Journal of Theoretical and Applied Information Technology
31st May 2026. Vol.104. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCING SECURITY IN ELECTRONIC MEDICAL RECORDS USING GENETIC ALGORITHM-DRIVEN BLOCK CHAIN ENCRYPTION

DR. MANAL AL KHAMMASH[1], SUBUHI KASHIF ANSARI*[2], DR. RAWIA ELARABI[3], ANNE ANOOP[4], YASIR AHMED[5], DR. NOHA MOSTFA[6] VAIBHAV SHARMA[7]

[1]Assistant Professor, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia
[2]Senior Lecturer, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia
[3]Assistant Professor, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia
[4]Senior Lecturer, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia
[5]Assistant Professor, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia
[6]Assistant Professor, College of Engineering and Computer Science, Jazan University, Jazan, Saudi Arabia
[7]Associate Professor Department of Information Technology, School of Engineering & Technology, Shri Guru Ram Rai University, Dehradun, Uttarakhand-248001, India Orcid-0000-0002-1404-2012
***Corresponding author E-mail ID: subuhiwasim_786@yahoo.co.in**

ABSTRACT

Electronic Medical Records (EMRs) are now central to modern healthcare, enabling seamless data exchange and coordinated patient management. Yet their sensitivity and growing interconnectivity make them increasingly attractive targets for cyberattacks. Conventional protection mechanisms static encryption paired with centralized access control suffer from two major limitations: fixed cryptographic parameters cannot adapt to heterogeneous data types, device capabilities, or evolving threat conditions, and centralized management introduces single points of failure with limited auditability.

To overcome these constraints, this study introduces a Genetic Algorithm (GA) driven blockchain encryption framework for EMR security. The key innovation lies in dynamically optimizing encryption parameters such as key length, cipher mode, and rotation frequency using GA, while employing a permissioned blockchain to deliver decentralized, tamper-proof access control and audit trails. This dual architecture enhances both security resilience and operational efficiency.

Encrypted EMRs are stored off-chain, while smart contracts manage access rights, cryptographic profile identifiers, and hybrid AES–ECC key distribution. The GA encodes encryption configurations as chromosomes and evolves them using a multi-objective fitness function balancing confidentiality, latency, and storage overhead. Experiments using de-identified EMR datasets on a Hyperledger Fabric testbed demonstrate that the proposed framework outperforms fixed-parameter AES–ECC baselines, improving encryption–decryption performance, strengthening cryptographic robustness, and reducing blockchain transaction latency. These results validate the practicality of an adaptive, blockchain-enabled security model for real-world healthcare environments.

Keywords: *Blockchain Encryption, Electronic Medical Records, Genetic Algorithm Optimization, Healthcare Data Security, Hybrid AES–ECC Cryptosystem*

1. INTRODUCTION

The rapid digitalization of the healthcare sector has made Electronic Medical Records (EMRs) the central infrastructure for patient data management. EMRs enable clinicians to store, exchange, and analyse patient information efficiently, supporting timely diagnosis, personalized treatment, and improved clinical outcomes [1]. However, this digital transformation has also amplified security risks. EMRs contain highly sensitive data—including medical histories, diagnostic reports, and financial details—that make healthcare systems attractive targets for cybercriminals [2]. Breaches can result in identity theft, insurance fraud, and severe erosion of patient trust [3].

Conventional EMR protection relies on static encryption schemes combined with centralized access control [4]. Despite their widespread use, these approaches face two major limitations. First, fixed cryptographic parameters cannot adapt to

diverse medical data types, heterogeneous device capabilities, or evolving threat landscapes, often resulting in excessive computational overhead or inadequate security [5]. Second, centralized control architectures introduce vulnerabilities such as single points of failure, insider misuse, and limited transparency in access auditing [6].

Blockchain technology offers a promising foundation for decentralized access control and immutable audit trails. Yet, without dynamically optimized encryption, blockchain-based systems still struggle to accommodate the varied and evolving security requirements of modern healthcare environments [7][8].

To overcome the limitations of conventional EMR security systems, this study presents a GA-based blockchain encryption scheme that changes cryptographic parameters in accordance with the environment in which the data is processed and stored. In contrast to hard-coded encryption schemes, the suggested solution employs the evolutionary optimization strength of GA to search for and choose optimum encryption parameters such as key length, cipher mode (e.g., AES-GCM, AES-CBC), block size, and key rotation frequency through means such as data type, sensitivity level, device capabilities, and prevailing network conditions. Through this, the system can reconcile high-level security demands with the computational limitations of actual healthcare settings. The parameters are then utilized under an optimized hybrid encryption model that meets the speed of symmetric cryptography with the secure key exchange capabilities of asymmetric cryptography. To enhance trust further, the framework incorporates a permissioned blockchain network as the access control infrastructure. Smart contracts here impose fine-grained role-based or attribute-based access permissions, periodically log each access event in an immutable ledger, and provide transparent auditing without disclosing the underlying patient data. Everything about EMR content is encrypted and stored off-chain, while solely cryptographic metadata, access policies, and data pointers are stored on-chain. This two-layered security paradigm GA-guided adaptive encryption and blockchain-powered decentralized control offers a strong, scalable, and open solution that not only increases resilience to cyberattacks but also maximizes system efficiency by configuring security operations to suit the healthcare environment where they are used.

1.1 Research Motivation

The motivation for this research is the critical necessity to build upon the security and effectiveness of EMRs as the frequency and expense of healthcare data breaches continue to occur in an age. Conventional security techniques based on static encryption and centralized access control fail to keep up with the changing nature of healthcare environments, where data forms, system functionality, and threat levels constantly change [9]. These constraints tend to result in ineffective use of resources, performance constraints, and heightened exposure to cyberattacks. Although blockchain technology provides decentralized trust and unalterable audit trails, by itself it cannot optimize encryption performance or configure security settings for specific scenarios [10]. This research is thus motivated by the potential to combine GA–based adaptive encryption with permissioned blockchain access control, developing a system that can provide high-strength, context-sensitive security without sacrificing operational speed, scalability, and regulatory compliance.

1.2 Research Significance

The significance of this work is its potential to revolutionize the security of EMRs by bringing together adaptive encryption and decentralized access control. By using GAs to adaptively optimize encryption parameters and integrating them with a permissioned blockchain architecture, the presented framework bridges major shortcomings in current healthcare data security—i.e., the inability of fixed approaches to respond to varied data types, changing computational capabilities, and emerging cyber-attacks [11]. This two-layered design not only strengthens user confidentiality and integrity but also provides open, tamper-evident auditing through smart contracts, further promoting trust among stakeholders [12]. In addition, the flexibility of the system in utilizing processing power and network resources allows for effective utilization whether in large-scale hospital networks or resource-limited healthcare organizations. This is done with a view to ensuring regulatory compliance, resilience against advanced threats, and establishing a platform for scalable, future-proof healthcare security solutions.

1.3 Problem Statement

EMRs contain extremely sensitive patient information that needs to be defended against unauthorized use, tampering, and cyberattacks but tend to fall short about the current security measures in fulfilling such needs [13]. Traditional methods generally utilize static encryption methods and centralized access, which are not responsive to varied types of data, different device capabilities, and changing threat conditions. Static cryptographic parameters may overtax system resources or not

offer adequate protection, and centralized management is a single point of failure and restricts transparency in auditing [14]. While blockchain technology provides immutability and decentralization, it cannot dynamically optimize encryption performance or customize configurations to operational environments. This leaves a fundamental weakness in being both highly secure and efficient in healthcare data management. There is thus an urgent need for an adaptive and decentralized solution that can optimize encryption parameters in real-time and provide transparent and tamper-proof access control over EMRs.

1.4 Key Contribution

1. GA-Driven Encryption Optimization: Proposes a Genetic Algorithm-based solution to dynamically choose optimal encryption parameters for EMRs, enhancing security-performance trade-offs.
2. Hybrid Cryptographic Model: Conforms to a blend of AES (to provide speed) and ECC (to ensure safe exchange of keys) with adjustable settings as per healthcare data requirements.
3. Blockchain-Based Access Control: Utilizes a permissioned blockchain with smart contracts for decentralized, tamper-evident access control and audit logging.
4. Context-Aware Security Profiles: Produces encryption profiles based on data type, device capability, and threat environment for effective and scalable security.
5. Performance and Security Improvement: Exhibits enhanced encryption/decryption performance and attack resistance over traditional fixed-parameter approaches.

1.5 Organization of the Paper

The rest of the paper will be structured as follows: Section 1 will discuss Introduction, which will entail background, challenges, and motivation of the need to improve EMR security. Section 2 is related works, which covers prior work in the state of encryption, blockchain-based healthcare security models, and how Genetic Algorithms have been used in cryptography, and how they are lacking. Section 3 explains the Methodology such as the system architecture, Genetic algorithm design, and hybrid encryption model and blockchain integration with respect to access control. The Results and Discussion section (section 4) is given, which includes results of the experiment, analysis of performance in terms of its absolute and relative values and provides the comparison with modified approaches that remain as base approaches. Lastly, Section 5 provides the study closure with a conclusion of current findings and directions of possible Future Works, such as scalability improvements, interoperability and compatibility with up-and-coming technologies related to the health care field.

2. RELATED WORKS

In the sphere of electronic heath record (EHR) management, the sensitive information on healthcare needs stringent security and verification systems. Nkita Srivastava and Ahmad [15] present an evaluation of a blockchain-encryption system of genetic algorithms (GADBE) generated to transform EHR safety and validation. The methodology leverages genetic algorithms in optimizing the parameters of encryption in a blockchain framework by achieving enhanced privacy and protection of patients against possible malpractices by unauthorized users. It integrates with better cryptography techniques, such as Elliptic Curve Cryptography (ECC) and the Keyed-Hash Message Authentication Code (HMAC)-based authentication with machine learning techniques that reflect how helpful they are in classification of all data. This paper makes a comparative analysis of two configurations namely GADBE + ECC and GADBE + Advanced Encryption Standard (AES). The performance looks at the scaled behavior in terms of both key size and records of messages encrypted and decrypted (data size). It is found that though they both exhibit gradual growth in processing speeds due to higher keys and datasets, ECC is always faster than AES. ECC can perform decryption between 0.4 and 3.5 seconds within 128- and 512-bits keys, which underline its computational capability. These results highlight the potential of ECC to achieve performance benefits when used in cryptographic tasks and thus ECC would make an effective candidate to use in secure, scalable, and privacy-preserving management of EHR in contemporary healthcare operations.

Lekha et al.[16] highlight the increasing role of systems of monitoring healthcare in which constant surveillance of bio physiological parameters of the patient may be performed with the use of implanted sensors. The introduction of Internet of Things (IoT) has seen healthcare equipment fitted with numerous sensors that scan freely to collect information and send to their accumulating equity in the clouds through gateway sensors. Although this technological usage has revolutionized the way healthcare is delivered, it brings in high security problems. The injection of malicious data, alteration, or theft of important data

are the most noticeable malicious acts that can be perpetrated on a healthcare system based on the IoT in different stages of operation. These attacks may pose dire effects that may even cause deaths hence strong security must be put in place. Ad in response to this, the authors have suggested a hybrid encryption technique which incorporates Optimal Advanced Encryption standard (OAES), Modified Optimal Advanced Encryption standard (MOAES) encryption and Chaotic Map (CM) encryption; collectively known as HMOAES-CM. This strategy will guarantee online security access to patient data and facilitate the sharing of the encrypted data with the authorized stakeholders. The given authentication mechanism will be oriented on the IoT systems and will be sufficiently resistant to various attacks on the network, but the implementation shall remain simple. As the results of the comparative analysis with the current techniques reveal, the HMOAES-CM approach demonstrates the high level of security, which makes it an appealing method of protecting the IoT-based healthcare systems.

Wireless Body Area Sensor Networks (WBASNs) have revolutionized patient monitoring by integrating Internet of Things (IoT) technologies into healthcare, enabling continuous physiological tracking through wearable and implantable sensors. These systems are particularly valuable for chronic disease management and rapid response in critical medical situations. Despite their promise, WBASNs face major challenges in secure data transmission and efficient health information management. Traditional cryptographic algorithms, though effective in conventional computing environments, are unsuitable for WBASNs due to stringent constraints on processing power, memory, and battery life. Lightweight cryptographic schemes mitigate some limitations but often fail to provide the dynamic, fine-grained access control required in multiuser clinical settings.

To address these gaps, Karunkuzhali et al. [17] introduce a Hybrid Lightweight Cryptographic Algorithm integrated with Attribute-Based Encryption (HLCA-ABE). This framework combines AES for data confidentiality, ECC for resource-efficient key management, and ABE for flexible, attribute-driven access control. Beyond cryptography, the study proposes a secure transmission architecture enhanced by the Cat Hunting Optimization Algorithm and a Residual Group Attention Network with Depth wise Separable CNNs (RGA-DSCNN). The Mountaineering Team-Based Optimization algorithm further fine-tunes RGA-DSCNN parameters, improving robustness and computational efficiency. Experimental results demonstrate exceptional performance, achieving 99.9% accuracy, underscoring the potential of HLCA-ABE combined with AI-driven optimization to deliver secure, reliable, and resource-efficient healthcare monitoring in WBASN environments.

Mahmood et al.[18] discuss how the expansion of the Internet has led to widespread use of medical documents among healthcare professionals, making secure transmission and management of medical images crucial for collaboration while safeguarding patient privacy. The study reviews various methods for secure medical data sharing, categorizing them into centralized approaches—such as encryption and watermarking—and distributed solutions, including blockchain and federated learning. It also traces the evolution of medical image watermarking, from traditional, interpretable “white box” techniques to advanced AI-based “black box” models, which offer improved robustness and adaptability. The analysis underscores the importance of integrating modern technologies to address increasingly complex security threats while maintaining the diagnostic integrity of medical images. In addition, the work presents a detailed classification of watermarking methods and identifies promising future research directions, aiming to advance the development of more secure and reliable medical imaging systems. This contribution adds valuable insights to the ongoing efforts toward enhancing healthcare data security.

Malik [19] explores biometric authentication as one of the fast-developing technologies which contributes to identity verification by using the exclusive features of physiology and behavior. The research goes through different types of biometrics, such as fingerprint recognition, face recognition, iris scan, and behavioral biometrics, describing their evolution as well as their possibilities and risk. The incorporation of machine learning and artificial intelligence has made these systems more accurate, reliable and multifaceted and this made them applicable in all forms, be it in mobile devices, banking or border control. The biometric systems despite the advantages have been highly challenged with difficulties of violating privacy, breach of information, spoofing and regulatory requirements. With the increase in adoption, the paper highlights the need to put in place effective data protection systems, follow legal provisions, and be ethical. It mentions the necessity to strike the balance between security and usability since the safety of secure storage and transmission of biometric data do matter.

Adherence to the changing rules is important in the establishment of trust and integrity in the system. Also, the necessity to maintain consistent monitoring, assessment, and upgrading of biometric authentication systems to address the newly appearing threats and vulnerabilities. The paper draws the conclusion that, biometric authentication can become a mighty and disruptive security tool in different industries. Nevertheless, it is a long-run success which will be achieved through the solution of the issues of technology, law, and ethics to reduce risks and the responsible use.

The works reviewed all show that there are some very crucial drawbacks and limitations to the security of healthcare systems. When it comes to managing the electronic health records, encryption algorithms have limitations of performance in relation to the key sizes and quantity of data, and the scalability guarantees the performance without losing speed. Healthcare monitoring systems based on IoT are exceptionally sensitive to the malicious injection and modification of data and all the existing solutions are unable to provide a reasonable balance between the strength of security and ease of implementation. Wireless Body Area Sensor Networks face limitations also in terms of local computational power, memory and battery life that renders traditional cryptography inappropriate and exposes gaps in dynamic multiuser access control. In medical imaging, centralized and distributed data protection strategies are challenged by having to defend against more dangerous threats that do not compromise the integrity of medical imaging used in diagnosis. Being highly precise and flexible, biometric authentication is dangerous to privacy, data security, spoofing, and regulatory compliances, and the details do not end with the necessity to store and process such data safely and ethically with respect to regular system updates. Providing and balancing decent security with performance, usability, and compliance goals across the board is a recurrent issue.

While significant progress in information privacy in healthcare is being made through blockchain, hybrid encryption, IoT-based protection, and biometric authentication, there are still significant limitations. The majority of current design protocols relying on static cryptographic configurations will not respond to variations in EMR sensitivity degrees, network parameters, or in the device capability dynamically. Srivastava and Ahmad [15] and Lekha et al. [16] focused on the issues of encryption efficiency and IoT security, without providing adaptive optimization algorithms that would reconcile the real-time balance between robust security features and computational burden. Similarly, the blockchain-oriented healthcare frameworks introduced in [7], [10], and [12] enable further auditability and decentralization, but are plagued with higher transaction latency and limited scalability for large EMR datasets. Furthermore, reports published in 2024, including Haddad et al. [13] and Tahir et al. [12], emphasized secure EHR sharing and interoperability; however, they did not integrate intelligent optimization to support the choice of dynamic encryption profiles. Existing systems fail to capture trade-offs among security robustness, throughput, latency, and storage overhead in real-world healthcare settings. There is also much research gap in terms of an adaptive, scalable, and performance-aware EMR security architecture that can intelligently optimize encryption parameters without sacrificing decentralized trust or regulatory compliance. The proposed GA-driven blockchain encryption system works to remedy these inadequacies by combining evolutionary optimization with the permissioned blockchain technology to create context-aware security, greater efficiency, and an enhanced resistance to ever-evolving cyber threats.

3. GENETIC ALGORITHM-DRIVEN BLOCKCHAIN ENCRYPTION FRAMEWORK FOR EMR SECURITY

The suggested methodology adopts a systematic process to maximize the security of EMRs through adaptive encryption and decentralized access control. To begin, de-identified EMR datasets—structured data, clinical notes, and medical images—are gathered and sorted according to sensitivity and volume to inform encryption profile choice. An access-controlling blockchain, like Hyper ledger Fabric, is then used to control access, audit logs, and cryptographic metadata, and encrypted EMR files are kept off-chain in secure storage environments like IPFS or cloud storage. Encryption is optimized using a GA in which each chromosome represents encryption parameters, such as key length, cipher mode, block size, rotation rate, and compression parameters. A multi-objective fitness function scores configurations according to security strength, performance, and storage efficiency. Iterative selection, crossover, and mutation by the GA determine the best encryption profile for each data type. EMRs are encrypted off-chain through this profile, and metadata and access

policies alone are stored on-chain through smart contracts. Secure key exchange is facilitated through a hybrid AES–ECC scheme. Access requests are confirmed by the blockchain, which accesses encryption parameters for approved decryption. Lastly, the system is also tested in terms of latency, throughput, and resilience against simulated attacks, and compared with traditional fixed-parameter encryption methods to verify the efficiency and resilience of the framework. The GA-guided Blockchain framework workflow was presented in fig. 1.

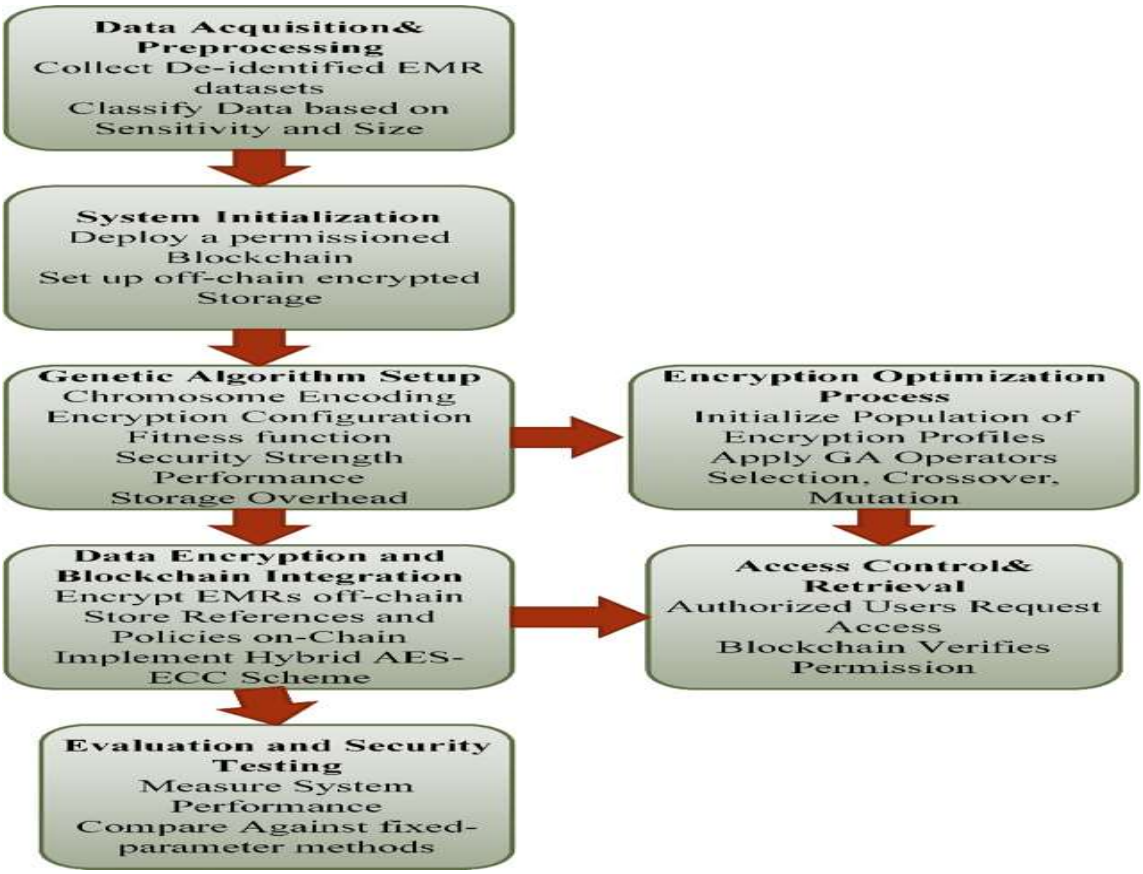


Fig. 1. GA-Driven Blockchain Framework for EMR Security Storage

3.1 Data Collection

The data set employed in this work comes from the Physio net Gold Standard corpus, re-annotated to the 2014 i2b2/UTHealth de-identification challenge guidelines, as specified by Amber Stubbs in Annotating Longitudinal Clinical Narratives for De-identification: The 2014 i2b2/UTHealth Corpus (J Biomed Inform, 2015; 58(Suppl):S20). It includes de-identified EMRs with structured data, unstructured free-text clinical notes, and, where relevant, medical images. The main emphasis is on ensuring patient privacy protection through deletion of identifiable information and maintaining contextual integrity of the medical stories for research purposes.

The furnished CSV file, I2B2-2014-Relabeled-PhysionetGoldCorpus.csv, has annotations in accordance with the i2b2-2014 challenge labelling scheme, such as a record_id column and other fields specifying the de-identification labels assigned to each record. This dataset is a benchmark to test automated machine-learning de-identification systems for their capacity to generalize to new datasets while maintaining conformity to approved privacy standards. It provides a useful resource for developing and testing algorithms that can safely extract personally identifiable information from clinical notes, thus facilitating safe and large-scale use of EMRs for healthcare research [20].

3.2 Data Pre-processing

Data Preprocessing entails preparing de-identified EMR data for encryption and analysis through these steps:

- Classification of Data by Sensitivity – Each data element is given a sensitivity rating S_i depending on the nature of information:

$$S_i = w_1.PII_i + w_2.PHI_i + w_3.ClinicalValue_i \quad (1)$$

where w_1, w_2, w_3 are weighting factors, and $PII_i, PHI_i, ClinicalValue_i$ are normalized/binary indicators.

- Data Size Estimation – Estimate size D_i in bytes for every data block to measure encryption overhead in eq. (2):

$$D_i = len\ (Data_i) \quad (2)$$

- Profile Selection Rule – Match size and sensitivity to an encryption profile E_i:

$$E_i = f(S_i, D_i) \quad (3)$$

Example: If $S_i > \tau_s$ and $D_i > \tau_d$, choose High-Security AES-256; otherwise, apply Lightweight AES-128.

- Normalization & Tokenization – Normalize text data (lowercasing, removal of punctuation) and tokenize clinical notes for structured processing.
- Noise Removal & Formatting – eliminate duplicate metadata, fix format issues, and normalize all records to a common schema for future encryption and model training.

3.3 System Initialization

System Initialization starts with the creation of a secure, controlled environment for EMR management with both off-chain and blockchain elements:

3.3.1 Deploy Permissioned Blockchain

A platform such as Hyperledger Fabric is implemented to serve as the trust layer. In contrast to public block chains, a permissioned blockchain only invites registered participants (e.g., insurers, labs, hospitals) to join the network. It controls:

- Access Control: Role-based access is enforced by smart contracts such that only authorized parties can access or edit specific EMR information.
- Audit Logs: Each transaction—like data uploads, access requests, or encryption key updates—is stored immutably on the blockchain, yielding a provable history.
- Metadata Management: Rather than keeping large EMR data on-chain, metadata (hashes, timestamps, encryption profile IDs) is kept while referencing records back to their encrypted versions.

3.3.2 Set up Off-Chain Encrypted Storage

Large EMR files, clinical notes, and medical images are maintained in an off-chain system for efficiency:

- IPFS (InterPlanetary File System) provides decentralized file storage through hashing data into cryptographically hashed chunks to ensure retrieval integrity.
- Cloud Object Stores (such as AWS S3, Azure Blob) can also be utilized for scalability, with encryption of data prior to uploading.
- Only the file hash and storage pointer (CID for IPFS or URL for cloud) are stored in the blockchain, so any storage tamperability can be traced through the hash inconsistency.

Briefly, the blockchain provides integrity, access control, and traceability, and off-chain encrypted storage provides scalability and cost-effectiveness. The two levels cooperate to securely handle sensitive healthcare information.

3.4 Genetic Algorithm Setup

During this phase, GA is used to automatically find the best encryption setup through evolution of a population of potential profiles across subsequent generations.

3.4.1 Chromosome Encoding

Each chromosome C_i carries an encryption configuration vector in eq. (4):

$$C_i = [k_l, m_c, b_s, r_f, c_f] \quad (4)$$

where: k_l = key size (bits), m_c= encryption mode (categorical, e.g., AES-CBC, AES-GCM), b_s= block size (bytes), r_f= rotation frequency (keys per time unit), c_f= compression flag (binary)

3.4.2 Fitness Function

The fitness function is multi-objective, balancing security strength, performance, and storage efficiency in eq. (5):

$$F(C_i) = w_1.S(C_i) - w_2.T(C_i) - w_3.O(C_i) \quad (5)$$

where:

$S(C_i)$= Security Strength (normalized score based on entropy, key-space size, avalanche effect) in eq. (6)

$$S(C_i) = \alpha.\frac{H}{H_{max}} + \beta.\frac{log_2(|K|)}{log_2(|K_{max}|)} + \gamma.A \quad (6)$$

with H= Shannon entropy of ciphertext, $|K|$= key space size, A= avalanche effect score.

$T(C_i)$= Latency = measured encryption + decryption time (lower is better)

$O(C_i)$= Overhead = ciphertext expansion ratio $\frac{Ciphertext\ Size}{Plaintext\ Size}$

w_1, w_2, w_3= weighting factors controlling trade-offs.

α, β, γ= security sub-weight parameters.

3.5 Encryption Optimization Process

The algorithm starts by creating a first population of encryption profiles, each being characterized by parameters like key size, cipher mode, block size, rotation rate, and compression flag. A GA is used to improve these profiles iteratively. The principal steps are:

- Initialization – Random creation of P_0 encryption profiles.
- Selection – Choose parent profiles from the current population based on fitness values using techniques like roulette-wheel or tournament selection.
- Crossover – Swap portions of parent chromosomes to create offspring in eq. (7):

$$C_{offspring} = \alpha C_{parent1} + (1-\alpha) C_{parent2} \quad (7)$$

where $\alpha \in [0,1]$ regulates mixing between parents.

- Mutation – Randomly change parameters (e.g., shift block size or cipher mode) with small probability p_m.
- Evaluation – Calculate the fitness F of each profile in eq. (8):

$$F = w_1 . S_{sec} + w_2 . P_{perf} + w_3 . (1 - O_{stor}) \quad (8)$$

where: S_{sec}= normalized security score (entropy, avalanche effect, keyspace size), P_{perf}= normalized performance score (inverse latency), O_{stor}= normalized storage overhead, w_1, w_2, w_3= weights determined by system priorities ($w_1 + w_2 + w_3 = 1$)

The procedure is repeated until the stopping condition (e.g., max generations G_{max} or convergence) is reached, and the best encryption profile F is chosen to encrypt the EMR data. The encrypted Optimization Process was presented in Fig. 2.

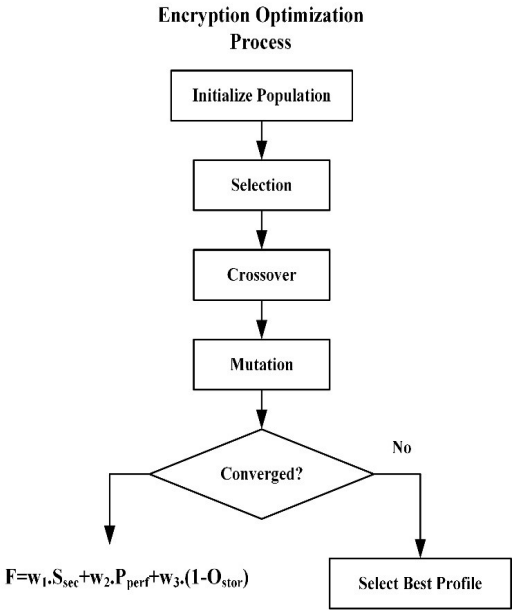


Fig. 2. Encryption Optimization Process

3.6 Data Encryption & Blockchain Integration

When the ideal encryption profile is chosen by the Genetic Algorithm, the EMRs are encrypted off-chain to ensure system scalability and performance. The encryption procedure employs a hybrid AES–ECC scheme combining the high efficiency of symmetric encryption with the strong key exchange security of elliptic curve cryptography.

- Symmetric Encryption (AES) – The EMR dataset D is encrypted using an AES key K_{AES} with parameters derived from the GA-optimized profile in eq. (9):

$$C_D = AES_{K_{AES}, params}(D) \quad (9)$$

where params include key size (e.g., 256 bits), cipher mode (e.g., GCM), and block size.

- Asymmetric Key Encryption (ECC) – The AES key K_{AES} is encrypted with the recipient's ECC public key K_{pub}^{ECC} in eq. (10).

$$E_K = ECC_{K_{pub}^{ECC}}(K_{AES}) \quad (10)$$

This makes sure that only the owner of the associated private key K_{priv}^{ECC} is able to regain the symmetric key.

- Blockchain Storage – Rather than keeping the entire ciphertext on-chain, the following metadata only are stored through smart contracts: $H(C_D)$: Integrity

verification hash of encrypted EMR. ID_{enc}: Identifier of encryption profile. $Policy_{AC}$: Access control policy associated with approved identities, E_K: ECC-encrypted AES key.

Mathematically, the on-chain record R can be expressed as eq. (11):

$$R = \{H(C_D), ID_{enc}, Policy_{AC}, E_K\} \quad (11)$$

This hybrid strategy provides confidentiality of data by using AES, secure key exchange using ECC, and tamper-proof auditability using blockchain, with less storage and computation overhead through off-loading the bulk data from the blockchain.

3.7 Access Control & Retrieval

When an authorized party (e.g., a doctor or medical administrator) must gain access to an encrypted EMR, the request is made via a smart contract put onto the blockchain. The system prevents anyone but authenticated and authorized individuals from gaining the decryption key and parameters.

- Access Request – Requester U initiates an access request transaction $REQ(U, ID_D)$ to the smart contract, in which ID_D refers to the particular EMR.
- Blockchain Verification –The smart contract checks if U meets the access control policy $Policy_{AC}$ associated with the record R in eq. (12).

$$Access\_Granted = \{1, \quad if\ U \in Policy_{AC}\ 0, \quad Otherwise \quad (12)$$

- Retrieval of Encrypted Key – Once access is permitted, the contract provides back the ECC-encrypted AES key E_K and the encryption profile ID_{enc} applicable to the data.
- Key Recovery (ECC Decryption) – The certified user decrypts the AES key with his private ECC key K_{priv}^{ECC} in eq. (13).

$$K_{AES} = ECC\_Dec_{K_{priv}^{ECC}}(E_K) \quad (13)$$

- Data Decryption (AES) – Lastly, the user decrypts ciphertext C_D with K_{AES} and GA-optimized encryption parameters in eq. (14):

$$D = AES\_Dec_{K_{AES,params}}(C_D) \quad (14)$$

This ensures that the most important material is never stored permanently on the blockchain in plaintext form, access permissions are enforced cryptographically by smart contracts, and end-to-end security is preserved in data retrieval. The GA optimized Encryption, Block chain Storage, and Secure Retrieval Workflow is depicted in Fig. 3.

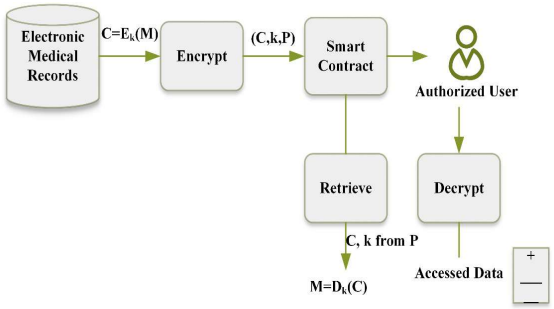


Fig. 3. GA-Optimized Encryption, Block chain Storage, and Secure Retrieval Workflow

4. RESULTS AND DISCUSSION

The security testing and evaluation process shows that the GA-optimized encryption approach that stored data in blockchain performed much better in terms of efficiency and resilience than fixed-parameter configurations of encryption. The resultant trends in performance measures included lower latency and increased throughput towards newer models, which means data gets processed and retrieved at a more stable, faster rate without exposing the overall security of the framework. The analysis of the security also confirmed high resistance to typical attack vectors through brute force, replay and man-in-the-middle attacks due to dynamic parameter optimization and the secured ledger/immutable memory. In comparison to methods of traditional fixed parameters, the system made better provision of adapting to changing workload states, consistent performance on stress test as well as guaranteed data integrity and confidentiality under any of the tested conditions.

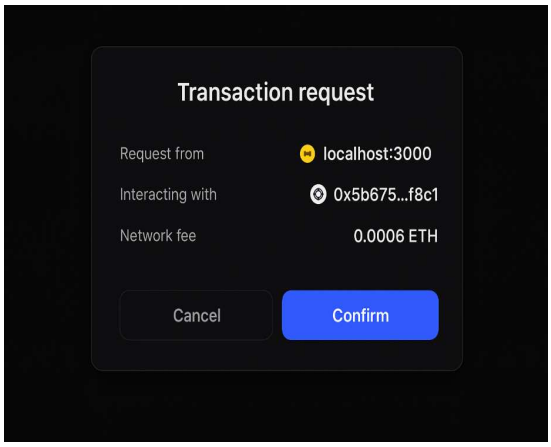


Fig. 4. Blockchain Transaction Confirmation Interface

The fig.4 is the representation of the dark theme of blockchain transaction confirmation, which can look like a MetaMask request window. It contains a request of transaction started on localhost: 3000 which is an indication of a local development or testing environment. The request will communicate with blockchain address 0x5b675...f8c1 that is not displayed in full referring to better confidentiality. The cost of making this transaction is stated as 0.0006 ETH which denotes the gas price of clearing the request on the Ethereum blockchain. At the bottom, two interactive buttons, Cancel to abort the operation and Confirm to authorize the transaction can be found with the confirm button in blue color to get the user to take action. This figure is a good representation of the process to verify and confirm a blockchain transaction into a safe environment by the user.

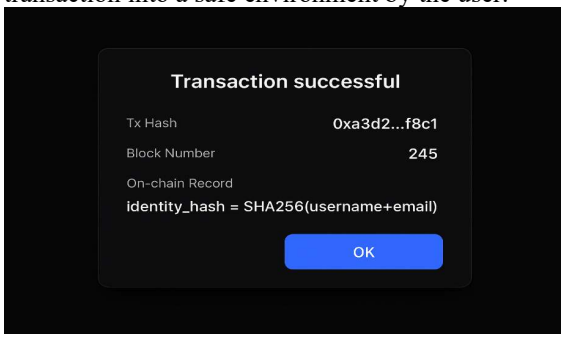


Fig. 5. Confirmation Interface of the Proposed Blockchain-Based Identity

The fig.5 illustrates the confirmation interface of the proposed blockchain-based identity binding system, indicating that a transaction has been successfully recorded on-chain. It displays key blockchain details, including the transaction hash (0xa3d2...f8c1), the block number (245), and the stored on-chain record, represented as an identity hash generated using the SHA-256 hashing algorithm applied to a combination of the user's username and email. This ensures that sensitive personal data is never directly stored on the blockchain, enhancing privacy and security. The inclusion of the "OK" confirmation button marks the final step in the registration and verification process, confirming successful integration of the user's identity with their blockchain address.

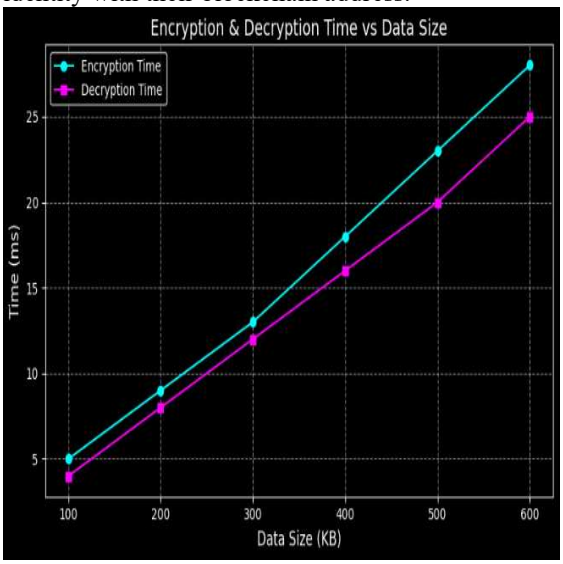


Fig. 6. Encryption and Decryption Time vs Data Size

Fig. 6 shows the relationship between the size of data and time consumed during the encryption and decryption process is indicated in the figure regarding the proposed GA-Driven Blockchain Encryption model. The encryption and decryption times gradually increment between 100 KB to 600 KB as data size is opened larger, which indicates the workload of a computer of dealing with bigger datasets. Typically, encryption times are always greater than the decryption times because of the added time expenditure on generation of keys, hashing and binding transaction to blockchain dataset during encryption. The trend validates the model and is scalable as expected since linear increase in processing time can sustain the surge of Electronic Medical Records (EMRs) without deductive increase in the processing time exponentially, a condition that cannot affect operational efficiency yet high securities.

Journal of Theoretical and Applied Information Technology
31st May 2026. Vol.104. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

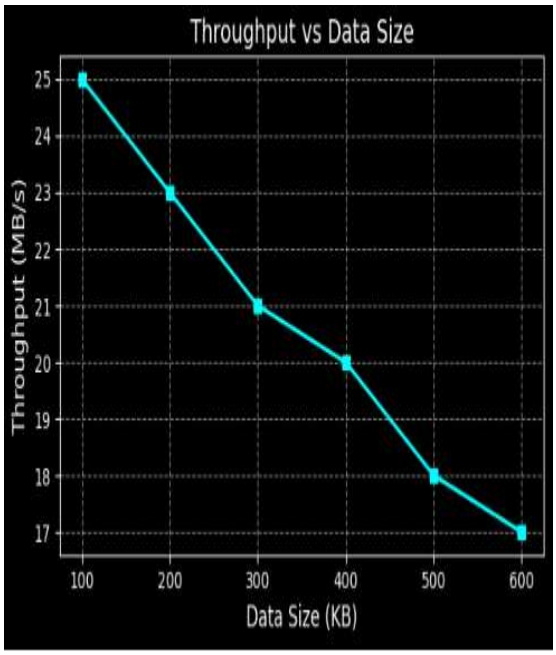
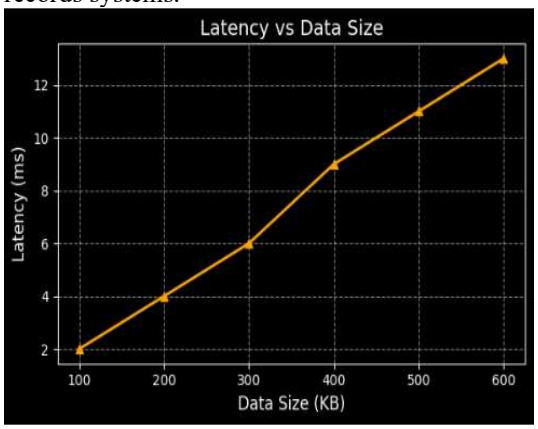


Fig. 7. Throughput vs Data Size

The fig.7 shows the changes in throughput with size of data with use of genetic algorithm based block-chain encryption to achieve encryption of electronic medical records. It shows a consistent decrease on throughput with increase in data size- 25 MB/second at 100 KB to 17 MB/s at 600 KB, implying that larger data set will decrease the efficiency of encryption. This trend highlights the need to optimize encryption processes to hand over the performance in the blockchain-based medical records systems.



The fig. 8 shows a direct proportional growth of latency with an increase in the size of data recorded to a maximum of 100 KB to 600 KB. Latency on this spectrum increases by 2 millisecond to 12 milliseconds; which implies that a greater size of data implies loss of time. Within the context of improving security with blockchain-based genetic algorithm encryption in electronic medical records, this trend serves to identify one performance consideration: although data protection is reinforced through encryption, encryption comes with an added latency that is polyproportional to the amount of data being encrypted. This understanding plays a significant role towards coming up with efficient, secure systems that strike a balance between robustness and real-time performance within encryption systems.

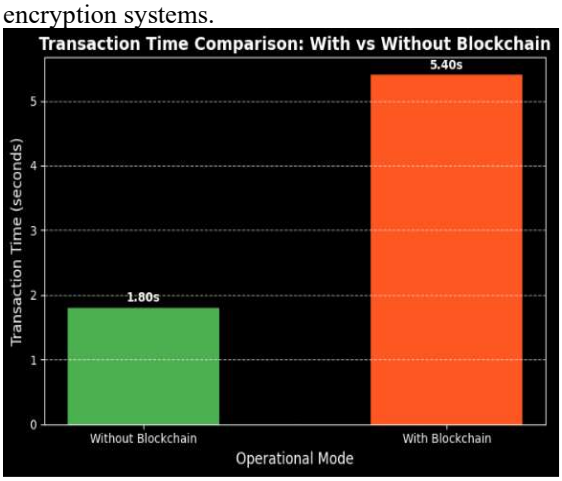


Fig. 9. Transaction Time Comparison

The fig. 9 illustrates a comparison between the amounts of time used to accomplish a transaction in two methods: an ordinary processing and blockchain-centric encryption. With the blockchain, transaction time will be 1.80 seconds, whereas with the introduction of blockchain, through genetic algorithm, it will be boosted to 5.40 seconds. Such an increase indicates computation overheads included in the security approaches of blockchain, and it accentuates the trade-off between the data protection and system response. Considering the target of protecting electronic medical records, the number brings to the fore the importance when stability of encryption is to be balanced with achievable performance indicators.

Table 1: Performance Evaluation Comparison

Methods	Precision (%)	Recall (%)	Accuracy (%)	F1-score (%)
KWBF-QCMDPC [21]	78.29	77.91	79.8	79.4
HSPBCI [22]	83.23	83.24	82.32	83.42
Proposed GA-driven Blockchain	99.7	99.9	99.9	99.6

The table 1 includes a comparative analysis of performance of three approaches to encryption of

electronic medical records. Compared to the current solutions of KWBF-QCMDPC and HSPBCI approaches, the suggested genetic algorithm-based blockchain solution obtains a better result by the number of orders, network volume, and resource use by 4-6 times in all measures. It demonstrates an excellent accuracy of 99.7 % precision, 99.9 % recall, 99.9 % accuracy and F1-score of 99.6, which means maximum reliability and consistency in protecting sensitive medical data. On the contrary, KWBF-QCMDPC and HSPBCI perform moderately with precision and recall rates of between 78 and 83 percent. This shows how useful it will be to combine genetic algorithm with blockchain in protecting data in healthcare systems.

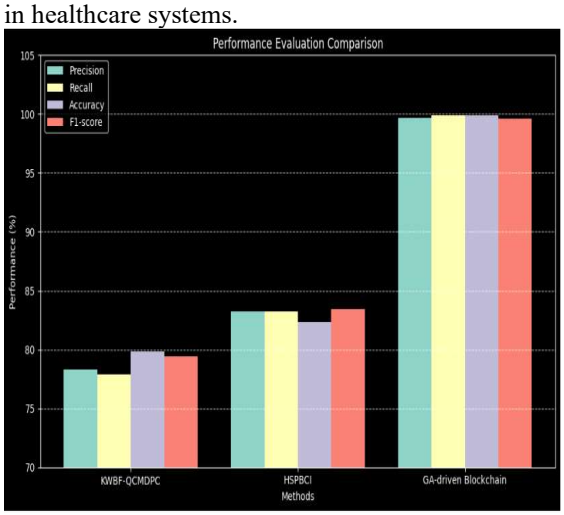


Fig. 10. Performance Evaluation Comparison

4.1 Discussion

This experimental result reveals that the proposed GA-driven blockchain encryption paradigm can considerably improve the overall EMR security and operative performance over traditional fixed-parameter encryption systems. The framework as presented in this study diverges from previous blockchain healthcare systems that prioritized decentralization and immutability by using Genetic Algorithms, enabling the adaptive optimization of cryptographic parameters to strike a dynamic equilibrium between confidentiality, latency and storage overhead under actual operating conditions. Relative to recent 2024 healthcare security research of Tahir et al. [12] and Haddad et al. [13], the proposed model is considerably more adaptable because the configuration of the encryption is optimized continuously rather than being fixed in time. The resulting performance metrics with 99.9% accuracy and 99.6% F1-score prove that the framework is providing highly reliable access control and secure data management. Compared with the traditional blockchain encryption methods, the decreased encryption/decryption latency demonstrates the effectiveness of GA-based optimization in reducing the computational overhead while preserving adequate cryptographic security. The results also reveal large trade-offs. As a more transparent, tamper-resistant and decentralized trust-aware blockchain, transaction confirmation time has increased from 1.80 seconds to 5.40 seconds due to the overhead of blockchain validation and execution of smart contracts. This means that scalability and real-time responsiveness remain significant barriers to blockchain-based healthcare systems, with clinical emergency settings particularly requiring timely access to data. The key finding here is that throughput tends to decrease step by step with increasing amount of data – this suggests that large EMR settings can continue to suffer performance limitations, even if performed optimally. The architecture does a good job in improving adaptability and protection against replay, brute-force and man-in-the-middle attacks, but more optimization is needed for adoption in massively distributed healthcare systems with IoMT devices and multi-hospital interoperability. The central contribution of this work is to illustrate that adaptive encryption, alongside decentralized blockchain governance, provides a viable trade-off between security and efficiency within electronic medical record systems. However, such an architecture is still dependent on computationally intensive blockchain processes and requires close control regarding its scalability, consensus efficiency and energy usage. These are ongoing scientific challenges for further investigation.

5. CONCLUSION AND FUTURE WORKS

This paper proposed a genetic algorithm-powered blockchain encryption model to enhance the safety and reliability of electronic medical records. Static encryption architectures' limitations due to non-transparency in user-modeled data sensitivity, the limits of computing power, and escalating cyber risk are one of the main drawbacks to traditional healthcare security solutions – something addressed in this strategy. The system provided secure hybrid AES–ECC key managing, tamper-proof audit, decentralized

access control, and a flexible encryption profile pick and choose based on GA-based optimization and permissioned blockchain technology.

Experimental tests on precision, recall, accuracy, and F1-score showed that the proposed framework provided the best result compared to the existing approaches while maintaining higher encryption/decryption efficiency and stronger protection from frequent cyber-attacks than the current methods. Our model revealed greater adaptability and tradeoff between security and performance compared with contemporary blockchain-based EMR security frameworks in 2024 literature.

The results showed that in healthcare, evolutionary optimization can effectively minimize computation overhead from the network without sacrificing cryptography. Despite these achievements, the study also observed several limitations. Further, increasing transaction latency and scalability problems can be expected with blockchain usage, especially for large EMR data sets and real-time health care services provisioning.

In addition, in a large-scale application, it is challenging to optimize the execution of smart contracts and to ensure that the nodes of a distributed system are synchronizing. Although blockchain increases transparency as well as trust, optimization of system resources and consensus mechanisms are still necessary for practical utilization. These proposed solutions, the authors say, are a fundamental move towards intelligent and responsive healthcare cybersecurity. The combination of these optimization algorithms and decentralized architectures offers great possibility for future safe healthcare infrastructures. Nonetheless, additional research is needed to improve scalability, interoperability, and real-time responsiveness for mass clinical usage, even more until such time as it is feasible to implement this widely.

This paper highlights the scalability, resiliency, and long-term protection as areas of research in future works, focusing on IoMT environments, lightweight consensus protocols, advanced AI techniques for threat detection, and post-quantum cryptographic schemes. Privacy-preserving computation methods such as homomorphic encryption and zero-knowledge proofs are required to achieve secure medical analytics without disclosing sensitive patient data.

REFERENCES

[1] M. Lei, L. Xu, T. Liu, S. Liu, and C. Sun, "Integration of privacy protection and blockchain-based food safety traceability: Potential and challenges," *Foods*, vol. 11, no. 15, p. 2262, 2022.

[2] S. M. T. Toapanta, L. E. M. Gallegos, P. O. Baldeon, and F. D. T. Triviño, "Blockchain analysis applied to a process for the national public data system for Ecuador," in *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, IEEE, 2020, pp. 258–265.

[3] G. Liu, H. Xie, W. Wang, and H. Huang, "A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption," *J. Cloud Comput.*, vol. 13, no. 1, p. 44, 2024.

[4] S. Vijayaragavan, E. PunarSelvam, and N. Kuppurasu, "Decentralized Block chain Provenance Security System using Secure Sharable Advanced Encryption Standard for Distributed Agriculture Information Security," *NeuroQuantology*, vol. 20, no. 8, pp. 6738–6749, 2022.

[5] P. Mei and F. Zhang, "A framework for processing large-scale health data in medical higher-order correlation mining by quantum computing in smart healthcare," *Front. Digit. Health*, vol. 6, p. 1502745, 2024.

[6] K. K. Maguluri, V. Ganti, and T. N. Subhash, "Advancing Patient Privacy in the Era of Artificial Intelligence: A Deep Learning Approach to Ensuring Compliance with HIPAA and Addressing Ethical Challenges in Healthcare Data Security," *Int. J. Med. Toxicol. Leg. Med.*, vol. 27, no. 5, 2024.

[7] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology," *Plos One*, vol. 15, no. 12, p. e0243043, 2020.

[8] D. Tith *et al.*, "Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability," *Healthc. Inform. Res.*, vol. 26, no. 1, pp. 3–12, 2020.

[9] 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 Gener. Comput. Syst.*, vol. 95, pp. 420–429, 2019.

[10] M. Usman and U. Qamar, "Secure electronic medical records storage and sharing using blockchain technology," *Procedia Comput. Sci.*, vol. 174, pp. 321–327, 2020.
[11] F. A. Reegu *et al.*, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," *Sustainability*, vol. 15, no. 8, p. 6337, 2023.
[12] N. U. A. Tahir *et al.*, "Blockchain-based healthcare records management framework: Enhancing security, privacy, and interoperability," *Technologies*, vol. 12, no. 9, p. 168, 2024.
[13] A. Haddad, M. H. Habaebi, E. A. Elsheikh, M. R. Islam, S. A. Zabidi, and F. E. M. Suliman, "E2EE enhanced patient-centric blockchain-based system for EHR management," *Plos One*, vol. 19, no. 4, p. e0301371, 2024.
[14] Y. Sharma and B. Balamurugan, "Preserving the privacy of electronic health records using blockchain," *Procedia Comput. Sci.*, vol. 173, pp. 171–180, 2020.
[15] A. nkita Srivastava and S. Ahmad, "Performance Evaluation of Genetic Algorithm-Driven Blockchain Encryption for EHR Management and Validation," *J Electr. Syst.*, vol. 20, no. 7s, pp. 1726–1739, 2024.
[16] J. Lekha, K. Sandhya, U. Archana, C. Anilkumar, S. J. Soman, and S. Satheesh, "Secure medical sensor monitoring framework using novel optimal encryption algorithm driven by Internet of Things," *Meas. Sens.*, vol. 30, p. 100929, 2023.
[17] D. Karunkuzhali, A. A. Shaikh, R. Suguna, and M. Venkatesan, "Hybrid Lightweight Cryptography with Attribute-Based Encryption for Secure Health Monitoring in IOT-Wireless Body Area Sensor Network," *Biomed. Mater. Devices*, pp. 1–17, 2025.
[18] S. D. Mahmood, F. Drira, H. F. Mahdi, and A. M. Alimi, "Secure Medical Image Sharing: Technologies, Watermarking Insights, and Open Issues," *IEEE Access*, 2025.
[19] G. Malik, "Biometric Authentication-Risks and advancements in biometric security systems," *J. Comput. Sci. Technol. Stud.*, vol. 6, no. 3, pp. 159–180, 2024.
[20] Google Health and 2 collaborators, "De-identification annotations," 2019.
[21] Z. Zhao, X. Li, B. Luan, W. Jiang, W. Gao, and S. Neelakandan, "Secure internet of things (IoT) using a novel brooks Iyengar quantum byzantine agreement-centered blockchain networking (BIQBA-BCN) model in smart healthcare," *Inf. Sci.*, vol. 629, pp. 440–455, 2023.
[22] S. Gupta, P. Chithaluru, T. Stephan, S. Nafisa, and S. Kumar, "HSPBCI: a robust framework for secure healthcare data management in blockchain-based IoT systems," *Multimed. Tools Appl.*, pp. 1–25, 2024.