic Health Records (EHRs) that offer private and secure solutions, ensuring efficient data management and accessibility while advancing medical research. Balasubramanium et al. [20] examined ways to prevent assaults on healthcare data security, highlighting the effectiveness of Blockchain storage, shared key encryption, and privacy-preserving methods for authorized user access in cloud computing.

Mubarakali [21] employs attribute-based encryption, ensuring that the Secure and Robust Healthcare-based Blockchain (SRHB) solution allows for the safe transfer of healthcare data. Future updates may explore privacy-preserving aspects of e-commerce strategies. Mubarakali [21] introduced the Secure and Robust Healthcare-based Blockchain (SRHB) solution that ensures the safe transfer of healthcare data using attribute-based encryption. Future updates may explore privacy-preserving strategies for e-commerce. Durga et al. [22] improved security in the IoT ecosystem by developing a blockchain-based chaotic encryption architecture. Future work may investigate expanding this architecture for networks enabled by 5G. Durga et al. [22] developed a blockchain-based chaotic encryption architecture to enhance security in the IoT ecosystem. Future work may explore expanding this architecture for 5G-enabled networks. Saha et al. [23] suggested access control approach utilizes private blockchain technology to facilitate safe data exchange across reputable hospital authorities for IoT-enabled healthcare applications. The method offers minimal communication and computing costs, better security features, and resilience against known threats. Li et al. [24] put out a Blockchain-based data aggregation plan with a focus on group authentication for authorized users and patient privacy in situations involving remote medical monitoring. Yadav et al. [25] promoted the confidence in patient reports that have been kept by highlighting the significance of utilizing blockchain technology to secure health data and stressing data chunking, hash chains, and two-way authentication for physicians' access.

Wang et al. [26] outlined a blockchain-based plan for the sharing of information that addresses access control, privacy, and keyword search problems. Christo et al. [27] highlighted the use of quantum cryptography, AES, and SHA algorithms for data retrieval, encryption, and authentication while introducing blockchain for safe patient medical reports. Kumar et al. [28] presented "BDSDT," a secure data transmission system that combines IPFS, blockchain, Zero Knowledge Proof, and deep learning for intrusion detection in healthcare that is enabled by the Internet of Things. Better performance is demonstrated by the experimental findings. Villarreal et al. [29] explained how to strike a balance between security and interoperability in healthcare systems using blockchain technology. Blockchain is taken into account for security and interoperability in the metaverse in future development. Kamal et al. [30] suggested the use of the Internet of Medical Things to create a safe, remote patient monitoring system (IoMT). Compared to current models, it exhibits better efficiency and security because of the use of consortium blockchains, cancellable biometrics, and encrypted data transfer. Table 1 presents summary of important findings. From the literature, it is observed that improving the protection of data stored in blockchain with secure and privacy-preserving techniques is desired.

Table 1. *Summary of important findings*

Reference No	Approach	Technique	Limitation
[1]	Searchable attribute-based encryption	Data sharing	Full use of blockchain technology is yet to be achieved
[5]	decentralized approach	key distribution techniques	In future, they intend to improve it with mechanisms to deal with key theft.
[7]	Decentralized Attribute-Based Encryption	medical file sharing scheme based technique	Zero-knowledge proof and proxy encryption are yet to be implemented.
[11]	Blockchain- based approach	BHEALTH adopted hybrid encryption techniques	Needs further improvement of BHEALTH for protecting privacy.
[13]	Blockchain- based approach	AI techniques	Communication overhead and low throughputs are issues to be addressed.
[18]	Blockchain- based approach	Reputation system technique	The solution is generic in nature and need improvements to adopt it for different blockchain networks
[21]	Secure and Robust healthcare- based Blockchain) approach	Privacy-preserving techniques	Privacy preserving enhancement is desired.
[28]	Deep Learning approach	BiLSTM	Needs improvement in IoT enabled healthcare context.
[29]	MDE approach	Reflection techniques	Metaverse in blockchain in the intended future scope
[30]	Blockchain based two stage federated learning approach	Cancelable biometric technique	To be extended to realize real-life secure health monitoring system.

3. Proposed Security Framework

This section presents a security framework and different algorithms defined for secure data storing and sharing in healthcare blockchain applications.

3.1 Framework

The proposed security framework depicted in Figure 1 incorporates different algorithms to realize secure data storage in blockchain and share it with other authorized users. To implement the framework, we use both symmetric and asymmetric encryption systems for different purposes instead of depending solely on one type of encryption technology. To implement the framework, both symmetric and asymmetric encryption systems are utilized for different objectives rather than relying solely on a single encryption technology. In the proposed system, the variable k_{sym} represents the private key, which is also referred to as the symmetric key in our methods. Both encryption and decryption are possible with this key, on both ends of the communication. There will be one key pair for an asymmetric encryption sender ($sk_{s_{priv}}$, $sk_{s_{pub}}$), and another pair of keys will be sent to the recipient (rk_{priv}, rk_{pub}). The receiver's public key rk_{pub} is used for encryption and the receiver's private key rk_{priv} is used for decryption . For the regular data file, we often use the acronym plaintext (P), while for the encrypted data file, we use ciphertext (C). The proposed framework uses AES-GCM (Advanced Encryption Standard - Galois/Counter Mode) as a cryptographic primitive for encryption/decryption of the data because of its more advanced properties relevant to secure data sharing for blockchain-based healthcare systems. AES-GCM is a well-known high-performance, secure, authenticated encryption algorithm that is commonly used to protect sensitive data such as healthcare data. It encrypts the data for confidentiality and contains an integrated authentication mechanism that ensures data integrity. The AES-GCM encryption process starts in this framework from an unique secret key generation which is used for symmetric encryption. The secret key is used to encrypt the plain healthcare data and create ciphertext. During decryption the tag is used to check that the data has not been tampered with and this tag is created by the mode of operation (Galois/counter mode (GCM)) which is used here along with AES. This ensures that if any such tampering or unauthorized changes are made with the data, then it is detected, which increases the security of the system. This secret key is encrypted asymmetrically with the public key of the recipient, allowing only them to decrypt it and access the key. This secret key (encrypted), as well as the ciphertext, is then saved on the blockchain in a safe manner. By using asymmetric and symmetric cryptography, this dual encryption method obtains a high level of both security and efficiency.

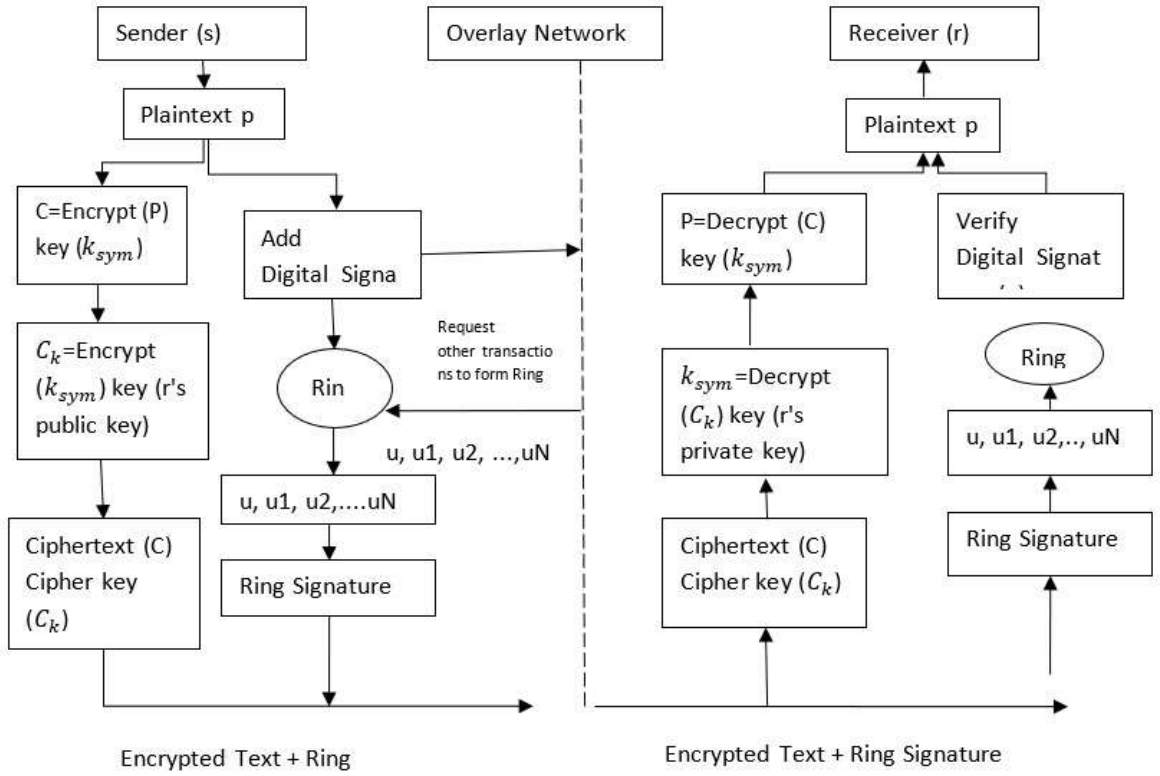

Figure 1. *Proposed security framework for healthcare data security and sharing in blockchain*

The AES-GCM is widely used in healthcare blockchain because it allows working with extensive datasets due to the high efficiency of encryption and authentication measures while supporting a high level of security assurance. With its authenticated encryption capability, this is an important tool to protect the integrity of electronic health records (EHRs) at rest and in transit, and is a solution needed to meet compliance with regulated healthcare data. In addition, the computation cost of AES-GCM is low, making it suitable to be deployed in resource-constrained devices such as IoT-based medical sensors and wearables which are normally used in remote patient monitoring systems. To achieve a compromise between security and performance, the framework integrates AES-GCM, using this mechanism to share healthcare information securely, reliably, efficiently, and without compensating the security provided by modern healthcare systems driven on blockchain technology. Using AES-GCM with elliptic curve cryptography supports modern application requirements and features that make it best practice.

3.2 Ring Signature

Ring signatures serve as essential components in the proposed framework enabling secure data sharing while preserving privacy in blockchain-based healthcare systems and guaranteeing both data privacy and anonymity. Ring Signatures are a type of, Digital signature scheme in which only a member (usually a person) can sign a message, however they only identify a subset (the "ring") of a group of signers (the actual signer remains indistinguishable within the ring) Such a cryptographic technique is useful for the cases where owners of the data need to be anonymous, i.e., for sharing sensitive healthcare data on multi-stakeholders. The ring signature mechanism is used to hide the ids of data owners when they enter their encrypted medical healthcare data with legal users. The first step is that the system generates a "ring" with public keys from multiple participants together with the data owner.

The data owner signs the transaction using their private key, but the signature looks indistinguishable from a signature created by another member of the ring (computationally). It keeps the identity of the actual signer private thus protects the data owner.

The use of ring signatures in the proposed framework yields two key security properties: signer anonymity and signature soundness. Therefore, if any adversary has access to all public keys in the ring, it will never be able to determine who the actual signer is. This is especially essential in healthcare, where the confidentiality and privacy of the data owner must be preserved to address ethical and legal concerns. The incorporation of ring signatures in the proposed framework ensures two key security properties: signer anonymity and signature soundness. Even if an adversary gains

access to all public keys within the ring, identifying the actual signer remains impossible. This feature is particularly vital in healthcare applications, where maintaining the confidentiality and privacy of data owners is essential to comply with ethical and legal standards. The signature correctness ensures that the signature is correct and relates to one of the public keys in a given ring, assuring the receiver that the data came from any of the users in the ring. Based on the aforementioned proposed framework, the secure distribution of a symmetric encryption key (used to encrypt the health care data) employs a combination of ring signatures and Diffie-Hellman (DH) key exchange. This dual-layer attribute adds to general security that guarantees that if the key is captured during travel, still the actual ID of the data owner will not be revealed.

Furthermore, the use of ring signatures enables private health records to be shared anonymously with both patients and providers through decentralized systems like blockchain networks. This approach allows for the duplication of shared data without disclosing the identities of the data providers to other participants in the network. Additionally, the use of ring signatures enables private health records to be shared anonymously with both patients and providers over decentralized systems such as blockchain networks, allowing data to be duplicated without revealing the identity of the data providers to other network participants. Such a feature is extremely useful as this allows multi-party collaborations, like a research study, to aggregate data from multiple healthcare providers without sacrificing anonymity. A proposed security framework based on ring signatures for data sharing has been built, which besides being highly anonymous, trustful, and difficult to verifiably hack, is therefore also very robust for secure data sharing in blockchain-driven healthcare applications. Such a model preserves the privacy of sensitive health information and alleviates privacy concerns, promoting wider participation and collaboration among stakeholders.

3.3 Digital Signature

To ensure authenticity, a digital signature is appended to the information. A set of public and private keys belongs to each user. It is common practice to utilize different key pairs for encryption and decryption than for signing and verifying. One key pair ($sk_{s_{priv}}$, $sk_{s_{pub}}$), will belong to the sender in this scenario, while the receiver will have a different key pair (rk_{priv}, rk_{pub}). The data is signed using the sender's private key, $sk_{s_{priv}}$ which is also referred to as the signature key. On the receiving end of the transmission, the sender's public key, $sk_{s_{pub}}$ is utilized for verification. After the signer sends the data, a hash value is computed. Next, the hash value $hash_p$ of the plaintext and the signature key is sent to the $sk_{s_{priv,}}$ and the resultant ciphertext is transmitted. The verifier uses the same hash function to produce the hash value, or $hash_r$ for the data it receives during the verification process. Additionally, the verifier uses the signer's public key and the verification procedure to retrieve the original hash value, or $hash_p$ plaintext. When $hash_p$and $hash_r$ have the same values, it confirms that the data remains unchanged during transmission.

Ring signature technology is utilized, which enables signers to sign anonymous data. No one knows who signed the communication except the real signer since the signature is jumbled up with those of other organizations (referred to as the "ring"). Rivest made the initial proposal for Ring Signature in 2001 [19]. A user submits a transaction mixing request to the blockchain network, including their public key pks. Upon receipt, the network collects public keys pk1,pk2,pk3,pk4 from other users (u1,u2,…,uN), along with pks, and sends them as part of the mixing process. This approach uses ring signatures to achieve two significant security characteristics: signer anonymity and signature correctness. The public key must be sent over the network in the suggested scheme The public key is also covertly distributed to further enhance data security. In order to securely distribute the public key $sk_{s_{pub}}$ to the entire network using the scheme named Diffie-Hellman.

A digital signature is one of the key components of the designed security framework that provides a guarantee of data authenticity, integrity, and non-repudiation for secure data storage and sharing in blockchain-based healthcare systems. It is used to ensure that the data was sent by a verified source and was not previously modified while in transit or at rest. Every data owner gets a unique pair of the private and the public key — the private key is used to generate the digital signature, while the public key is used to verify it. For example, when data is shared, the sender first signs the data with their private key, and the recipient uses the sender's public key to validate the signature. By doing this, it prevents impersonation attacks for an end user and builds trust between the parties.

In addition, digital signatures make it possible to detect any tampering with the data during transmission or while at rest. By signing the data, a hash of the data is created and encrypted with the sender's private key, and this forms the signature.

On the side of the receiver, the same hash function is applied to the data that has been received, and its digest is compared to the digest decrypted from the signature. Matching hashes can confirm that the data are in an unaltered state and the integrity of sensitive healthcare data such as electronic health records (EHRs) is then maintained. As an added benefit, signing with the sender's private key also provides non-repudiation, as the sender cannot deny sending the data. This particular feature is significantly important in healthcare applications where traceability is essential, like sharing medical prescriptions, diagnostic reports, or inter-hospital data sharing.

Digital signatures that secure transactions in the blockchain-based system also protect additional transactions in that only authenticated and authorized transactions can be logged in the blockchain. It makes the decentralized ledger more trustworthy and secure. Moreover, digital signatures are combined with ring signatures in the proposed framework, thus providing the data owner with optional anonymity. Ring signatures provide added privacy in sensitive data-sharing scenarios, where although the digital signature verifies the provenance and integrity of the data, it is actually only the identity of the signer that can be obscured in a group.

The digital signature mechanism collaborates with the Diffie-Hellman key exchange to securely transfer the symmetric key used for data encryption. This combination of mechanisms guarantees that the keys which are being exchanged are authentic, and that they cannot have been intercepted or tampered with by an eavesdropping entity with malicious intent. The combination of digital signatures along with these sophisticated cryptographic methods offers a powerful and effective approach to ensure both security and reliability with data sharing in healthcare uses of blockchain technology. Digital signatures are critical in solving the security-related issues of sensitive healthcare management and sharing due to their unique features of authenticity, integrity, and non-repudiation.

3.4 Secure Key-Sharing Process in the Proposed Framework

The key-sharing process of the proposed framework is a crucial component that ensures the secure transfer of the symmetric key used to encrypt healthcare data. Using this method, a mixture of asymmetric cryptography and the Diffie-Hellman (DH) key exchange is used to share keys between entities who are legally permitted to see them while keeping everything else safe. The sender generates a unique symmetric key in the key-sharing process for encrypting the healthcare data. Next, we get that symmetric key encrypted with the public key of the receiver, so only the owner of a private key can decrypt the symmetric key. This method makes sure that the symmetric key cannot be obtained in transmission time if the communication channel is compromised.

As an additional security measure, the Diffie-Hellman key exchange is integrated into this framework. In this approach, both sender and receiver agree on two numbers known to everyone: a big prime number and a base (generator). Then, each party selects a private secret number and calculates the public value, which is the base raised to the secret number mod prime. The two parties exchange these public values, and each derives the shared secret key by computing the received public value raised to the power of their private secret number (modulo the prime). This common secret is employed to generate the symmetric encryption key. Diffie-Hellman key exchange will secure the mechanism of sharing the symmetric key so that the key is not transmitted in clear text.

To provide optional anonymity, the mechanism of ring signature is also incorporated into the key sharing. Anonymous message — In this method, the sender will hide his signature by mixing it with the signature of others (other nodes in the network node). It ensures that the new receiver can access the shared key without revealing the sender’s identity, maintaining privacy and security. It enables the new receiver to access the shared key without revealing the sender's identity, ensuring confidentiality. The proposed framework has a series of steps that need to be carried out (1) creating the symmetric key, (2) performing asymmetric encryption using the public key of the recipient, (3) sharing the symmetric key through the Diffle-Hellman method, and (4) applying a ring signature for anonymity if necessary. The asymmetric encryption combined with the Diffie-Hellman key exchange embodies these two layered approaches, such that the symmetric key is safeguarded from interception, unauthorized access and tampering. With these mechanisms, the proposed framework not only ensures highly secured and efficient key sharing, but also significantly facilitates encrypted data storage and secure sharing in blockchain-based healthcare systems. It guarantees that only the intended receivers can decrypt and read sensitive healthcare data, safeguarding the privacy of the system.

3.5 Proposed Algorithms

Using the symmetric key $k_{sym}$and, we encrypt the data file in our encryption algorithm 1 and create a file C with ciphertext. Following encryption, we encrypt the key k_{sym} via the use of public key cryptography and apply the twofold encryption approach. The symmetric key is encrypted by us k_{sym} and using the recipient's public key, $rk_{pub}$and transmit the key encrypted using ciphertext C. We use $C_k$to represent the symmetric key that is encrypted.

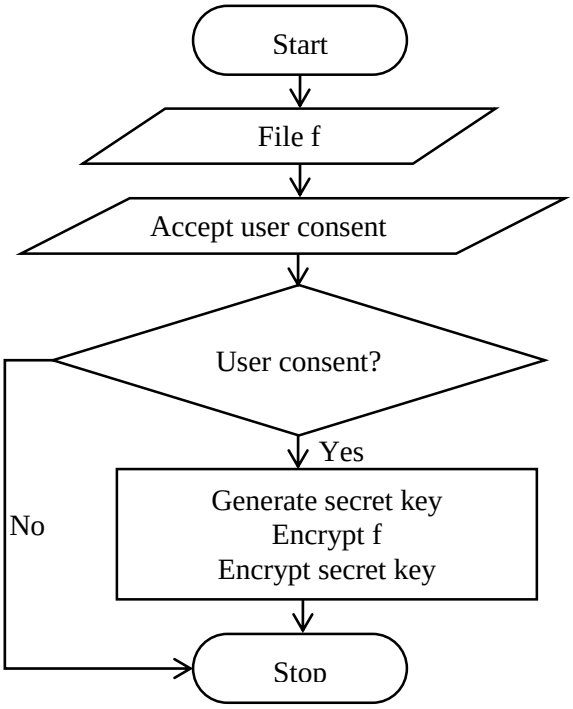

Figure 2. *Flowchart of encryption process*

As presented in Figure 2, the encryption process is visualized using flowchart. It takes given file with plaintext as input and generates encrypted file encrypted key.

Algorithm 1. *Encrypt*

Algorithm 1: Encrypt
Input: File f
Output: Encrypted file C and encrypted key C_k

1. Begin
2. userConsent←getUserConsent() //for storing in blockchain
3. If userConsent=yes Then
4. k_{sym}←generateSecretKey()
5. C←symmetricEnc(f, k_{sym})
6. C_k←asymmetricEnc(rk_{pub}, k_{sym})
7. End If
8. End

Two keys ($sk_{s_{pub}}$, $sk_{s_{priv}}$) that are distinct from the encryption/decryption keys can be used by senders for the electronic signature. The hash function receives the data file from the sender first, generate hash, denoted as $hash_p$, of the data, before adding the digital signature. Next, user uses his private key $sk_{s_{priv}}$ to sign the data, providing the hash value $hash_p$ and the value of the Signature Algorithm's secret key. Data on the receiving end may be verified using the signer's public key, $sk_{s_{pub}}$ we incorporate the ring signature into our Algorithm 2 in order to apply the patient's or user's anonymity.

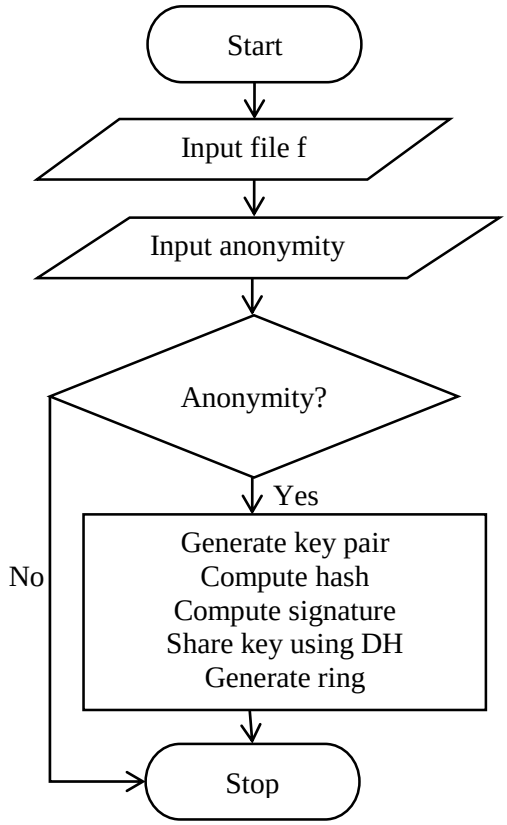

Figure 3. *Flowchart of key sharing process*

A flowchart of the key-sharing process in visual form is shown in Figure 3. According to Figure 3, the key sharing process is visualized using flowchart. It takes given file with plaintext as input and generates key pair, hash, signature and ring.

Algorithm 2. *Key Sharing*

Algorithm 2: Key Sharing
Input: File f
Output: Key pair, hash, signature, ring

1. Begin
2. anonymity←getUserAnonymity ()
3. If anonymity=yes Then
4. ($sk_{s_{pub}}$, $sk_{s_{priv}}$)←generateKeyPair ()
5. hash←computeHash(f)
6. signature←createDigitalSign(hash, $sk_{s_{priv}}$)
7. Using DH share $sk_{s_{pub}}$ to receiver
8. ring←mixSign(networkgroup)
9. End If
10. End

In order to add ring signatures to transactions the user will look up other accounts on the network that have the same want. After that, a list of network users willing to use ring signatures will be sent to them. After that, transactions are merged with those of other users prior to forwarding. None can figure out who first signed with the ring gang. The block diagram of the model (Figure 1) explains the procedure.

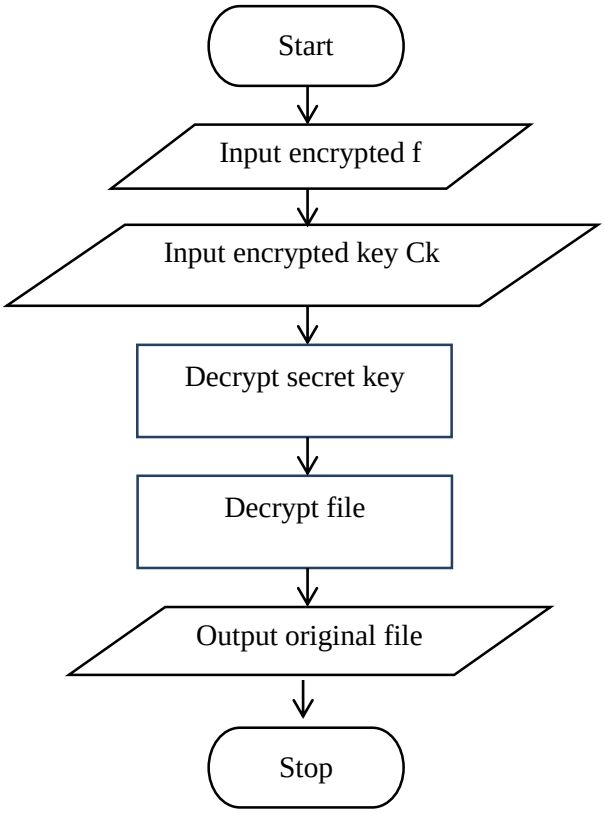

Figure 4. *Flowchart of decryption process.*

As presented in Figure 4, the decryption process is visualized using flowchart. It takes given cipher text and encrypted key as inputs and perform decryption of encrypted file to acquire the original file.

Algorithm 3. *Decrypt*

Algorithm 3: Decrypt
Input: C, C_k
Output: f

1. Begin
2. k_{sym}←asymmetricDec(rk_{priv}, C_k)
3. f←symmetricDec(k_{sym}, C)
4. End

The symmetric key ksym, as shown in Algorithm 3, is required to convert ciphertext into plaintext. Only the receiver's private key, 〖rk〗_priv could decrypt the key as it is in encrypted form. Using the receiver's private key 〖 rk〗_priv, we first decode the Ck in order to obtain the secret key, k_sym. Then that key is utilized for converting cipher text to plain text.

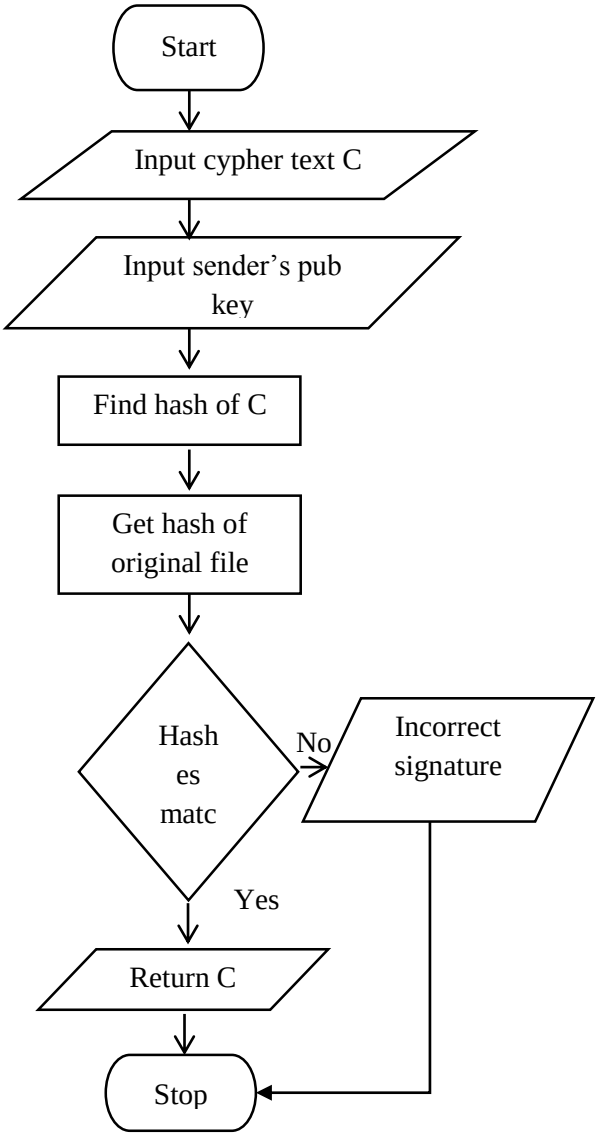

Figure 5. *Flowchart of verification process*

As presented in Figure 5, the verification process is visualized using flowchart. It takes given cipher text and sender's public key as inputs and perform verification for data integrit.

Algorithm 4. *Verify*

Algorithm 4: Verify
Input: C, $sk_{s_{pub}}$
Output: Verification results

1. Begin
2. $hash_c$←findHash(C)
3. $hash_p$←findHashOfSenderFile($sk_{s_{pub}}$)
4. If $hash_p$=$hach_c$ Then
5. C is returned
6. Else
7. Display "Incorrect signature"
8. End If
9. End

In the process of verification, a hash value denoted as, $hach_c$, is generated of incoming data (ciphertext) as in Algorithm 4. Additionally, the hash value $hash_p$ of the original data (plaintext) is recovered by the verifier by entering the digital signature hash value correctly. Public Key Infrastructure (PKI) is a complicated and hefty system. Thus, the lightweight Diffie-Hellman method is used, where a secret key is automatically calculated between two parties instead of exchanging keys. The following is the essential exchange with DH. Two prime numbers, n (11) and g (7), are decided upon by two parties involved in the conversation and can be made public. After selecting a secret number X, sender calculates $A = g^X$ then forward it to receiver. Likewise, receiver selects a secret number Y and calculates $Y = g^Y$ then forward it to sender. Next, sender calculates $K1 = B^X$ and receiver calculates mod n $K2 = A^Y$ mod n. K1=K2 indicates that the key exchange is successful.

3.6 Block Validation in the Proposed Framework

Given the aforementioned framework, the block validation in the blockchain is an important process to guarantee the integrity, authenticity and consistency of the healthcare data stored in blockchain. There are different steps in the approval of block validation which together form a pipeline to ascertain only the valid blocks can be added to the blockchain unaffected to any tampering. Below is an elaboration of the process that validation of the block follows in the designed framework: Validation starts from block header by checking the block header, which contains metadata such as the timestamp, previous block hash, nonce, and Merkle tree root. This metadata is then used to recalculate the hash of the block which is then compared to the hash given in the block. If the two hashes are the same, the block is checked for integrity, which means the contents of the block have not been modified in any way. Then the framework verifies the proof-of-work (PoW) or proof-of-stake (PoS), if it uses this consensus mechanism, of the block using the specific blockchain protocol used. In PoW, the current nonce in the block is validated by calculating the hash again and ensuring that it meets the difficulty level set by the network. This mechanism makes it more difficult to create fake blocks because it makes sure that a mined block is created with computational effort.

Afterwards, the digital signatures of the many transactions in the Block are checked. If a transaction's digital signature is validated with the sender's public key, it means that the data was received from a legitimate user and it was not changed on the way to the other side. It ensures that each block only carries legitimate, confirmable transactions. It also verifies the ring signatures from anonymous transactions. In this method, ring signatures are verified to ensure accurate obfuscation of the data owner's identity while keeping the transaction valid. This allows for user privacy while also proving that their signed data is from one of the designated members of a ring. This Merkle root, stored within the block header, is used to validate the integrity of this block's transactions. By using Merkle tree, it computes the Merkle tree structure with the transactions in the block and compares its root with the stored Merkle root. Then, if those two values match, it indicates that none of the transactions on that block have been altered, and the data must remain unchanged.

Finally, the block undergoes a protocol compliance check where the structure & format of the block is checked against the set protocols defined by the blockchain. Ensuring that the size of the block, the number of transactions and any other constraints that might be specified by the blockchain system, are not broken. If a block qualifies all these verifications, it is deemed valid and is allowed to be added to the blockchain. The blockchain itself is also a secure, tamper-proof cluster of data due to this rigorous passing process, which is vital to the healthcare industry where sensitive patient information needs to be handled safely. Incorporating such validation steps in the proposed framework allows the system to have the secure sharing of data between various healthcare stakeholders while ensuring the integrity of the blockchain [24].

3.7 Role of Hash Function in the Proposed Framework

To ensure persistence and security of data related to healthcare, a cryptographic hash function is used in the proposed framework which is SHA-256 (Secure Hash Algorithm 256-bit). SHA-256 (Secure Hash Algorithm 256) This is one of the most well-known hash functions among them. It creates a fixed-size 256-bit (32-byte) hash value from input data of any size. This means it is computationally infeasible for two different inputs to generate the same hash value; i.e., it is collision-resistant. This feature is particularly important for blockchain systems, where it is critical to preserve the integrity and authenticity of data. Creating a hash with SHA-256 starts with message preprocessing. First, the input message (in this example, the healthcare data) is converted into binary. The binary message is then padded such that its length is a multiple of 512 bits.

Padding is adding one '1' binary digit, then the required number of '0' binary digits, and finally the length (in bits) of the original message (in binary, 64 bits). After padding the message, it breaks the data up into 512-bit chunks for digest computation. The way SHA-256 works is by first initializing 8 hash values, which are constants related to the fractional parts of the square root of the first eight prime numbers. One 512-bit block is processed in 64 rounds. In these rounds, a sort of message schedule expands it into 64 words. The message schedule and intermediate hash values are manipulated via logical functions (Ch, Maj, Σ0, Σ1) and bitwise operations. The process also includes constants calculated from the prime numbers 1 through 64 (taken to the cube root, actually). These operations result in the iterative update of the eight hash values. Once all blocks are handled, the last hash value is calculated based on the updated hash values, thereby turning into a unique 256 bits of hash.

The proposed framework makes use of SHA-256 for a number of different functions. It guarantees the integrity of the healthcare data in digital signings, where the data hash is signed with the private key of the sender. At verification, the hash is computed again and the newly calculated hash is compared with the signed hash and thus, ensures that the contents remain unchanged. Block validation is another important function of SHA-256 in the blockchain as the hash of the previous block is stored in each block and calculated by the SHA-256 algorithm. This chaining of blocks means that if you take a single block and alter it, all blocks after it are then invalid in the chain, which is what makes it tamper proof. n the proposed framework, SHA-256 is used to enhance system security by ensuring the data remains unchanged, it guarantees the data is intact, authenticating the transactions and creating a foundation for the healthcare applications that are driven on blockchain. Hashing — Well, this powerful hashing tool solves the problem of data protection and integrity (the need of the hour) intensively required in sensitive environments such as healthcare.

4. Experimental Results

The experimental results assess the suggested security framework from presumed real-world settings containing identifiable healthcare records in a de-identified manner utilizing the MIMIC-III Clinical Database. As a comparison for efficient encryption, AES-GCM; secure key exchange, Diffie-Hellman; and asymmetric encryption, RSA were used as state-of-the-art models (Johnson et al., 2016; Rivest et al., 1978). The experiments were performed in a controlled environment using an Intel Core i7 processor with 16GB of RAM and Python-based cryptographic libraries. The assessment covered considered the encryption/decryption time, key-sharing, and security strength, so that the performance of the proposed framework can be compared with existing approaches to ensure robustness and scalability of healthcare systems.

4.1 Dataset Used for the Application

The MIMIC-III Clinical Database [31], the most publicly used and available dataset for healthcare-based research, was utilized to evaluate the proposed security framework, as well as the algorithms behind it. Abstract MIMIC-III is a freely accessible critical care database that comprises health-related data associated with more than 40,000 patients, including information on their diagnosis, procedures, gender, and medications. It is also a realistic dataset of Electronic Health Records (EHRs) that we use in our setting & is suitable for simulating the secure storage and sharing of healthcare data on a blockchain and cloud setting. The dataset was used to simulate a realistic scenario of storing and sharing sensitive patient data across various healthcare providers, Ethics Statement: The dataset is completely de-identified to maintain privacy, and access was granted upon signing the appropriate data use agreement from the database managers. In the testing process, the framework proposed the encryption, decryption, and secure key-sharing mechanisms considering key attributes including patient IDs, age, gender, diagnosis, prescriptions, and treatment records.

The MIMIC-III dataset was divided into several blocks, with each block corresponding to a batch of transactions. As part of this, upon blocks being stored in the blockchain, that blocks are encrypted by the AES-GCM algorithm first, to provide confidentiality and integrity. Transactions were authenticated using digital signature and ring signature to meet the anonymity requirements. The Diffie-Hellman key exchange method was also used to securely exchange the symmetric encryption keys between the routers. Using this dataset, the performance of encryption and decryption time, key-sharing and system security can be measured for the proposed framework. MIMIC-III Clinical Database serves as a realistic as well as challenging testbed to evaluate the effectiveness and utility of the proposed framework in practical healthcare settings. This selection of the dataset shows the strength of the framework to work with sensitive healthcare data in secure way

while enabling efficient sharing in blockchain-enabled environments.

4.2 Results

A prototype application is built for empirical study of the proposed framework and underlying algorithms. Particularly evaluation of encryption and decryption algorithms are evaluated with different workloads. The workloads are measures in Mega Byte (MB) scale. In addition to the execution time required by the proposed and existing cryptographic primitives, security analysis is made to know the strength of the algorithms in terms of their level of security when applied to data of data owners. Figure 6 shows performance of proposed algorithm compared with existing ones in terms of time required for encryption.

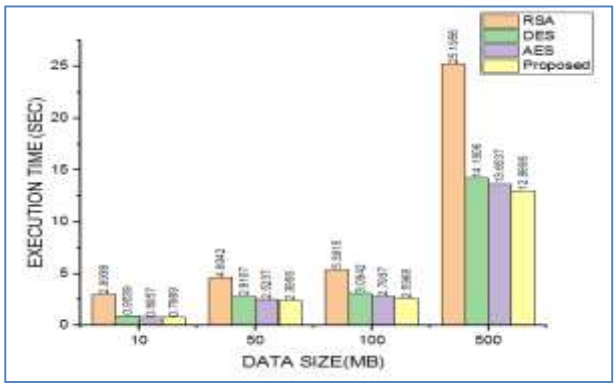

Figure 6. *Time taken for encryption done by different algorithms against varied workloads*

The encryption time is measured in seconds. It was observed that there is linear increase in execution time as there is increase in workload. Another observation is that each cryptographic primitive has shown different time required for encryption of given data. The rationale behind this is the underlying modus operandi of each algorithm. When 50 MB data is encrypted, RSA required 4.6 seconds, DES 2.8 seconds, and AES 2.5 seconds while the proposed algorithm needed 2.3 seconds. This kind of trend in execution time is reflected with all workloads.

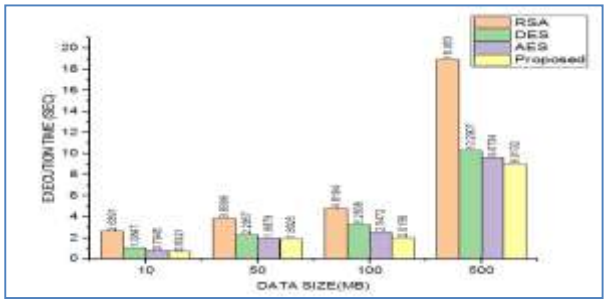

Figure 7. *Time taken for decryption done by different algorithms against varied workloads*

The least execution time for encryption is exhibited by the proposed algorithm. Figure 7 shows performance of proposed algorithm compared with existing ones in terms of time required for decryption. The decryption time is measured in seconds. It was observed that there is linear increase in execution time as there is increase in workload. Another observation is that each cryptographic primitive has shown different time required for decryption of given data. The rationale behind this is the underlying modus operandi of each algorithm. When 50 MB data is decrypted, RSA required 3.8 seconds, DES 2.2 seconds, and AES 1.9 seconds while the proposed algorithm needed 1.8 seconds. This kind of trend in execution time is reflected with all workloads. The least execution time for decryption is exhibited by the proposed algorithm. Figure 8 shows security strength of proposed algorithm compared with existing ones

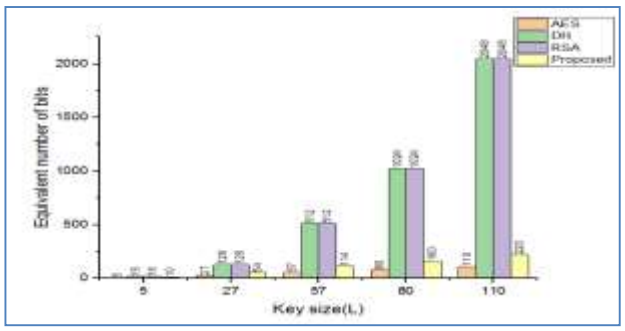

Figure 8. *Security strength of algorithms against key size in terms of equivalent number of bits*

In cryptography, it is known fact that key size has its impact on level of security. Provided this proposition, security strength analysis is made in terms of equivalent number of bits against key size. In horizontal axis, key size is provided in terms of number of bits (denoted as L). The vertical axis shows the equivalent number of bits required for given cryptographic primitive to provide same level of security. In other words, it is considered to be equivalent number of bits for which reverse computation of key is made in equal amount of time for all considered cryptographic algorithms. The base algorithm considered here is AES. With key size 5, AES required 5 bits to provide equivalent security, DH needed 16 bits, and RSA also required 16 bits while the proposed algorithm required only 10 bits to provide equivalent security. With key size 27, AES required 27 bits to provide equivalent security, DH needed 128 bits, and RSA also required 128 bits while the proposed algorithm required only 54 bits to provide equivalent security. With key size 57, AES required 57 bits to provide equivalent security, DH needed 512 bits, and RSA

also required 512 bits while the proposed algorithm required only 114 bits to provide equivalent security. With key size 80, AES required 80 bits to provide equivalent security, DH needed 1024 bits, and RSA also required 1024 bits while the proposed algorithm required only 160 bits to provide equivalent security. With key size 110, AES required 110 bits to provide equivalent security, DH needed 2048 bits, and RSA also required 2048 bits while the proposed algorithm required only 220 bits to provide equivalent security.

4.3 Comparison with the State of the Art

A comparison of the framework with state-of-the-art models referenced in this paper is provided in Table 2. This shows that execution time of the proposed framework outperform other framework in which AES-GCM is used for encrypting blocks, Diffie-Hellman with ring signatures used for consensus and Proof-of-Authority (PoA) is used for consensus. Data confidentiality, data integrity, data source non-repudiation, and user privacy can be guaranteed with the proposed approach with the lower encryption (2.3 seconds) and decryption (1.8 seconds) times for 50 MB data than the existing ones such as RSA and DES. Moreover, it promises very good scalability and strong data-sharing privacy, even far beyond the existing state-of-the-art methods by having the required efficiency and security level to address real health-care blockchain bottlenecks.

5. Discussion

The new security framework proposed in this research is necessary to enable secure and efficient data storage and sharing in healthcare applications based on blockchain technology. The layer uses AES-GCM that provides strong encryption with low computational overhead for both large volumes of data and resource-constrained IoT devices typically found in healthcare environments. Diffie-Hellman integrates with ring signatures to protect the anonymous identity of data owners and at the same time ensures that they are authentic and their data is secure [4]. It employs a Proof-of-Authority (PoA) consensus mechanism of the blockchain to achieve high throughput and low latency to meet the needs of strict real-time healthcare data processing.

The experimental results show that the framework is not only performs well but also scales very well, while significantly improving from state-of-the-art. Comparison of execution times with AES and RSA for 50 MB Last of execution times compared to AES and RSA for 50 MB size limit, exhibiting the superiority of execution times of the proposed algorithms over conventional encryption algorithms (AES, RSA and DES)in encryption as well as decryption times. Indeed, its scalability on progressively larger workloads and datasets such as MIMIC-III also reinforces the practicality of the framework.

The dual-layer approach to cryptographic mechanisms is one of the highlights of the framework. Thus, symmetric and asymmetric encryption not only protects health care data before these records are stored in the blockchain, but it also allows for sharing amongst authorized individuals in a secure and private fashion. Ring signatures are an additional way to hide the identity of data owners when they share sensitive information on the network. It has also integrated lightweight public key encryption, which can be made interoperable with different healthcare systems and devices. To summarize, our proposed

Table 2. *Qualitative analysis with state of the art studies*

Aspect	Proposed Framework	State-of-the-Art References
Encryption Algorithm	AES-GCM	RSA, DES, AES [1, 6]
Key Exchange Mechanism	Diffie-Hellman with Ring Signature	Basic Diffie-Hellman [20]
Consensus Algorithm	Proof-of-Authority (PoA)	Proof-of-Work (PoW), Basic Consensus [6]
Security Features	Confidentiality, Integrity, Non-repudiation, Anonymity	Confidentiality, Integrity [4]
Efficiency (Encryption Time)	2.3 seconds for 50 MB	AES: 2.5 seconds for 50 MB, RSA: 4.6 seconds [1]
Efficiency (Decryption Time)	1.8 seconds for 50 MB	AES: 1.9 seconds for 50 MB, RSA: 3.8 seconds [2]
Scalability	High (Tested with synthetic and MIMIC-III datasets)	Moderate (Limited to small datasets) [3]
Data Sharing Privacy	Ensured using Ring Signature and PKI	Partially Ensured (Focused on PKI only) [11]

framework aims to fulfil secure as well as efficient data sharing in blockchain-enabled healthcare applications. Due to these advantages, it could be an effective solution to overcome the weaknesses of current healthcare data security systems in the aspects of encryption efficiency, privacy, and scalability.

5.1 Limitations

The current study is limited to laboratory experiments to evaluate the proposed framework and algorithms. Application to real life blockchain driven healthcare applications is yet to be done. There is need for developing a comprehensive cloud-based data sharing system as the work in this paper has mechanisms to realize such sophistication in near future. Integration of the propped security framework to a blockchain healthcare application being used by corporate hospitals is an indispensable work yet to be done. These limitations could be considered as directions for future research.

6. Conclusion and Future Work

A resilient security framework specific to blockchain-based healthcare systems was proposed. that directly deals with the most important challenges of data sharing, storing, and privacy. Using AES-GCM for encryption, and a combination of Diffie-Hellman key exchange for key sharing, as well as ring signatures, the framework is able to guarantee data confidentiality, integrity, and anonymity. With PoA being the consensus algorithm used, fast transaction validation without latency is a key factor for these time-sensitive healthcare environments. The experimental results using MIMIC-III Clinical Database show that our approach is significantly faster (in both encryption and decryption), more scalable, and provides more information sharing privacy than the state-of-the-art methods. Its performance with big workloads and security makes the framework a suitable candidate for modern healthcare applications. This study has some limitations even though it has several strengths. The feature has been tested in a laboratory setting with synthetic and real-world datasets. Unknowns in actual deployment settings, especially on distributed health systems, remain. In addition, the framework provides a good level of security, however the overhead in terms of energy consumption and computational resources required by IoT devices should be further investigated. These limitations will be overcome in future work by instantiating the framework into live healthcare settings and testing its efficacy in a real-world context. Energy efficiency will be examined, with a focus on the IoT and edge computing landscape. It will also look at hybrid consensus mechanisms implementation, mixing Proof-of-Authority with Proof-of-Stake, in order to increase scalability and strength of resilience. The other major path is to broaden the framework to facilitate data sharing on a cross-border basis and to respond to various healthcare regulations such as GDPR and HIPAA. Such future work will serve to improve the framework such that it may be used more widely and will be more impactful in facilitating the secure management of healthcare data.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Niu, S., Chen, L., Wang, J., & Yu, F. (2019). Electronic health record sharing scheme with searchable attribute-based encryption on blockchain. *IEEE Access*. 7;164530-164542. https://doi.org/10.1109/ACCESS.2019.2959044

[2] Pournaghi, S. M., Bayat, M., & Farjami, Y. (2020). MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. *Journal of Ambient Intelligence and Humanized Computing*. 11;6857-6877. https://doi.org/10.1007/s12652-020-01710-y

[3] [Authors not provided]. (2021). Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System. *IEEE/CAA Journal of Automatica Sinica*. 8(12);1919-1932. https://doi.org/10.1109/jas.2021.1004003

[4] Shamshad, S., Minahil, Mahmood, K., Kumari, S., & Chen, C. M. (2020). A secure blockchain-based

e-health records storage and sharing scheme. *Journal of Information Security and Applications*. 55;102590. https://doi.org/10.1016/j.jisa.2020.102590

[5] Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems*. 95;511-521. https://doi.org/10.1016/j.future.2018.12.044

[6] Zhang, R., Xue, R., & Liu, L. (2021). Security and Privacy for Healthcare Blockchains. *IEEE Transactions on Services Computing*. 14(6);1741-1749. https://doi.org/10.1109/tsc.2021.3085913

[7] Tao, J., & Ling, L. (2021). Practical Medical Files Sharing Scheme Based on Blockchain and Decentralized Attribute-Based Encryption. *IEEE Access*. 9;127950-127960. https://doi.org/10.1109/access.2021.3107591

[8] Andola, N., Raghav, Prakash, S., Venkatesan, S., & Verma, S. (2019). SHEMB: A secure approach for healthcare management system using blockchain. *IEEE Conference on Information and Communication Technology*. 1-6. https://doi.org/10.1109/CICT48419.2019.9066237

[9] Itnal, S., Kannan, K. S., Suma, K. G., & Neelakandan, S. (2022). A secured healthcare medical system using blockchain technology. *Springer*. pp.1-8. https://doi.org/10.1007/978-981-16-7985-8_17

[10] Ghazal, T. M., Hasan, M. K., Abdullah, S. N. H. S., Abu Bakar, K. A., & Al Hamadi, H. (2022). Private blockchain-based encryption framework using computational intelligence approach. *Elsevier*. 23(4);69-75. https://doi.org/10.1016/j.eij.2022.06.007

[11] Islam, A., & Shin, S. Y. (2020). A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. *Computers & Electrical Engineering*. 84;106627. https://doi.org/10.1016/j.compeleceng.2020.106627

[12] Lin, G., Wang, H., Wan, J., Zhang, L., & Huang, J. (2022). A blockchain-based fine-grained data sharing scheme for e-healthcare system. *Elsevier*. 132;1-12. https://doi.org/10.1016/j.sysarc.2022.102731

[13] Zou, R., Lv, X., & Zhao, J. (2021). SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. *Information Processing & Management*. 58(4);102604. https://doi.org/10.1016/j.ipm.2021.102604

[14] Liu, X., Wang, Z., Jin, C., Li, F., & Li, G. (2019). A Blockchain-based Medical Data Sharing and Protection Scheme. *IEEE Access*. 7;118943-118953. https://doi.org/10.1109/ACCESS.2019.2937685

[15] Chen, Z., Xu, W., Wang, B., & Yu, H. (2021). A blockchain-based preserving and sharing system for medical data privacy. *Future Generation Computer Systems*. 124;138-152. https://doi.org/10.1016/j.future.2021.05.023

[16] Swetha, M. S., Pushpa, S. K., Muneshwara, M. S., & Manjunath, T. N. (2020). Blockchain enabled secure healthcare Systems. *IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)*. 1-5. https://doi.org/10.1109/icmlant50963.2020.9355970

[17] Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). Healthchain: A Blockchain-based Privacy Preserving Scheme for Large-scale Health Data. *IEEE Internet of Things Journal*. 6(5);8770-8781. https://doi.org/10.1109/JIOT.2019.2923525

[18] Madine, M. M., Battah, A. A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Pesic, S., & Ellahham, S. (2020). Blockchain for Giving Patients Control Over Their Medical Records. *IEEE Access*. 8;193102-193115. https://doi.org/10.1109/access.2020.3032553

[19] Sharma, Y., & Balamurugan, B. (2020). Preserving the Privacy of Electronic Health Records using Blockchain. *Procedia Computer Science*. 173;171-180. https://doi.org/10.1016/j.procs.2020.06.021

[20] Balasubramanium, S., Sivasankar, K., & Rajasekaran, M. P. (2021). A Survey on Data privacy and preservation using Blockchain in Healthcare organization. *International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. 1-6. https://doi.org/10.1109/icacite51222.2021.9404650

[21] Mubarakali, A. (2020). Healthcare Services Monitoring in Cloud Using Secure and Robust Healthcare-Based BLOCKCHAIN(SRHB)Approach. *Mobile Networks and Applications*. 25(4);1330-1337. https://doi.org/10.1007/s11036-020-01551-1

[22] Durga, R., Poovammal, E., Ramana, K., Jhaveri, R. H., Singh, S., & Yoon, B. (2022). CES Blocks—A Novel Chaotic Encryption Schemes-Based Blockchain System for an IoT Environment. *IEEE*. 10;11354-11371. https://doi.org/10.1109/ACCESS.2022.3144681

[23] Saha, S., Sutrala, A. K., Das, A. K., Kumar, N., & Rodrigues, J. J. P. C. (2020). On the Design of Blockchain-Based Access Control Protocol for IoT-Enabled Healthcare Applications. *IEEE International Conference on Communications (ICC)*. 1-6. https://doi.org/10.1109/ICC40277.2020.9148915

[24] Li, C. T., Shih, D. H., Wang, C. C., Chen, C. L., & Lee, C. C. (2020). A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System. *IEEE Access*. 8;173904-173917. https://doi.org/10.1109/ACCESS.2020.3025898

[25] Yadav, D., Shinde, A., Nair, A., Patil, Y., & Kanchan, S. (2020). Enhancing Data Security in Cloud Using Blockchain. *4th International Conference on Intelligent Computing and Control Systems (ICICCS)*. 753-757. https://doi.org/10.1109/ICICCS48265.2020.9121109

[26] Wang, S., Zhang, D., & Zhang, Y. (2019). Blockchain-based personal health records sharing scheme with data integrity verifiable. *IEEE Access*. 7;102887-102901. https://doi.org/10.1109/ACCESS.2019.2931531

[27] Christo, M. S., Anigo Merjora, A., Partha Sarathy, G., Priyanka, C., & Raj Kumari, M. (2019). An Efficient Data Security in Medical Report using Block Chain Technology. *International Conference on Communication and Signal Processing (ICCSP)*. 0606-0610. https://doi.org/10.1109/ICCSP.2019.8698058

[28] Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R., Jolfaei, A., & Islam, A. K. M. N. (2023). A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. *Elsevier*. 172;69-83. https://doi.org/10.1016/j.jpdc.2022.10.002

[29] Dulce Villarreal, E. R., García-Alonso, J., Moguel, E., & Hurtado Alegría, J. A. (2023). Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security. *IEEE*. 11;5629-5652. https://doi.org/10.1109/ACCESS.2023.3236505

[30] Kamal, R., Hemdan, E. E., & El-Fishway, N. (2023). Care4U: Integrated healthcare systems based on blockchain. *Elsevier*. 4(4);1-12. https://doi.org/10.1016/j.bcra.2023.100151

[31] Johnson, A. E. W., Pollard, T. J., Shen, L., Lehman, L. W. H., Feng, M., Ghassemi, M., Moody, B., Szolovits, P., Celi, L. A., & Mark, R. G. (2016). MIMIC-III, a freely accessible critical care database. *Scientific Data*. 3;160035. Available at: https://physionet.org/content/mimiciii/1.4/