Blockchain-Based Modified AES with Chaotic Random Key Generation for Secured E-Medical Data Sharing

M.Vinothkumar[1*], R. Saravana Ram [2]

[1]Assistant Professor, Department of CSE, Anna University, Madurai, Tamilnadu, India.

[2]Assistant professor, Department of ECE, University College of Engineering, Dindigul, Tamilnadu, India.

*Corresponding Author mail id: vinothkumardr2018@gmail.com

Abstract

The Electronic Medical Documentations have gained vitality and are stated as the pillar of digital healthcare. It is the main platform to store and retrieve the information of patients. It possesses numerous benefits like cost minimization, few medical errors with better healthcare access and tracking. Though the advantages and adoption of EMD have been extensively stated, the challenges entangled with their usage persist, particularly with the safety and integrity of the patient's data that are stored in the cloud. Conventional data sharing methods have been centralized and encountered problems of sole point-of-failure. Thus, a decentralized system is required where the blockchain concept comes into play. Moreover, protecting personal details from unauthorized entrée by guaranteeing data integrity is vital where cryptography gains its significance. Though traditional methods have used algorithms based on these concepts for secured EMD sharing, they lacked with regard for privacy and security. To rectify this problem, the objective of the present study proposes Modified-Advanced Encryption Standard based on the chaos random key generation. In a traditional AES system, a static key finds applicability which must be swapped in advance and assured to be maintained safely. Nevertheless, in the proposed model, a chaotic system's synchronization technology is introduced wherein the static key turns random and dynamic which avoids the need to be maintained or transferred in any open channels. Besides, a Modified Digest hashing algorithm is also used with M-AES for feeding the encrypted text and hash into data blocks. Performance of the proposed merging technique encompassing a hybrid pattern from both patient ID and medical records is assessed about significant metrics for determining its efficiency. The overall model performance are estimated using various estimation parameters such as the execution time, decryption time, encryption time, memory consumption and usage rates and the time required for key generation. Findings of the proposed work deliberates that higher level of security are ensured, whereby a long-term protection are used, which intends to prevents adversaries from gaining a static target for prolonged attacks. Additionally, the security level of the proposed system performs better in terms of integrity, privacy, authentication, access control, and cryptographic function.

Keywords: *Electronic Medical Documentations, Modified-Advanced Encryption Standard, Chaotic Based Random Key Generation, Modified Digests*

I. INTRODUCTION

In recent years, the medical industry has turned more digital than before. For example, the progress from X-rays and MRI (Magnetic Resonance Imaging) to ultrasound scans and CT (Computed Tomography) to EMD (Electronic Medical Documentations) explores the digital transformation in the medical sector. Processing these medical data in a secured way is a significant chore of the medicine 4.0 standard. The potentiality of these records

is also proven by the current COVID-2019 virus pandemic where distant patient monitoring has been accomplished with healthcare deliveries to combat the situation [1, 2]. From the previous era, it has been observed that the medical sector encompasses huge data introduced, circulated, saved, and also fetched repetitively. Presently, cloud storage has gained a crucial part in healthcare information. Through the storage of EMD data on the cloud server, the corresponding data could be conveniently and efficiently shared among diverse medical organizations. This cloud system affords more convenience for clinicians and patients. It also assists the patients in controlling their condition in a better manner.

Nevertheless, when the users store their data on the cloud server, particular data is vulnerable to several threats like data privacy, data integrity, and data authentication. Weak cybersecurity and data loss possess disastrous implications for which numerous individuals hesitate to agree with EMDs [3]. Traditional data sharing systems are also centralized and face issues of distinct point-of-failure [4]. On the other hand, a decentralized system possesses multiple coordinators. When few co-ordinator nodes collapse in a network, individual nodes persist to manage communication through other co-ordinators in a decentralized system. Information sharing and decentralized computation permit authorities who deny trusting one another for cooperation, collaboration, and coordination in judicious decisions making are considered a blockchain network. It is a reliable and decentralized distributed system that does not require any third-party interference. Trust relationships amongst the distributed nodes are established through cryptography algorithms and mathematical models rather than semi-trusted central institutions. Systems based on blockchain could alleviate the restrictions of distinct point-of-failure. Moreover, as the data gets recorded in a public ledger, all the blockchain network nodes possess ledger backups, it could access such data anywhere and anytime. These data also confirm the transparency of data and assist to construct trust within the distributed nodes. Thus, the main intention of blockchain has been to decentralize and avert information meddling [5].

Currently, numerous investigators have been attempting to utilize blockchain in several areas due to some of its distinct features like a deficiency in centralized control, consensus distributed upon the decentralized networks, and maximum anonymity degree [6, 7]. The field of protecting confidential details from unauthorized entrée by assuring data authentication and integrity is cryptography. The method of hashing allows confirming that transmitted messages don't get tampered [8]. Considering this, researchers have used varied blockchain and cryptography-based methods to secure data transmission of EMD. Correspondingly, the study [9] has used CP-ABE (Cipher text Policy-Attribute Based Encryption) relying on authorized blockchain for ensuring access control and data confidentiality of the healthcare data. To select an ideal encryption key, HGHO (Hybrid deer Grasshopper Hunting Optimization) has been used to attain maximum security for the transmission of medical data through the reduction of computational cost, encryption cost, and ciphertext size. Better outcomes have been attained [10]. To secure the privacy of patients, a proxy re-encryption strategy has been used during data transfer. Several chain codes have been designed and executed for dealing with the business strategy agreed upon by the network members. The suggested method has enabled the patients to seamlessly gain their archives from additional clinics. Access log has been stored immutably and transparently in the ledger which has been utilized for auditing. A web-based medical record has been developed with the integration of asymmetric cryptographies into an authorization approach for ensuring the integrity and confidentiality of medical information. The secured EMD system has afforded significant operations of general EMD and averted unauthorized individuals from

accessing essential information. However, it is significant that further researches have to be undertaken for enhancing EMD security through the incorporation of an additional security approach. In addition, a quantitative evaluation has to be achieved for assessing the performance of the considered system [11].

Similarly, the article [12] has designed a user-oriented data sharing and storage technique in MCPS (Medical Cyber-Physical Systems) based on the cloud for protecting the privacy and safety of the user's EMD data that could secure the privacy and safety when keys and cloud servers are bargained. The feasibility of the recommended system based on MEC (Medical Edge Computing) has been assessed on smartphone setup for confirming the efficiency enhancement in comparison to typical encryption algorithms. The suggested methodology could be utilized for data protection with a high level of efficiency, data integrity, and protection. Nevertheless, execution works for using hash and AES on MCPS have been required in the future.

Though conventional works have shown better performance, they possess certain limitations concerning security and privacy. Few studies have also failed to consider performance evaluation which is the significant process to confirm the efficiency of the suggested system, while, few works lacked in terms of encryption time. On contrary, the Blockchain concept is being adopted by researchers. However, only a few conventional works have used this concept for secured EMD sharing. Hence, the blockchain concept has to be considered for enhancing the cloud-supported EMD systems to functionality, security, and performance. Due to enormous EMD, there also arises a need for computationally efficient and robust cryptographic techniques to form a blockchain network. An optimal solution is required for EMD sharing to confirm the process of secure sharing of the information by averting the stalker to infer the user's identity or gain possible information about the user. To provide such a solution, the present study proposes a secure framework that is applicable for both medical experts and patients while accessing EMD from the cloud based on the below objectives,

The main contributions of this study are given below,

- To propose a security framework based on a merging algorithm for integrating the patient ID and medical records as useful information for enhancing security levels.
- To integrate cryptography and blockchain-based concepts for securing the data during access and retrieval of EMD by the proposed M-AES (Modified-Advanced Encryption Standard) and MD5 hashing algorithm for data integrity.
- To propose M-AES by using a chaotic-based random key generation for encrypting and decrypting the EMD for permitting only the authorized users to access EMD thereby making it robust for the intruder to breach the system by enhancing the confidentiality.
- To evaluate the performance of the proposed work by assessing its efficiency to execution time, memory consumption for different encrypted file sizes, key generation time, encryption time, and decryption time.
- To analyze the security level of the proposed system by comparing it with the conventional systems by undertaking a security analysis about significant functions namely blockchain-based, integrity, privacy, authentication, access control, and cryptographic function.

Motivation of the Study

The growing digitalization of healthcare information, financial transactions, and personal communications has emphasized the urgent requirement for cryptographic systems that are robust, efficient, and secure. While traditional cryptographic methods have proven effective, they frequently encounter challenges related to scalability, performance under substantial data loads, and susceptibility to new attack strategies, such as side-channel and brute-force attacks. Therefore, proposed research aims to create a chaos-based cryptosystem that utilizes the unpredictable nature and sensitivity of chaotic systems to produce high-entropy keys and bolster security. By incorporating chaotic dynamics into the encryption framework, the proposed system aspires to enhance both the security and efficiency of cryptographic processes, providing a more resilient alternative to conventional techniques.

Paper Organization

Section I discusses the recent trends in securing EMD during access and retrieval, the problems faced during access and retrieval along with the main contributions of the present study are given. Following this, section II reviews the existing works and emphasizes the main problems in this area. Subsequently, the overall proposed methodology is comprehensively presented in section III with research flow and algorithms. Results obtained from the execution of proposed methods are discussed in section IV. Lastly, the proposed system is concluded in section V with future suggestions.

II. REVIEW OF EXISTING WORK

This section discusses the cryptographic and blockchain-based approaches used by conventional studies for secured access and recovery of electronic medical records from the cloud. Further, the major drawbacks identified during the evaluation of these works are also emphasized.

2.1. Cryptographic algorithms for securing Electronic Medical Documentations

Security has become susceptible due to the enormous usage of numerous communication technologies, especially in the healthcare area. Thus, it is vital to enhance security in EMD (Electronic Medical Documentations). To achieve this, conventional works have used different cryptographic algorithms. Accordingly, the study [13] suggested a MAC (Multi-authority Access Control) framework through CP-ABE (Ciphertext Policy-Attribute Based Encryption). Performance analysis has revealed that the endorsed attribute revocation methodology has assisted in resolving backward and forward security issues. It has also minimized the time complexity. Comparative analysis has also been performed and the results explored the better performance of the considered method regarding encryption time and decryption time.

However, it lacked in terms of communication cost and key generation time. To enhance system performance, ABE has been considered along with policy hiding strategy and public traceability. The suggested technique has been designed to accomplish certain features like partial hiding of access policy, making attributes free from public parameters, efficient tracking of the user disclosing the corresponding decryption key, and requirement of minimum bilinear pairing functions during decryption. Though better outcomes have been exposed, AA (Attribute Authority) has been presumed to be a complete trusted party. Nevertheless, in reality, it might seem to be an illogical assumption [14]. Moreover, earlier protocols have only considered partial hiding of attribute values, however, they ignored the protection of attribute names. For solving this problem, the article [15]

used ABF (Attribute Bloom Filter) and modified CP-ABE that hides the attributes along with their value. The suggested method operates for all the access structures. ABF supports decrypting the data through the assessment of attributes that reside in access policies. Performance assessment and security analysis have been considered which reveal its satisfactory performance.

In addition, SKE (Symmetric Key-based Encryption) has been employed along with an attribute-based system. Protocols have been developed for data storage and data retrieval. AVISPA (Automated Validation of Internet Security Protocols and Applications) has been used to assess the security features of the considered protocol. Analysis has shown that the protocol has been simple. It has also disregarded several complexities which might evolve during deployment in real-time. Many mobile medical information strategies relying on ABE suffer from the high cost of computation. Considering this, the research [16] utilized an offline and online ABE method for developing SMHS (Secure Mobile Health System). Evaluation has explored that, the suggested method has ensured confidentiality, better decryption verification, and effective keyword search operation from EMD. Further, SMHS has employed an offline encryption stage for minimizing the computational cost, especially on the patient's side. Empirical results have explored the feasibility of SMHS [17].

Further, to enhance the turn-around time and energy consumption, the study [18] has aimed to use an incremental-proxy re-encryption method without certificates. Outcomes have revealed significant enhancement in file modification to the considered metrics. The suggested technique has been validated by the Z3 solver which has shown better results. Under the conventional healthcare cloud model, an encrypted model has been suggested that incorporates low overhead communication approaches namely MedGreen which rely on bilinear pairing and elliptic curve [19, 20]. This integrates key computation and identity verification. MedGreen could efficiently maintain the functionalities of mediating authenticating centers. It could also resist attacks like man-in-the-middle. Additionally, EHR data encryption algorithms namely MedSecrecy relying on Huffman compression and RC4 algorithm has been used. Through these suggested methods, the data repetition rate has diminished [21]. To avert various other attacks like tag cloning and replay attacks thereby solving the authentication issue in NFC (Near Field Communication), the study [22] has endorsed TEA (Tiny Encryption Algorithm). The suggested method has been improvised with a yarrow-pseudo generator to restrict the considered attacks. Analysis has stated that the yarrow approach has the capability of defending against cryptanalytic attacks. However, it lacks suitable strength for generating entropy. Similarly, the article [23] has recommended AES for securing EMD in NFC. Better results have been attained. A suggestion has also been provided stating that when patients permit any other parties to access their medical records, then, confidentiality seems to be uncertain in this case.

Further, a web system has been deployed to validate the model. MD5 (Message Digest5) and SHA1 (Secure Hash Algorithm) have been utilized for encrypting the data during the transfer of information to confirm data integrity and confidentiality. Outcomes attained from the patients and clinical administrators have confirmed the user-friendliness of the suggested model [24]. A key agreement has also been considered along with the suggested fair exchange approach. It concentrates on protecting against data breaches of EMD. Evaluation results have explored that, the endorsed methodology acts as an effective contactless data transmission technique that permits healthcare data aggregation thereby preventing the anonymity of patients, particularly, in the COVID-19 context [25]. Similarly, IFHDS (Intelligent Framework for Healthcare Data Security) has been recommended for securing data in EMD through encryption methods in distributed way amongst varied cloud platforms. The initial stage is

specifically assisted by DSL (Data Sensitivity Level) which states that the sensitivity stage for individual attributes and partitions sensitive information from non-sensitive information. Subsequently, SLE (Sensitivity Level Encryption) has been developed for using cryptographic algorithms within the sensitivity level. Further, D3S (Duplication and Distribution Data Security) approach has been stated for replicating and distributing encrypted data to several cloud providers [26].

On the other hand, decryption has been performed by DSD (Decrypt Sensitivity Data). The main challenge resolved by IFHDA has been to secure the medical data from the direct reach of the cloud providers. The main drawback of the suggested strategy is that the present version has stated the data sensitivity level through a configuration file which is maintained by a data owner [27]. For assuring secured data access, HLE-SO (Hybrid Lightweight Encryption using Swarm Optimization) has been used which performs medical data encryption and transmits it from one end to the other end. Simulation has been undertaken and a comparison has been performed with the conventional DLCE technique. Results have explored that, processing time and error have been minimized [28]. To afford reliable security with better speed, a lightweight crypto-hash function has been used to generate SKE (Symmetric Key Encryption) and OTP (One Time Password). A security tool named scyther has also been used for authenticating the patients. Analytical outcomes have concluded that most of the OTP-based key management and authentication resolves the issues related to password schemes and dynamic ID, particularly in the medical sector. It has been safe to utilize features like key management, authentication, etc [29, 30].

2.2. Blockchain-based strategy for secure retrieval of data from EMD

Blockchain is an evolving technology for solving security problems of EMD in the decentralized form on the cloud. Thus, to solve the security issues during the data retrieval from EMD, the blockchain concept has been considered by a few conventional works. Accordingly, the study [31] suggested an attribute-based crypto approach based on blockchain for accomplishing authentication, data integrity, and confidentiality while sharing EMD. For accomplishing varied operations of ABE, IBS (Identity Based Signature), and IBE (Identity Based Encryption) in a cryptosystem, a cryptographic primitive termed C-AB/IB-ES (Combined-Attribute Based/Identity Based-Encryption and Signature) has been used. Outcomes have revealed that the endorsed system averts the need for suggesting cryptographic approaches for diverse security needs. Similarly, a lightweight authentication approach namely CMBC (Cloud-based Medical Blockchain) has been suggested. Security associated with the EHR transactions of patients is verified through PoS (Proof of Stake) and PoW (Proof of Work) methods. Performance analysis has revealed that the suggested technique has accomplished minimum computational time [32]. To protect significant EHRs against peripheral attacks, BSF (Blockchain Security Framework) has been recommended. The patient has also been capable of independently managing and sharing their EHRs through the suggested approach. Empirical outcomes have also exposed that, BSF-EHR has shown better sharing of data amongst users [33]. As different studies have used different blockchain-based strategies, the research [34] has used hyper-ledger fabric-oriented certificate authority for executing smart contracts. Data has been assessed through Origin lab Pro and PHYCHARM. Comparison has been undertaken with conventional frameworks. Analytical results have explored the better performance of the suggested system concerning security and throughput.

In addition to the execution of blockchain for EHR, granular access rubrics have been considered for securing EMB storage. Moreover, role-based access has also been regarded as a benefit of the suggested system as healthcare records have been only accessible to related and trusted individuals. The suggested method also resolves the information asymmetry issue in the EHR system [35]. To assure the privacy of sub-contracted EHR from any illegal alterations without the introduction of any trusted party, a cloud-supported e-health system has been used. It applies a key agreement approach based on passwords for establishing secure channels amongst the clinicians and patients. Comparative assessment has stated the better performance of the suggested system which could repel password-guessing attacks [36, 37]. To enhance the conventional delegated PoS (Proof of Stake), a lightweight healthcare data sharing model has been suggested that relies on blockchain. A symptom matching approach has been designed for the patients registering in diverse clinics who possess similar disease symptoms. A single session key might be set amongst the patients succeeding in the completion of mutual authentication. It has been concluded from the evaluation that, the suggested scheme could assist patients in communicating information about the disease [38].

Furthermore, Proof of Concept has been used along with chameleon hashing for reducing the fragmentation of data thereby minimizing resource consumption for secured data retrieval from EHR. Outcomes have revealed that the suggested ASIN (AES encrypted data, Static encryption key, Incremental storage, No server-side encryption) has been the fastest with the least bandwidth while, PDIY (PRE encrypted data, Dynamic keys, Incremental storage, Server side encryption) has explored better outcomes [39]. Analytical evaluation of blockchain in medical data management has been studied. From the analysis, it has been found that blockchain has shown a positive impact in healthcare while using a consensus scheme and standard AES for encrypting and decrypting data [40].

2.3. Problem Identification

The main issues identified during the review of the above conventional studies are listed,

- Secured medical data storage and data sharing based on the blockchain concept have to be accomplished [30]. The use of the blockchain concept for improving the cloud-supported electronic medical systems about performance, security, and functionality has to be considered [36].
- Though better outcomes have been attained, effective privacy and security solutions seem to be lagging [41].
- The solution has to be added for medical data sharing to assure that process involved in information sharing averts the intruder to deduce the user identity or attain probable user information [21].
- Encryption time is 137.2ms which has to be further reduced to enhance the system performance [28].
- Due to huge EHR, there exists a demand for a robust and computationally effective cryptographic algorithm for forming a blockchain framework [6].

III. PROPOSED METHODOLOGY

The research focuses to accomplish secured data transfer and retrieval of EMD in the cloud through the integration of cryptography and blockchain concepts. Though existing studies have attempted to perform this, they have been deficient in privacy, security, performance evaluation, and encryption time. These studies have

also disregarded the use of computationally effective cryptography algorithms to form a blockchain model which negatively impacted the security of EMD data sharing. To rectify these drawbacks, the present study proposes a hybrid security pattern model which involves certain processes as shown in figure.1. Besides in the proposed system, various key lengths were tested to assess the performance and security capabilities of the encryption methods. Specifically, the key lengths used for testing ranged from 100 bits to 4096 bits, ensuring a comprehensive analysis of the system's performance across different security levels. This range was chosen to demonstrate the proposed system's adaptability and efficiency with varying levels of encryption strength.

- 100 bits: Used to evaluate the system's performance with smaller, less secure keys, providing a baseline for comparison.
- 128 bits: A commonly used length in modern encryption standards, balancing security and performance.
- 256 bits: Known for providing strong security, this key length is often used in high-security applications.
- 512 bits to 4096 bits: Higher key lengths were tested to analyze the proposed system's performance under extreme security demands, including future-proofing against potential advancements in computational power.

These key lengths enabled a detailed comparison of encryption time, decryption time, and key generation time against conventional methods, highlighting the proposed system's efficiency and robustness. Then the process involved in figure 1 is depicted as follows. Initially, the IoT (Internet of Things) medical sensor data is acquired from the dataset. From the dataset, the medical records and patient ID is gathered based on a merging algorithm. After this, the encryption process is considered for encrypting the text. To perform this process, the proposed M-AES (Modified-Advanced Encryption Standard) is regarded. In this case, a chaotic based random key is generated based on which AES algorithm is used to encrypt the text. Simultaneously, MD5 hashing is considered for generating the hash. In the projected approach, making use of Modified-Advanced Encryption Standard algorithm, is based on the chaos random key generation. Using the projected chaotic system, which is used in transforming the static cryptographic keys to a dynamic and random forms of counterparts. This results in avoiding the need of maintenance, and tends to transfer any of the open channels. Whereas, in the chaos-based model, the random and dynamic states of synchronized chaos, are used as secret keys. These are used in enhancing the synchronized forms in aspects of generating a random key of 256 bits, for Modified-Advanced Encryption Standard algorithm in view of improving the security. The chaotic system is integrated into the proposed cryptosystem to enhance security by leveraging the inherent properties of chaotic maps, such as sensitivity to initial conditions, unpredictability, and aperiodicity. Moreover, chaos-based cryptosystem characteristics make chaotic systems ideal for generating complex, high-entropy keys that are extremely difficult to predict or reproduce, thus enhancing the robustness of the encryption process. Unlike traditional cryptographic techniques, which can be vulnerable to patterns and statistical attacks, chaotic systems ensure that the cryptographic keys are highly random and dynamic. This unpredictability not only strengthens the encryption but also mitigates the risk of unauthorized access, making the cryptosystem resilient against various types of cryptographic attacks. The approach has also made use of Modified Digest5 algorithm, for encrypted text and hashing them into data blocks.

Subsequently, the encrypted text and hash are fed into the block of data to form a blockchain. In this data block, the ledgers of user hashing are reliable as it relies on the blockchain concept that comprises the recordings of all the transaction details. The encrypted text can be decrypted using M-AES by splitting the features from the merged

(medical records and patient ID). The patients can view their medical records through the entry of their patient ID and medical records. The proposed model checks if the input data matches the data stored in the cloud. If the data matches, the records are displayed, or else, it determines that the user is unauthorized and maintains the data security.

The Security analysis upon the projected approach are analysed using various security functions such as privacy, access control, integrity, authentication, cryptographic function, and blockchain-based systems.

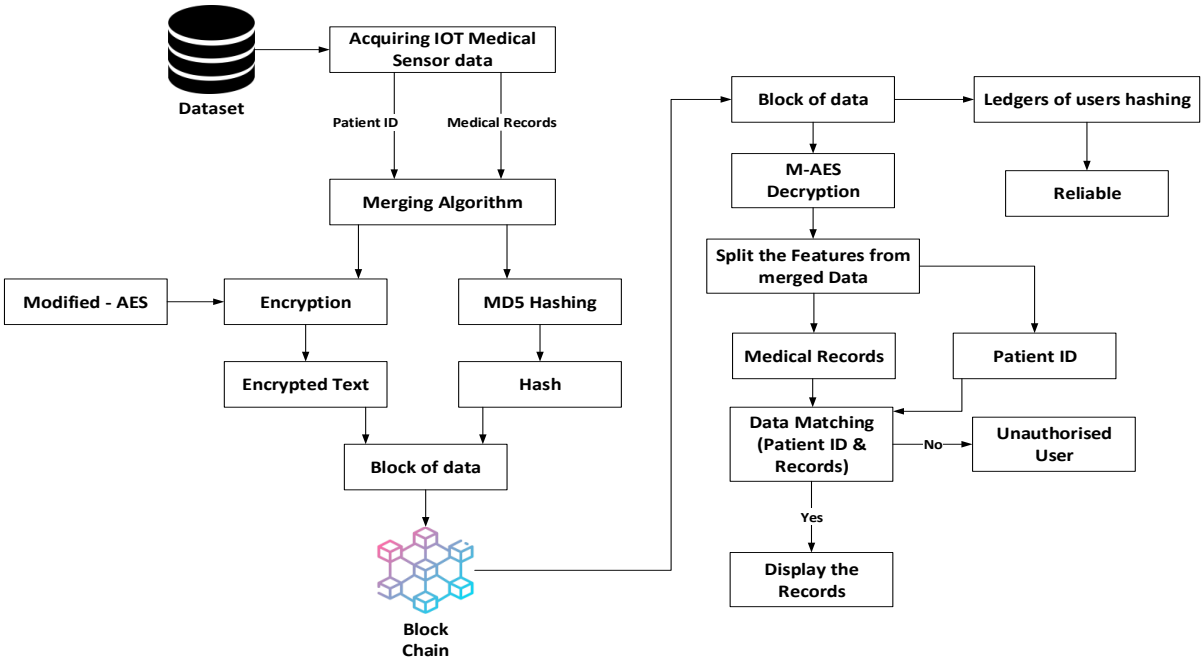

Figure 1 Overall view of the research flow

3.1. Blockchain-based model for securing EMD during access and retrieval

The proposed model is applicable in the real world where the EMD vendors can execute the blockchain patron within their EMD software which interacts with the medical information automatically and directly to blockchain-based PHR (Personal Health Record) as shown in figure.2.

Figure 2 appears to represent a process of validation between an Electronic Health Record (EHR) system, which is integrated with blockchain technology, and a patient.

EHR System with Blockchain Client Node: A healthcare provider engages with an Electronic Health Record (EHR) system, which is integrated with a Blockchain Client Node. This integration signifies that the EHR system utilizes blockchain technology for the management and verification of health records. The Blockchain Client Node is responsible for securely recording patient data, ensuring its immutability, which means that once data is entered, it cannot be altered.

Validation with Record and Patient ID: In the central section, a box labeled "Validation with Record and Patient ID" indicates that the validation process is focused on matching the patient's identification number with their corresponding health records stored on the blockchain. This validation process is essential for ensuring that the health record is accurate, authentic, and appropriately assigned to the patient. By leveraging blockchain

verification mechanisms, the system likely assesses the integrity and authenticity of the health records, thereby reinforcing the reliability of patient data management. This approach not only enhances data accuracy but also fosters trust in the healthcare system by ensuring that patient information is securely linked to verified identities.

Patient: On the right side, an image representing a patient illustrates the linkage and verification of the patient's records through blockchain technology. This process signifies that the patient's health records have undergone validation via the blockchain, ensuring their accuracy and authenticity. By utilizing the decentralized and immutable nature of blockchain, the system guarantees that patient data remains secure and tamper-proof. This integration not only enhances the integrity of health records but also fosters trust among patients and healthcare providers, as it ensures that sensitive information is reliably linked to verified identities.

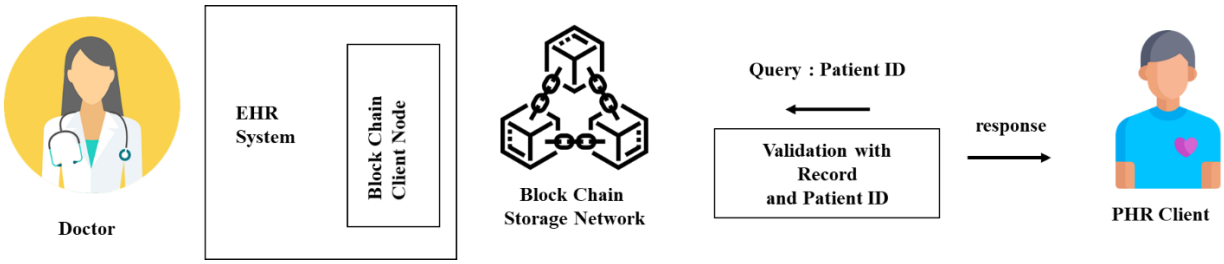

Figure 2 Architecture for EMD based on blockchain

After accomplishing any data access or retrieval, the EMD saves the respective data locally, then, it prepares the encounter data in the C-CDA version and transmits it to the blockchain patron which encrypts the corresponding document through the public key of the patients. It is then connected to the blockchain for transmitting the document. Now, the C-CDA version document with metadata regarding the subject and source of the subject is car-accomplished as an operation to the blockchain. Following this process, the blockchain nodes utilize a consensus mechanism for determining the validity of a transaction. If the nodes accept any alteration, then, it gets permanently stored in the public ledger. In this way, all the documents of all the patients are stored in the blockchain ledger. PHR Client is then able to connect with blockchain to download the documents corresponding to respective patients. The private key of the patients is used for decrypting the documents. Validation is undertaken with records and patient ID, if this validation is authorized, the patients attain the ability to see the decrypted documents as well as share those documents.

Thus, to secure EMD against any modifications during transmission, hashing concept is used in blockchain where the unreadable string is generated with a fixed size. Generally, hashing functions are utilized in blockchain for encrypting information within the block of data. In this study, MD5 hashing is used as it possesses an innate ability of less collision ratio. For securing the proposed hybrid pattern which is generated as a binary string of one dimension, two copies corresponding to the pattern are generated. Following this, cryptography is executed using the M-AES algorithm on a copy of the pattern for transferring data to corresponding nodes. As depicted in figure.3, the hash function is executed using MD5 on another copy corresponding to the hybrid pattern.

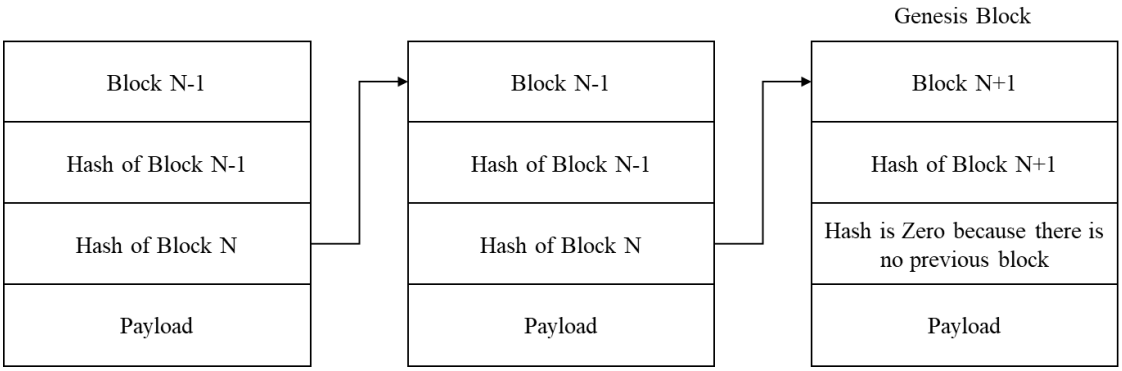

Figure 3 Blockchain hash generation (data transfer)

Through the hashing process, an arbitrary amount could be attained from input, and output of fixed size is generated called a hash. In this case, the input could be a random number (in bits) that indicate characters of different size, while, the output has a fixed size based on the chosen hash function. The hashes corresponding to individual patients get stored in respective ledgers individually. The security of the chaotic-based key generation process are unpredictable keys. If the chaotic system used in the projected approach are well-designed, tends exhibits properties such as sensitivity to all of the initial conditions and non-linearity, which in turn enhances the chances of overall strength of the encryption. Followed by, the performance metrics, are used in analysing the effectiveness.

Typically, the process of data acquisition and encryption begins with the system acquiring medical data from IoT sensors or other sources, which includes essential information such as patient IDs and medical records. This data is then merged using a specified algorithm and subsequently encrypted using the Modified-AES (Advanced Encryption Standard) to ensure confidentiality. Following the encryption, the encrypted text, which represents a block of data, is processed through the MD5 algorithm to generate a hash value. This hash serves as a fixed-length string that uniquely represents the encrypted data. The generated hash value is stored in the blockchain as part of the data ledger, where each block of data is indexed using this hash, thereby maintaining the integrity of the data. The blockchain's structure inherently ensures that any alteration of the data would result in a different hash, immediately indicating potential tampering. When a user requests access to specific medical records, the system retrieves the corresponding block of data from the blockchain using its hash value. This hash is then utilized to verify the integrity of the data before it is decrypted and presented to the user, ensuring both security and reliability in accessing sensitive medical information.

3.2. Merging Algorithm

- A merging algorithm is introduced for securing the hybrid pattern thereby averting intruders from breaching EMD. This algorithm utilizes a binary string of the medical records and patient ID. The algorithm works correctly when altering the medical records in the future. To merge, medical records and patient ID, three phases are utilized. The initial phase includes binary pattern labelling. In the next phase, a few manipulations are performed on this binary data based on information from medical records. After this process, a chaotic function is executed on data as per equation.1 and equation.2, where CD indicates the Chaos Degree.

- In conventional static keys, the CRK tends to dynamically transform from the initial random state, which is done by eliminating the need of regular maintenance or transfer upon open channels. But the current, projected model tends to add an additional layer of unpredictability, which results in enhancing the system's resistance to an unauthorized form of access.
- Adopting the MD5 hashing algorithm, are used in producing the fixed-size hash value from input data. Using M-AES (Modified Advanced Encryption Standard), algorithm encrypting the text and hash, later involves in organizing them into data blocks for secured range of transmission and storage of the data.

$$ptn_{n+1} = ptn_n + CD \sin(\theta_n) \quad (1)$$

$$\theta_{n+1} = \theta_n + ptn_{n+1} \quad (2)$$

Pseudo-code-I represents the introduced merging technique where the hybrid binary pattern is taken as input to obtain the chaotic hybrid pattern as output.

Pseudo-code-I: Merging Technique
Input： Hybrid Binary Pattern
Output： Chaotic Hybrid Pattern
Start
for i = 0 to length (hybridBinaryPattern)
ptn(i + 1) = ptn(i) + CD ∗ sin(i)
i + 1 = i + ptn(i + 1)
end for
chaoticIndices = int()
chaoticIndices = chaoticIndices % length(hybridBinaryPattern)
chaoticHybridBinaryPattern = hybridBinaryPattern
for i = 0 to length(hybridBinaryPattern)
idx1 = i
idx2 = chaoticIndices(i)
swap(chaoticHybridBinaryPattern(idx1),
chaoticHybridBinaryPattern(idx2))
end for
End

3.3. M-AES (Modified-Advanced Encryption Standard)

Generally, AES is a renowned symmetric key encryption approach. Main AES architecture is represented in figure.4. For the generation of uniform cipher text distribution, linked operation sequences are encompassed in the AES cryptosystem. Few of the associated functions are undertaken by substituting inputs through the use of certain output feedback. The AES runs all computations through the use of bytes. AES (Advanced Encryption Standard) are one of the widely used symmetric encryption algorithm. These are used in securing the sensitive data by performing the action of transforming the data to an unreadable format, by making use of secret key. The static key finds showing the applicability and are maintained in a safer manner. In the projected Modified AES a

chaotic system's, synchronization technology are adapted as the static key turns both the random and dynamic modes, which avoids the need of maintenance or transfer among any of the open channels. Moreover, MD5 (Modified Digest5) hashing algorithm are used for feeding the encrypted text and hash into data blocks. This finally enhances the rates of security, which are used by dynamically altering keys and employing them to robust encryption methods.

Hence, AES detached information block of 128 bits into sixteen bytes which are then converted into matrix format with four rows and columns for operation processing. In AES cryptosystem, operation rounds rely on the chosen key length. Different key lengths are used with varied round keys retrieved from the actual static-AES key.

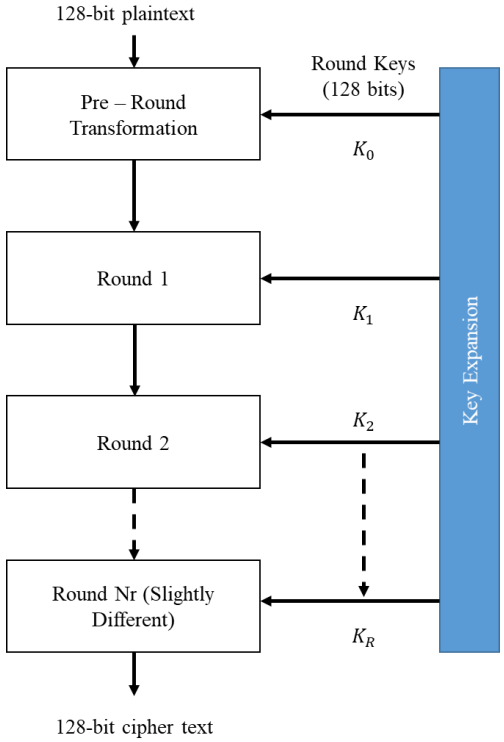

Figure 4 Process of Conventional Advanced Encryption Standard

Typically, for an AES symmetric cryptosystem, keys indicate shared secret keys in communication systems which would assure secured transfer of information. Nevertheless, in comparison to an asymmetric key system, the main drawback of a symmetric-key cryptosystem is the secret key requirement. If this fixed secret key gets stolen, the information becomes vulnerable to exposure. Hence, to resolve this issue, in this study, M-AES based on chaotic random keys is proposed as shown in figure.5.

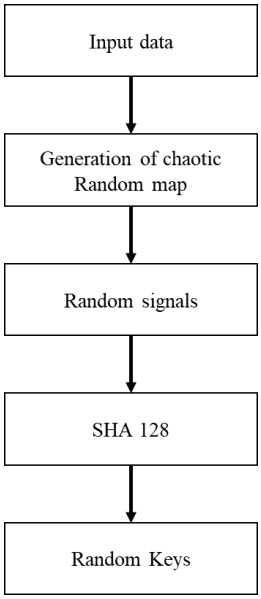

Figure 5 M-AES with Chaotic Random Key Generation

The random keys are generated for the input data based on the production of a chaotic random map. Generation of Chaotic Random Map refers to the process where input data is used to create a sequence of chaotic values. This process utilizes a mathematical model known as a chaotic map, which generates random-like outputs that are highly sensitive to initial conditions. The generated chaotic signals are used as a foundation for random key generation in encryption, enhancing security by introducing unpredictability. This approach effectively prevents unauthorized access, as the random keys produced are difficult to replicate due to the chaotic nature of the generation process. In proposed work, a combination of logistic maps and other nonlinear systems are used to create the chaotic signals, which are then processed further to produce high-entropy random keys. The process is comprehensively presented in figure.6. In the proposed chaos-based M-AES, random dynamic states of the synchronized chaos are utilized as secret keys. This enhanced design could afford random states in the synchronized form to generate a random key of 256 bits for M-AES to improvise its security.

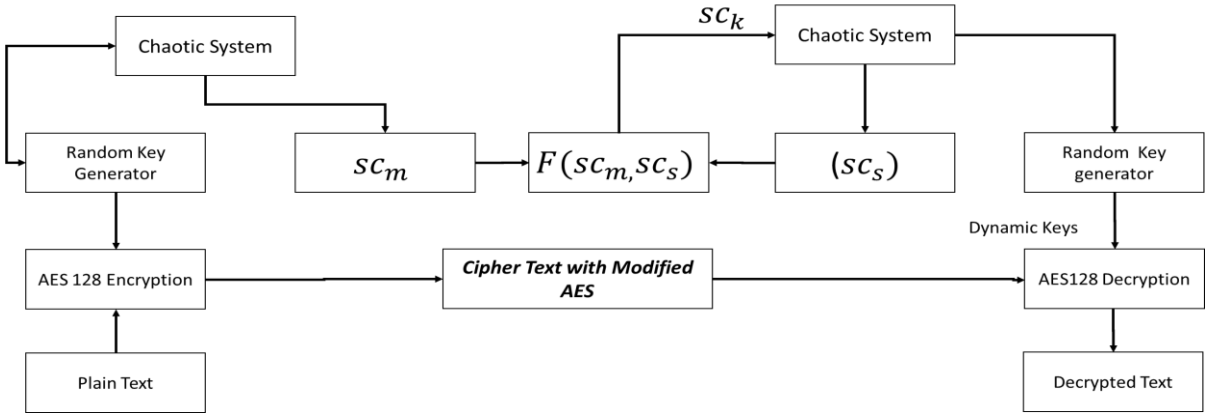

Figure 6 Process of Modified-Advanced Encryption Standard

Through the introduction of the designed controller for slave chaotic architecture, slave states might be synchronized along with master states. Moreover, for improvising practical application security, a synchronization

controller (sc(k)) is decomposed as $sc_m(k)$ and $sc_s(k)$ that is computed from slave and master chaotic architecture. Then, the controller is comprehended at the receiver end with $sc(k) = F(sc_m(k), sc_s(k))$. Even when hackers possess these synchronization controller parameters, they would not be capable of attaining the master states and slave states individually. They would also be incapable of restructuring the synchronization controller. Thus, the security of an encrypted system with dynamic keys would be assured. After accomplishing synchronization, similar chaos signals might be obtained concurrently. After this, synchronized random key construction is accomplished at the transmitter side and receiver side. Fixed keys of conventional AES are substituted by random signals that are synchronized and do not require to be fed in advance or communicated over public channels. Consequently, key storage issues could be averted and encryption security could be enhanced due to the synchronized random keys. Likewise, timing diagram for proposed model is depicted in figure 7.

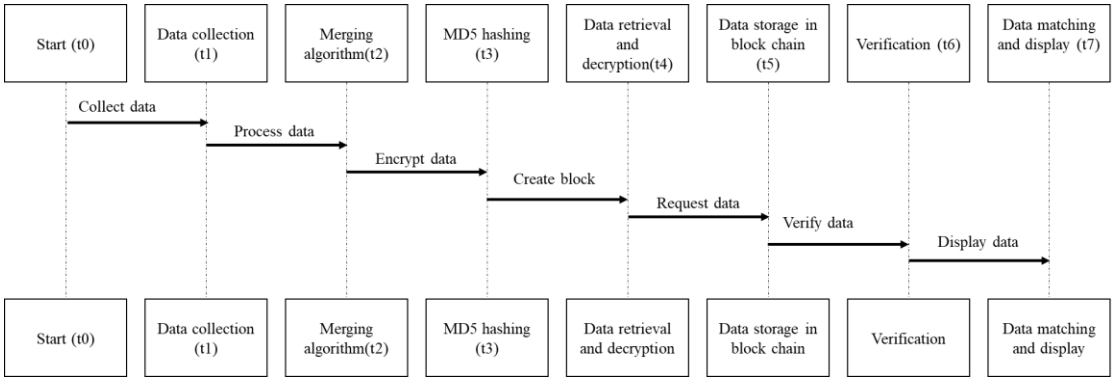

Figure 7 Timing diagram of proposed model

Steps involved in timing diagram is demonstrated as follows. Here, the process of acquiring and managing IoT medical sensor data involves a series of steps that occur within defined time intervals. During the initial phase (t0 - t1), data from IoT medical sensors is collected and transmitted to a merging algorithm. In the next stage (t1 - t2), the merging algorithm processes the incoming data, which includes Patient ID and Medical Records, preparing it for encryption. A Modified-AES algorithm is then applied to encrypt the data.

Following encryption, the data undergoes MD5 hashing (t2 - t3) to create a unique representation of the encrypted information. In the subsequent step (t3 - t4), a block of data is created that contains both the encrypted text and its corresponding hash. This block is then stored in a blockchain for secure and immutable record-keeping.

When a data request is made (t4 - t5), the system retrieves the relevant block from the blockchain. It then decrypts the data using the Modified-AES algorithm and prepares it for verification. The decrypted data undergoes verification (t5 - t6) by comparing its hash with the stored hash to ensure integrity and authenticity. If verification is successful, the system matches the Patient ID with corresponding records (t6 - t7) and displays the relevant medical data for review. This structured approach ensures secure handling of sensitive medical information while facilitating timely access to patient data.

IV. RESULTS AND DISCUSSION

Dataset used in this study is described in this section along with the results corresponding to performance analysis and comparative analysis. In addition, the security analysis is undertaken to analyse the efficiency of the proposed system than conventional systems about significant security functions.

4.1. Dataset description

The present study has considered a sample heart disease dataset for accomplishing a secured framework for data access and retrieval of this EMD through the proposed system. The considered data is a multi-type dataset that encompasses several statistical or mathematical variables. It comprises of 14-attributes of heart disease and this study has taken it as a sample from,

https://www.kaggle.com/datasets/redwankarimsony/heart-disease-data

4.2 Laboratory Conducts

The testing environment for proposed research is structured to optimize performance through both hardware and software configurations as well via tools and technologies and testing protocols.

In the hardware environment, high-performance computing systems that are equipped with multi-core processors and substantial memory capacity are utilized. This setup is essential for efficiently managing extensive computational tasks, enabling parallel processing that significantly enhances processing speed and overall system performance.

In terms of the software environment, proposed work primarily operates on various versions of Windows 11 to ensure compatibility with a wide range of software tools and advanced testing frameworks like Python along with libraries such as NumPy, SciPy, and TensorFlow for data processing and machine learning applications are utilized. Additionally, a custom-built software solutions tailored to meet specific testing requirements is developed, ensuring that proposed approach is both flexible and effective in addressing the diverse needs of proposed research projects.

For tools and technology factor, a diverse array of tools and technologies are used to enhance data analysis and simulation capabilities. For data analysis, visualization tools such as Python's Matplotlib and Excel is employed, which permits to interpret test results and present findings effectively. These tools facilitate the graphical representation of data, making it easier to identify trends and insights. Additionally, simulation software is leveraged to model and analyze complex systems and processes, including cryptographic simulations, encryption testing, and performance evaluations. This software is crucial for understanding the behavior of various algorithms under different conditions. Besides, to ensure efficient collaboration and version management, tools like Git and GitHub is used. These platforms enabled to track changes to code and documentation meticulously, fostering a collaborative environment in order to contribute effectively while maintaining the integrity of the project's development.

To maintain the integrity and reliability of proposed research outcomes, established standardized procedures for testing protocols, ensuring consistency and reproducibility of results is used. This involves comprehensive documentation of testing procedures, meticulous calibration of equipment, and thorough validation of results to uphold the highest standards of accuracy. Additionally, quality assurance measures is implemented which rigorously monitor and verify the accuracy of the testing processes. This includes regular maintenance of equipment and systematic validation checks to identify any discrepancies or issues promptly. By adhering to these stringent protocols, findings of the study ensured in both reliable and valid outcome, thereby contributing to the overall credibility of proposed framework.

4.3 Comparative Analysis

The proposed system has been comparatively assessed with conventional works concerning significant performance metrics and the obtained outcomes are presented in this section. Initially, the proposed work has been compared with the traditional study [42] that includes enhanced AES encryption and standard AES encryption in terms of execution time. Obtained outcomes are shown in table-1 with its graphical representation in figure.8.

Table-1 Comparative Analysis concerning execution time [42]

Size of Input (in blocks)	**1**	**5**	**10**	**20**	**30**	**40**	**50**
Execution time of existing enhanced AES encryption	1500	2300	6400	9000	16500	21000	28500
Execution time of AES encryption	1600	2400	6600	9500	17000	22250	32600
Proposed	**1420**	**2235**	**2360**	**8500**	**15400**	**20145**	**27580**

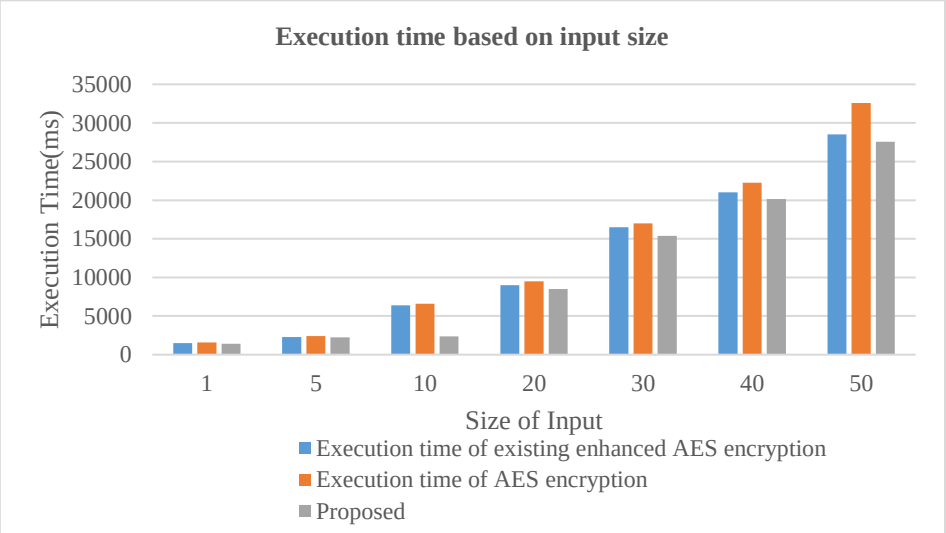

Figure 8 Analysis concerning execution time for varied input sizes [42] (in blocks, one block=128 bit)

From the evaluation outcomes, it is found that the existing enhanced AES has taken 1500ms for encrypting one block, while, AES has taken 1600ms for encrypting one block. On the other hand, the proposed method has taken 1420ms to encrypt a block. The execution time increased with the block size (in the order 5, 10, 20, 30, 40, and 50). When 50 blocks are considered, the execution time of enhanced AES has shown 28500ms, AES has explored 32600ms, while, the proposed system has shown 27580ms. Thus, it is clear that the proposed system has taken less time for encrypting the input in comparison to the conventional system. In addition, the proposed system is assessed concerning execution time for the varied size of cipher text. For this analysis, different conventional methods are considered which include TEA (Tiny Encryption Algorithm), AES, and FlexenTech (Flexible Lightweight encryption). Obtained outcomes are shown in table-2 with its graphical representation in figure.9.

Table-2 Performance analysis of execution time [43]

Methods	**Encryption time for different cipher text size**				
	128	**256**	**512**	**1024**	**2048**
FlexenTech	3	5.5	5.5	8.7	14.6
TEA	4	5.4	8.6	15	22.98
AES	5.3	9.3	15	23.6	30
Proposed	**2.8**	**4**	**4.1**	**6.7**	**13.5**

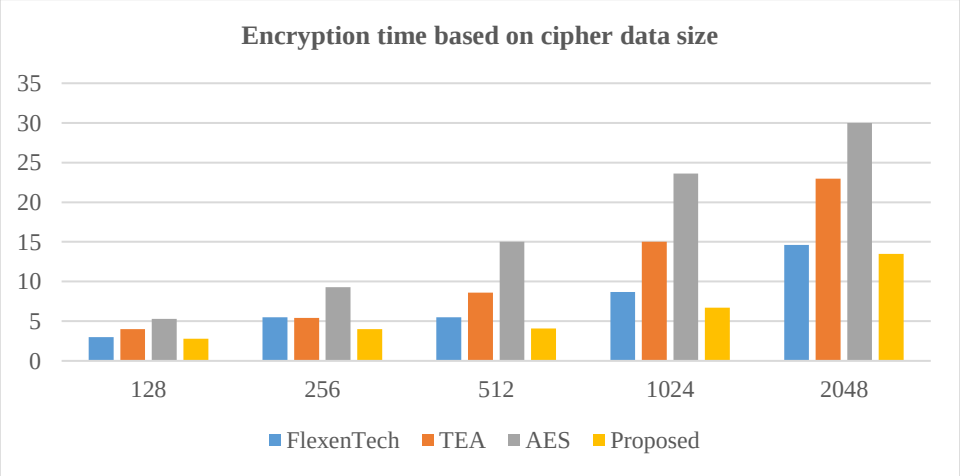

Figure 9 Analysis of encryption time for varied cipher data size (in byte) [43]

From the analysis, it is found that TEA has taken 4ms for encrypting 128-byte data, FlexenTech has taken 3ms for encrypting 128-byte data, and AES has taken 5.3ms. On contrary, the proposed technique has taken 2.8ms for 128-byte data. The proposed system has taken less time for encryption than conventional works for different data sizes which are presented in the above representations. Analysis has also been undertaken about memory consumption. To perform this analysis, existing methodologies namely Elgamal, ECC-CRT (Elliptical Curve Cryptographic Encryption-Chinese Remainder Theorem), and RSA (Rivest Shamir Adleman) have been considered. Obtained outcomes are presented in table-3 with its graphical representation in figure.10.

Table-3 Comparative Analysis of memory consumption [44]

Algorithm	**Memory Consumption for the different varied sizes of encrypted file**		
	5000 kb	**10000 kb**	**15000 kb**
Proposed	12548	15423	25186
ECC-CRT	19855	36458	56981
ElGamal	37587	69458	124589
RSA	52896	120000	155683

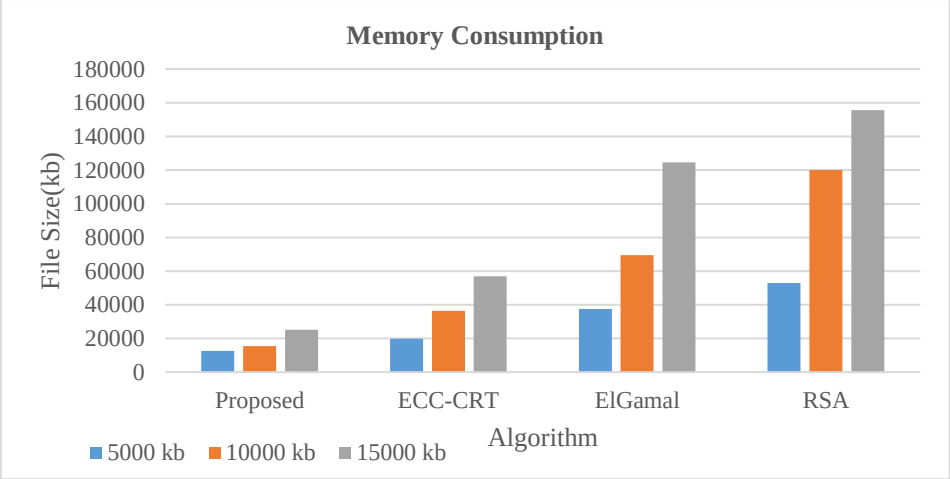

Figure 10 Analysis of memory consumption for varied file sizes [44]

From the analysis, it is found that existing ECC-CRT has consumed 19855, Elgamal has consumed 37587 memory, while, RSA has consumed 52896 memory. However, the proposed system has consumed 12548 memory. As the file size increased, the memory consumption also increased. However, in comparison to existing methods, the proposed method has consumed less memory which is seen in the above analytical outcomes. Further, analysis has been undertaken about key generation time, encryption time, and decryption time. Different conventional methods have been considered for this analysis which includes MRSAC (Modified RSA Cryptosystem), MRSA (Modified RSA), RSA, and ECDHC (Elliptic Curve Diffie Hellman Cryptosystem). The results about key generation time are shown in table-4 with its graphical representation in figure.11.

Table-4 Analysis of key generation time [45]

Key length (in a bit)	ECDHC	RSA	MRSA	MRSAC	Proposed
100	78	72	110	158	72
128	79	92	144	244	75
256	94	469	484	584	90
512	110	140	172	192	100
1024	391	469	625	1625	382
2048	781	2453	8125	8925	775
4096	7637	91,542	93,899	1,23,899	7,621

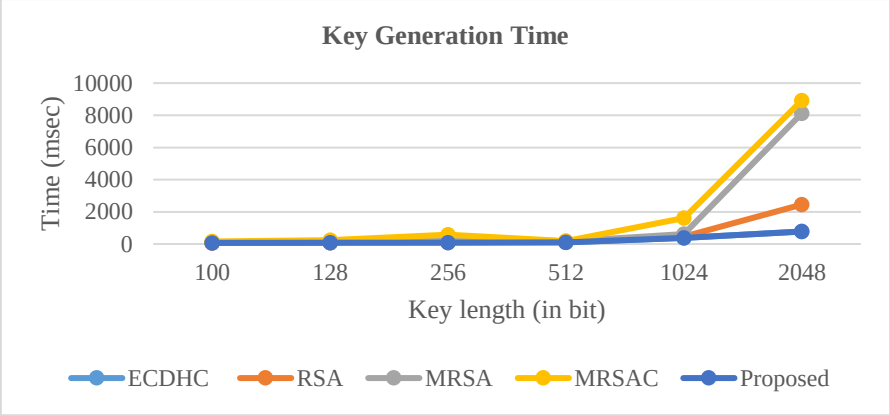

Figure 11 Comparative Analysis of key generation time for varied key length [45]

From the analysis, it is found that ECDHC has taken 78ms for generating a key when the key length is 100bits, RSA has taken 72ms to generate a key for the same 100 bits, while, MRSA has taken 110ms and MRSAC has taken 158ms. However, the proposed system has taken a minimum time of 72ms. Though this rate is equivalent to RSA, the key generation time of RSA increased with an increase in key length. However, the proposed method has shown steady progress with less time taken for key generation for different key lengths which are confirmed through the results. Further, the results about encryption time are shown in table-5 with its graphical indication in figure.12.

Table-5 Analysis of encryption time [45]

Key length (in a bit)	ECDHC	MRSA	MRSAC	Proposed
100	10	222	188	9
128	12	205	305	11
256	15	329	409	13
512	19	1672	2762	15
1024	30	11,625	13,625	25
2048	50	99,891	10,880	45
4096	92	1,10,907	21,887	85

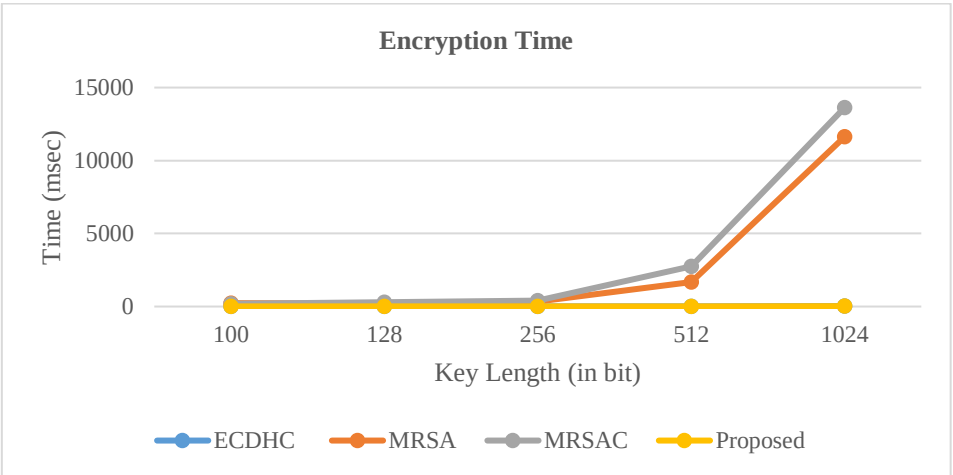

Figure 12 Comparative Analysis of encryption time for varied key length [45]

From the analysis, it is seen that ECDHC has taken 10ms for encrypting 100bits, while, MRSA has taken 222ms and MRSAC has taken 188ms. On contrary, the proposed system has taken 9ms for encrypting 100 bits. Though existing ECDHC has shown better performance, the proposed work is found to be outstanding. The encryption time increased with an increase in key length. However, the present work has explored better outcomes than conventional methods. Similarly, analysis has been performed about decryption time and the attained results are shown in table-6 with its graphical indication in figure.13.

Table-6. Analysis of decryption time [45]

Key length (in a bit)	ECDHC	RSA	MRSA	MRSAC	Proposed
100	16	88	107	212	14
128	31	188	122	188	26
256	47	62	156	203	40
512	63	218	968	688	56
1024	78	1453	6938	7038	70
2048	109	15,203	53,609	83,709	98
4096	187	18,381	10,957	10,957	175

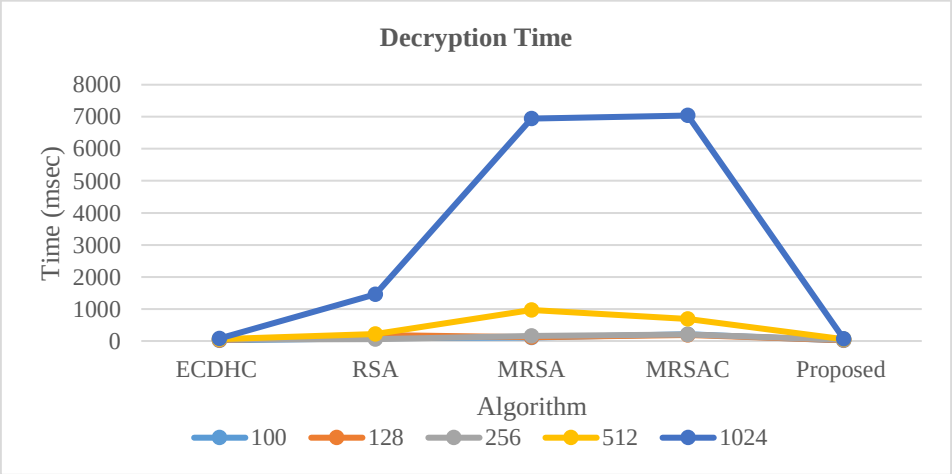

Figure 13 Comparative Analysis of decryption time for varied key lengths [45]

From the analysis, it is found that ECDHC has taken 16ms for decrypting 100bits, while, MRSA has taken 107ms, RSA has taken 88ms and MRSAC has taken 212ms. On contrary, the proposed system has taken 14ms for decrypting 100 bits. Though existing ECDHC has shown better performance, the proposed work is found to be outstanding. The decryption time increased with an increase in key length. However, the present work has explored better outcomes than conventional methods. Thus, from the overall comparative analysis, the proposed system has shown better outcomes in comparison to conventional methods regarding execution time, memory consumption for different encrypted file sizes, key generation time, encryption time, and decryption time. Besides, proposed system demonstrates significant improvements in execution time compared to conventional

encryption methods. Specifically, the proposed system shows a reduced execution time by approximately 5-10% compared to enhanced AES encryption and up to 20% compared to standard AES encryption, especially when dealing with larger input sizes. For instance, when encrypting 50 blocks of data, the proposed system took 27,580 ms, whereas enhanced AES and standard AES required 28,500 ms and 32,600 ms, respectively. These results highlight the efficiency of the proposed system in handling various encryption tasks more swiftly than existing methods, making it a superior choice for real-time and high-performance applications. In addition to these analysis, various analysis like resistance to attacks such as Potential privacy leakage, Aggregation attack, Collusion attack are assessed for emphasizing the performance of the model.

Potential Privacy Leakage

Potential privacy leakage is a critical concern in the handling of medical data, occurring when unauthorized parties gain access to sensitive information due to vulnerabilities in the system. The proposed system employs modified AES encryption and blockchain technology to store encrypted data blocks, providing a high level of security. However, if encryption keys are not managed properly or if there is a flaw in the encryption algorithm, attackers could potentially decrypt the data, exposing private medical information. To mitigate privacy leakage, it is essential to implement robust key management practices, regularly update encryption algorithms to address any discovered vulnerabilities, and employ multi factor authentication (MFA) for accessing encryption keys.

Aggregation Attacks

Aggregation attacks pose another risk, involving the combination of data from multiple sources to infer sensitive information that may not be apparent from any single source alone. In this context, an aggregation attack could occur if an attacker gains access to multiple encrypted data blocks from the blockchain and attempts to correlate them to reconstruct patient information. To defend against such attacks, data should be fragmented so that individual data blocks are insufficient to reconstruct meaningful information. Additionally, implementing differential privacy techniques, where random noise is added to the data, can help prevent attackers from drawing accurate inferences.

Collusion Attack

Collusion attacks involve multiple parties conspiring to break the security of the system by combining their access to different parts of it to gain unauthorized access to sensitive information. In the proposed architecture, a collusion attack could occur if multiple unauthorized users or nodes in the blockchain network collaborate to decrypt and access medical records. A potential defense against collusion attacks includes employing a consensus mechanism within the blockchain that prevents any single node or small group of nodes from controlling the decision-making process. Furthermore, using secure multi party computation (SMPC) can ensure that no single party has full access to sensitive data, even when collaborating.

While the current system architecture offers strong protection against many types of attacks, further research is necessary to analyze and improve its resistance to these threats. This includes conducting penetration testing and security audits as well as developing new techniques aimed at enhancing data privacy and security in response to evolving threats. Additionally, the proposed system has been evaluated for security which is briefly described in the subsequent section.

4.2. Performance Analysis – Security Analysis

The performance of the present work is examined by undertaking a security analysis of different security functions namely privacy, access control, integrity, authentication, cryptographic function, and blockchain-based. Three conventional types of research have been considered for this analysis [46-48]. Obtained outcomes are shown in table 7.

Table-7 Security Analysis

Function	**[46]**	**[47]**	**[48]**	**Proposed system**
Blockchain-based	✓	✓	✓	✓
Privacy	✓	✓	✓	✓
Integrity	✗	✗	✓	✓
Access control	✗	✓	✗	✓
Authentication	✓	✓	✓	✓
Cryptographic function	✓	✓	✓	✓

From the analysis, it is found that the existing study [46] has considered four functions namely privacy, authentication, cryptographic function, and blockchain-based. Whereas, the conventional work [47] has regarded privacy, authentication, cryptographic function, access control, and blockchain-based, while, the study has disregarded integrity. Similarly, the research [48] has focussed on functions namely privacy, authentication, cryptographic function, integrity, and blockchain-based, while, the study has disregarded integrity access control. On contrary, the proposed system provides all the 6 security functions considered for analysis which explores its outstanding performance than conventional works. Besides, security analysis is performed with specific values and portrayed as follows,

Key Sensitivity Analysis

Key sensitivity analysis focuses on demonstrating how sensitive the encryption/decryption process is to minor changes in the key. Original key used is 0.123456789 and modified key used is 0.123456780. Thus, the decryption with original key successfully decrypts to the original plaintext and the modified key resulted in completely different or unreadable text. Here, success rate of decryption fails and resulted in completely different and unreadable text.

Entropy Calculation

The primary motto of the entropy calculation deals with measuring the randomness of the generated keys. Here, the key entropy obtained is 7.98 bits per byte and the entropy value obtained for sample 1 is 7.98 bits per byte, entropy for sample 2 is 7.95 and entropy value for sample 3 is 7.97.

Avalanche Effect Measurement

Avalanche effect measurement primarily indicates on determining how a small changes in input affects the output. Where, 52% of bits changed in the cipher text when a single bit in the plaintext is modified. Here, 1 bit change resulted in 52% percentage of bits changed in cipher text.

Correlation Analysis

Correlation analysis focuses on assessing the correlation between the plaintext and ciphertext, ensuring no patterns exist. Here, the correlation coefficient resulted in 0.002, thereby indicating that there are no detectable pattern. Hence, Pair 1 of plaintext- Ciphertext results in correlation coefficient of 0.002, Likewise, Pair 2 and Pair 3 of plaintext- Ciphertext results in correlation coefficient 0.003 and 0.001 correlation coefficient.

Resistance to Known Attacks

Resistance to known attack factor quantify the resistance of the cryptosystem against brute force differential and linear cryptanalysis. Here, size of key space is 2128 to crack, then differential Cryptanalysis of success probability is 290 and linear cryptanalysis success probability is 280. Here, estimated time to break for brute force attack is 1020, where for differential cryptanalysis and linear cryptanalysis is considered to be infeasible.

Efficient Metrics Comparison

Eventually, the model is compared with system efficient metrics against conventional AES-128 for different parameters. where, the key generation time is improved by 36% faster than traditional model. likewise, encryption time (ms), decryption time (ms) and memory usage in kb for 20% faster, 19% faster and 11% less than the traditional model.

The proposed system is capable of eliminating the demerits of storing keys and enhancing the encryption security due to M-AES with the use of random keys relying on chaos synchronization. Furthermore, as the study relies on the blockchain concept with MD5 hashing, security gets enhanced further. Due to the advantageous nature of the proposed work, better outstanding results have been attained which is confirmed through comparative and security analysis.

V. CONCLUSION

The study aimed to secure the proposed merging technique encompassing patient ID and medical records using Modified-AES based on Chaotic Random Key Generation and MD5 hashing algorithm to achieve data integrity. The performance of the proposed work was evaluated to assess its efficacy in execution time, memory consumption for different encrypted file sizes, key generation time, encryption time, and decryption time.

In practical implication approach, the projected model can be used as a novel synchronization technology among chaotic systems, in aspects of enhancing security by dynamically changing the static keys. The use of MD5 hashing and M-AES encryption strengthens and enhances the rates of data protection. Whereas, on a theoretical implication aspect, the dynamic key system are relied to enhance the rates of resistance against cryptographic attacks. Whereby, the combination of MD5 and M-AES are involved in ensuring the rates of secured norms of data transmission. Moreover, higher level of security are ensured, whereby a long-term protection are used, which intends to prevents adversaries from gaining a static target for prolonged attacks. Additionally, the security level

of the proposed system was examined by comparing it with the traditional system by undertaking a security analysis in terms of significant functions namely blockchain-based, integrity, privacy, authentication, access control, and cryptographic function. Analytical outcomes have revealed the outstanding performance of the proposed system than conventional works that showed less execution time, memory consumption, key generation time, encryption time, and decryption time. The proposed system also fits all the security functions considered in the analysis. This system could benefit both the doctors and the patients to retrieve their data securely due to its outstanding performance. In the future, different hashing and cryptographic algorithms can be considered. Some of the other advantages of the projected system are,

- ➔ The proposed model can be leveraged to generate keys having a higher range of entropy, which is achieved by enhancing the randomness of the encryption keys.
- ➔ Additional layer to the chaotic systems in aspects of key generation, the complexity tends to make them more difficult for attackers for the action of decrypting the data if they are devoid to have access upon the current key.
- ➔ The Chaotic based systems are prone to exhibit properties such as sensitivity to some of the initial conditions, which in turn makes them to be resistant to certain forms of cryptographic attacks.

As a part of future scope,

Chaotic-based key generation can be explored based upon the act of integrating them with quantum-resistant cryptographic schemes and their usage with applications. Thus, upon the investigation the use of dynamically changing chaotic systems for the aspects of key generation, can involve in making the system parameters to enhance the security.

- Investigating and implementing more advanced hashing and cryptographic algorithms could enhance the overall security of the system.
- This in turn involves in exploring parallel processing, distributed computing, or cloud-based solutions.

Followed by, the Limitation of the projected model are,

- The effectiveness of a chaotic system in cryptographic applications, rely upon the unpredictability and sensitivity to initial conditions.
- The chaotic system's synchronization are used the static key which turns random and dynamic mode, which has to be maintained at any of the open channels.

Acknowledgement

None

Funding

There is no funding for this study

Conflict of interest

There is no conflict of interest for this study

References

[1] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informatics Journal,* vol. 22, no. 2, pp. 177-183, 2021.

[2] A. J. Holmgren, N. L. Downing, M. Tang, C. Sharp, C. Longhurst, and R. S. Huckman, "Assessing the impact of the COVID-19 pandemic on clinician ambulatory electronic health record use," *Journal of the American Medical Informatics Association,* vol. 29, no. 3, pp. 453-460, 2022.

[3] B. L. Jimma and D. B. Enyew, "Barriers to the acceptance of electronic medical records from the perspective of physicians and nurses: A scoping review," *Informatics in Medicine Unlocked,* p. 100991, 2022.

[4] P. Pandey and R. Litoriya, "Securing and authenticating healthcare records through blockchain technology," *Cryptologia,* vol. 44, no. 4, pp. 341-356, 2020.

[5] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Computers & security,* vol. 97, p. 101966, 2020.

[6] H. B. Mahajan *et al.*, "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems," *Applied Nanoscience,* pp. 1-14, 2022.

[7] W. Bani Issa *et al.*, "Privacy, confidentiality, security and patient safety concerns about electronic health records," *International Nursing Review,* vol. 67, no. 2, pp. 218-230, 2020.

[8] K. B. Adedeji, N. I. Nwulu, C. Aigbavboa, and S. L. Gbadamosi, "Assessment of Encryption and Decryption Schemes for Secure Data Transmission in Healthcare Systems," in *2019 IEEE AFRICON*, 2019, pp. 1-6: IEEE.

[9] M. N. V. Pardakhe and V. Deshmukh, "A Secure EHR Protection Strategy by Hybrid Encryption Scheme with Permissioned Blockchain," *JOURNAL OF ALGEBRAIC STATISTICS,* vol. 13, no. 2, pp. 2102-2120, 2022.

[10] S. O. Ganiyu, O. M. Olaniyi, and T. Orooniyi, "Securing Electronic Health Record System Using Cryptographic Techniques," 2019.

[11] D. Tith *et al.*, "Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability," *Healthcare informatics research,* vol. 26, no. 1, pp. 3-12, 2020.

[12] H. Qiu, M. Qiu, M. Liu, and G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0," *IEEE journal of biomedical and health informatics,* vol. 24, no. 9, pp. 2499-2505, 2020.

[13] S. Mhatre and A. V. Nimkar, "Secure cloud-based federation for EHR using multi-authority ABE," in *Progress in Advanced Computing and Intelligent Engineering*: Springer, 2019, pp. 3-15.

[14] P. Zeng, Z. Zhang, R. Lu, and K.-K. R. Choo, "Efficient policy-hiding and large universe attribute-based encryption with public traceability for internet of medical things," *IEEE Internet of Things Journal,* vol. 8, no. 13, pp. 10963-10972, 2021.

[15] G. Ramu, "A secure cloud framework to share EHRs using modified CP-ABE and the attribute bloom filter," *Education and Information Technologies,* vol. 23, no. 5, pp. 2213-2233, 2018.

[16] S. Farzana and S. Islam, "Symmetric key-based patient controlled secured electronic health record management protocol," *Journal of High Speed Networks,* vol. 25, no. 3, pp. 221-237, 2019.

[17] N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "Secure mobile health system supporting search function and decryption verification," *Journal of Ambient Intelligence and Humanized Computing,* vol. 12, no. 2, pp. 2221-2231, 2021.

[18] T. Bhatia, A. K. Verma, and G. Sharma, "Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing," *Concurrency and Computation: Practice and Experience,* vol. 32, no. 5, p. e5520, 2020.

[19] F. AthishMon and K. Suthendran, "Combined cryptography and digital watermarking for secure transmission of medical images in EHR systems," *International Journal of Pure and Applied Mathematics,* vol. 118, no. 8, pp. 265-269, 2018.

[20] J. G. M. Srivastava and R. Sheeja, "Design and implementation of crypto based water marking techniques for EHR security," *Test Engineering and Management,* vol. 82, pp. 10788-10792, 2020.

[21] J. Zhang, H. Liu, and L. Ni, "A secure energy-saving communication and encrypted storage model based on RC4 for EHR," *Ieee Access,* vol. 8, pp. 38995-39012, 2020.
[22] Y. S. Abdulsalam, O. M. Olaniyi, and A. Ahmed, "Enhanced tiny encryption algorithm for secure electronic health authentication system," 2018.
[23] M. B. Renardi, N. C. Basjaruddin, and E. Rakhman, "Securing electronic medical record in near field communication using advanced encryption standard (AES)," *Technology and Health Care,* vol. 26, no. 2, pp. 357-362, 2018.
[24] N. Titus and M. Johnson, "A Framework to Enhance Patients Electronic Health Records Sharing," *International Journal of Technology and Management,* vol. 6, no. 2, pp. 11-11, 2021.
[25] M.-T. Chen and T.-H. Lin, "A Provable and Secure Patient Electronic Health Record Fair Exchange Scheme for Health Information Systems," *Applied Sciences,* vol. 11, no. 5, p. 2401, 2021.
[26] A. Sowmyashree and B. Sahanaraj, "An Efficient Method for Secure Access of EHR."
[27] Y. M. Essa, E. E.-D. Hemdan, A. El-Mahalawy, G. Attiya, and A. El-Sayed, "IFHDS: intelligent framework for securing healthcare BigData," *Journal of medical systems,* vol. 43, no. 5, pp. 1-13, 2019.
[28] K. Tamilarasi and A. Jawahar, "Medical data security for healthcare applications using hybrid lightweight encryption and swarm optimization algorithm," *Wireless Personal Communications,* vol. 114, no. 3, pp. 1865-1886, 2020.
[29] N. M. Hamed and A. A. Yassin, "Secure Patient Authentication Scheme in the Healthcare System Using Symmetric Encryption," *Iraqi Journal for Electrical And Electronic Engineering,* vol. 18, no. 1, 2022.
[30] P. Chinnasamy and P. Deepalakshmi, "HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud," *Journal of Ambient Intelligence and Humanized Computing,* vol. 13, no. 2, pp. 1001-1019, 2022.
[31] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *Journal of medical systems,* vol. 42, no. 8, pp. 1-9, 2018.
[32] B. Arunkumar and G. Kousalya, "Blockchain-based decentralized and secure lightweight e-health system for electronic health records," in *Intelligent Systems, Technologies and Applications*: Springer, 2020, pp. 273-289.
[33] I. Abunadi and R. L. Kumar, "BSF-EHR: blockchain security framework for electronic health records of patients," *Sensors,* vol. 21, no. 8, p. 2865, 2021.
[34] A. Ali *et al.*, "A Novel Secure Blockchain Framework for Accessing Electronic Health Records Using Multiple Certificate Authority," *Applied Sciences,* vol. 11, no. 21, p. 9999, 2021.
[35] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access,* vol. 7, pp. 147782-147795, 2019.
[36] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain," *Information Sciences,* vol. 485, pp. 427-440, 2019.
[37] S. G. Alonso, J. Arambarri, M. López-Coronado, and I. de la Torre Díez, "Proposing new blockchain challenges in ehealth," *Journal of medical systems,* vol. 43, no. 3, pp. 1-7, 2019.
[38] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A blockchain-based medical data sharing and protection scheme," *IEEE Access,* vol. 7, pp. 118943-118953, 2019.
[39] R. H. Hylock and X. Zeng, "A blockchain framework for patient-centered health records and exchange (HealthChain): evaluation and proof-of-concept study," *Journal of medical Internet research,* vol. 21, no. 8, p. e13592, 2019.
[40] P. A. Sri and D. L. Bhaskari, "Blockchain technology for secure medical data sharing using consensus mechanism," *Materials Today: Proceedings,* 2020.
[41] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," *Journal of Big Data,* vol. 5, no. 1, pp. 1-18, 2018.
[42] M. Gupta and A. Sinha, "Enhanced-AES encryption mechanism with S-box splitting for wireless sensor networks," *International Journal of Information Technology,* vol. 13, no. 3, pp. 933-941, 2021.
[43] O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," *Ad Hoc Networks,* vol. 115, p. 102448, 2021.

[44] B. Rasina Begum and P. Chitra, "ECC-CRT: An Elliptical Curve Cryptographic Encryption and Chinese Remainder Theorem based Deduplication in Cloud," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1683-1702, 2021.
[45] E. Subramanian and L. Tamilselvan, "Elliptic curve Diffie–Hellman cryptosystem in big data cloud security," *Cluster Computing*, vol. 23, no. 4, pp. 3057-3067, 2020.
[46] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *Journal of medical systems*, vol. 42, no. 8, pp. 1-13, 2018.
[47] O. I. Khalaf, G. M. Abdulsahib, H. D. Kasmaei, and K. A. Ogudo, "A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications," *International Journal of e-Collaboration (IJeC)*, vol. 16, no. 1, pp. 16-32, 2020.
[48] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future generation computer systems*, vol. 95, pp. 420-429, 2019.