Hindawi
International Journal of Intelligent Systems
Volume 2024, Article ID 6995202, 16 pages
https://doi.org/10.1155/2024/6995202

Research Article

An Efficient Secure Sharing of Electronic Health Records Using IoT-Based Hyperledger Blockchain

Velmurugan S.[1], **Prakash M.**[2], **Neelakandan S.**[3] **and Eric Ofori Martinson**[4]

[1]*Department of Information Technology, R.M.D. Engineering College, Kavaraipettai, India*
[2]*School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India*
[3]*Department of Computer Science and Engineering, RMK Engineering College, Chennai, India*
[4]*Department of Electronics and Communication Engineering, All Nations University, Koforidua, Ghana*

Correspondence should be addressed to Eric Ofori Martinson; emartinson@anuc.edu.gh

Received 23 September 2023; Revised 27 December 2023; Accepted 11 March 2024; Published 22 March 2024

Academic Editor: Said El Kafhali

Electronic Health Record (EHR) systems are a valuable and effective tool for exchanging medical information about patients between hospitals and other significant healthcare sector stakeholders in order to improve patient diagnosis and treatment around the world. Nevertheless, the majority of the hospital infrastructures that are now in place lack the proper security, trusted access control, and management of privacy and confidentiality concerns that the current EHR systems are supposed to provide. *Goal*. For various EHR systems, this research proposes a Blockchain-enabled Hyperledger Fabric Architecture as a solution to this delicate issue. The three steps of the suggested system are the secure upload phase, the secure download phase, and authentication. Patient registration, login, and verification make up the authentication step. The administrator grants authorization to read, edit, delete, or revoke the files following user details verification. In the secure upload phase, feature extraction is carried out first, and then a hashed access policy is created from the extracted feature. Next, the hash value is stored in an IoT-based Hyperledger blockchain. The uploaded EHR files are additionally encrypted before being stored on the cloud server. In the secure download step, the physician uses a hashed access policy to send the request to the cloud and decrypts the corresponding files. The experimental findings demonstrate that the system outperformed cutting-edge techniques. The proposed Modified Key Policy Attribute-Based Encryption performs better for the remaining 10 to 25 mb file sizes. This IoT framework compares MKP-ABE with certain efficiency indicators, such as encryption, decryption period, protection level analysis and encrypted memory use, resource use on decryption, upload time, and transfer time, which are present in the KP-ABE, the ECC, RSA, and AES. Here, the IoT device suggested requires 4008 ms for data encryption and 4138 ms for the data decryption.

1. Introduction

The basis of a happier life is good health. The subject of social interest was still on public health issues [1]. Current healthcare services are technologically complicated and expensive. But effective health record keeping, the usage of insurance providers, and technology blockchain can mitigate this [2]. This is also probable. Blockchain [3] is an unchangeable data base technology with an ever-growing list of papers, distributed and encrypted [4]. It is also a joint pooled data collection technology that will decentralise data storage to enhance patient results by improving data access activities and data protection simultaneously [5]. Consumer details should not be misused, and patients do not have power of the identities of robberies, financial data violations, or spam. This is the solution to these problems by the hyperleader fabric. Transactions involving the health records of a patient are registered with certain special IDs in the ledger [6].

Electronic Health Record (EHR) systems have significantly transformed the way in which patient health information is managed and made accessible, constituting a critical milestone in healthcare technology. These systems perform the digitization and consolidation of extensive patient data, encompassing not only medications and treatment plans but also medical histories and diagnoses.

Electronic health records (EHRs) optimize healthcare processes by facilitating workflows, boosting provider-to-provider communication, and augmenting patient care via timely access to vital data. They enable patients to access their health records more conveniently, promote data-driven decision-making to deliver personalized healthcare, and facilitate the secure exchange of information. There are multiple classifications of electronic health record (EHR) systems. These include hybrid EHRs, which integrate features of both on-premise and cloud-based solutions, on-premise systems that are deployed locally within healthcare facilities, and cloud-based EHRs that operate on remote servers accessed via the Internet. Every category presents unique benefits with regard to usability, expansion, protection, and tailoring, accommodating the varied requirements of healthcare providers. The ongoing advancement in healthcare is really helpful. By eliminating mistakes in data, they have increased the quality and clarity of health information [7].

In addition, EHRs may be useful for obtaining clinical records at any time and everywhere, thus minimising the potential of repeating checks, diminishing gaps in care, and informing patients in improved decision-making [8]. Each patient care centre has its own EHR administration system, making it hard to communicate health records across medical channels. Medical histories are untraceable. EHRs can now be shared across numerous platforms, thanks to blockchain technology [9]. EHR management using Hyperledger Fabric, we can build a permissioned peer-to-peer blockchain network with a large number of well-known and registered healthcare businesses. However, certain difficulties must be taken into consideration in the application of EHRs. Managing the EHR system through a secure and efficient architecture built on Hyperledger Fabric. In order to maximise interoperability, security, privacy, scalability, and permissioning, this allows us to create a peer-to-peer, private, permissioned blockchain network with several registered and identifiable healthcare stakeholders. Certain problems concerning two factors: privacy and security [10] risk the secrecy, credibility, and availability of user details, fake injection [11], Sybil Attack vulnerability [12], and a single failure point because of centralised control [13]. Drawbacks of EHR are as health data are shared electronically, patient privacy concerns are growing. To ease these concerns, policymakers have protected patient data. The Health Insurance Portability and Accountability Act's privacy and security regulations have been reinforced by recent legislation that requires the interchange of electronic health information. EHRs may increase medical errors, bad emotions, power shifts, and technology dependence. 40 CPOE has been linked to medical errors due to poor system interfaces or a lack of end-user training. Other income decreases may result from EHR implementation. Because EHRs reduce redundancies, errors, and durations of stay, a provider may be able to avoid chargeable transactions that would have resulted in third-party payer reimbursements, especially if the payment system is fee-for-service. Each organization's reimbursement rates may fall, while EHR system efficiencies may increase revenue.

Because Hyperledger Blockchain technology combines two cutting-edge concepts, its integration with the Internet of Things offers a powerful answer. The convergence of the Internet of Things (IoT) and Hyperledger Blockchain results in an unprecedented synergy that presents a novel framework for the administration of data in a secure, transparent, and efficient manner. This convergence facilitates the development of decentralized ledgers that are tamper-proof and distributed, guaranteeing the integrity, authenticity, and immutability of data generated by the Internet of Things. The revolutionary impact of the seamless incorporation of IoT devices with Hyperledger Blockchain extends to various sectors, including supply chain management, healthcare, finance, and more, by enhancing traceability, enabling real-time data sharing, and facilitating automated transactions devoid of trust. This integration serves as a resilient resolution, enhancing the possibility of interconnected, scalable, and secure systems that revolutionize contemporary technological implementations [14].

Using lightweight cryptographic features like elliptical curve encryption, Rivest–Shamir–Adelman (RSA), and others, the majority of modern approaches use key exchange between the parties involved. The coded data will be jeopardised if a hostile party obtains the key [15]. Based on elliptic curve theory, elliptic curve cryptography (ECC) can provide cryptographic keys that are more efficient, quicker, and smaller than those used by current methods. It is used in elliptic curve cryptography (ECC). Elliptic Curve Cryptography is comparable to Rivest–Shamir–Adleman (RSA) (ECC). It creates digital signatures for digital currencies like Bitcoin and Ethereum and one-way encrypts emails, data, and software, as well as RSA and ECC. Some programmes provide an access control mechanism with an attribute-based encryption scheme. In this situation, the attribute-bases cryptography induces the increasing operation period in line with the number of users who are unrevoked and is unable to deter internal attacks, and blockchain's irreversibility is an obstacle to the revocation of consent [16].

The motivation for this innovation originates from the urgent requirement to tackle persistent issues in healthcare systems: the secure transmission of confidential patient data between disparate entities, while simultaneously guaranteeing the availability, integrity, and confidentiality of the information. Through the integration of Internet of Things (IoT) devices with Hyperledger Blockchain, this proposed solution aims to address these deficiencies by creating a resilient infrastructure that enhances the security of health records and enables the seamless integration of real-time data, thereby fostering a holistic perspective of patient well-being. The main goal is to equip healthcare providers with secure and efficient tools that enable them to seamlessly share critical patient data. This will ultimately lead to improved decision-making processes, increased collaboration

among stakeholders, and an overall enhancement in the quality and efficiency of healthcare delivery. The following is a discussion of this paper's main goals and contributions:

(i) We introduce a decentralized system for access control and authentication intended for BC-based EHS. Medical service providers can produce paired secret keys during the key management step in order to implement secure communication. After negotiating with one another, users and medical healthcare providers can create session keys during the authentication and access control phase.

(ii) Encrypts sensitive health records to prevent unwanted access and maintain data integrity by using Hyperledger Blockchain technology and strong encryption standards.

(iii) The security of the proposed protocol's mutual authentication and session key exchange is examined through a formal security analysis that employs Burrows–Abadi–Needham (BAN) logic. The communications that are exchanged specify the security objectives. A nonformal security evaluation of the protocol is additionally offered to assess its resilience against certain established assaults.

(iv) Facilitates accurate and secure data transmission across various healthcare systems, allowing for the safe transfer of electronic health records (EHRs) between medical professionals without compromising patient privacy.

(v) Improves the quality and efficiency of healthcare services by streamlining administrative tasks and minimising the likelihood of mistakes.

The majority of the paper is structured as follows. Several associated works and context material on blockchain technologies in a cloud setting were provided in Section 2 utilising the Hyperledger and electronic health record framework. Section 3 explains the stable distribution of EHR by the Hyperledger blockchain is used in the proposed approach. Section 4 displays the performance of the model as well as the disputes. To end, Section 5 displays the nm.

2. Related Work

Wang and Song [17] using blockchain technology and attribute-based cryptosystems, a secure electronic health record (EHR) system was constructed. The scheme has embraced a contemporary primitive form of cryptography known as the hybrid attribute-based/identity-based encryption and signature (C-AB/IB-ES) in order to carry out the many duties connected with ABE, IBE, and IBS while operating within a particular cryptographic system. According to the research' findings, the system is able to perform at levels that are acceptable. However, there is a potential that the system will result in a variety of significant problems, including complete confidentiality, difficult computation, and high storage costs.

Dagher et al. [18] recommended a blockchain-based system for patient, vendor, and third-party reliable, interoperable, and productive access to medical data, while ensuring the protection of personal details for patients. In an Ethereum-based blockchain, the framework was called Ancile and used smart contracts to enhance access protection and data obstruction and sophisticated encryption methods for increased defence. The method specifically explores how Ancile deals with the diverse interests of patients, clinicians, and third parties and how the process will solve a long-standing challenge in healthcare privacy and protection. However, the blockchain technology did not meet the legislative standards for medical data, and it provided less security.

Mubarakali [19] proposed that a Blockchain- (SRHB-) based on a safe and stable healthcare-based cryptography be used to securely transfer the EHR. The machine obtained data from the patient in a standardised healthcare system focused on the wearable technology. In a cloud computing server, the patient received data were uploaded and processed. In order to administer medications and measures for fast healing, the doctor checked the patient's health examination, genetic details, and observational study. Blockchain principle applied in health data to protect secrecy. A separate block as a chain was generated every time. The device took some time to exchange health data and to access health records in the database server storage.

Bayat and Farjami [15] implemented a stable and powerful framework focused on blockchain-based technologies and encoding-based attributes named "MedSBA," for the recording and store of healthcare data and for the security and privacy of the system (GDPR). The MedSBA used private blockchains to boost the ability and it is a problem with attribute-based encryption, to revoke rapid access. The device was seen to be secure and functional on the basis of the Burrows–Abadi–Needham (BAN) logic, and storage showed the reliability of the system. However, the device does not trade the cryptocurrency for data users and individuals for the sharing of medical data.

Cao et al. [20] a hybrid blockchain-based medical record exchange system was demonstrated. A consortium-approved medical information control system may extract data for correct diagnosis. A work prototype was introduced to illustrate how the hybrid blockchain enables pharmacy practises in an environment for the management of health knowledge. A Hyperledger Calliper blockchain benchmarking method was used to test the achievement of a hybrid electronic medical record exchange device for efficiency and average latency that was feasible and outstanding. The framework did not, however, illustrate the exact extent of protection of the system.

Xia et al. [21] provided data exchange in cloud environments on the basis of blockchain for electronic medical records. The scheme was built on a blockchain permit that only invited and thus authenticated users could use. Responsibility was assured because the blockchain was already known to all developers and held a record of their behaviour. After authentication of their identity and cryptographic keys, the framework supports requests for public pool data. The framework was discovered to be light and adaptable throughout the system analysis. The findings also indicate

that relative to the current methodologies the framework worked higher. The device, however, produced less efficiency.

According to Laghari et al. [22], the goal of this study is to analyse the gaps that exist between connected IoV devices during network communication and to highlight current security and privacy strategies and protocols. In this work, we provide a Hyperledger sawtooth-enabled IoV architecture with lightweight-BIoV capabilities to decrease blockchain DLT resource adaptability and enhance system acceptability. Without abandoning the Hyperledger sawtooth, this lightweight-BIoV demonstrates how the architecture and design are resource-efficient while preserving effective information traceability and reliability. However, in order to investigate the validation and verification of car node transactions while utilising fewer computing resources, we create, develop, and implement smart contracts in addition to a number of PoW consensus techniques. In this study, [23] focuses on blockchain technology, its characteristics, and the fundamental technologies that form the foundation of the blockchain network. The history of blockchain is narrated in chapters that flow gradually from cryptocurrencies to blockchain technology platforms and applications that are widely used in the financial and industrial sectors worldwide because of their greater security, transparency, and ease of use focuses on using blockchain technology as a data repository and in the Internet of Things.

Khan et al. [24] use distributed ledger blockchain technology (BHIIoT) to provide a novel and secure architecture for the protection of E-healthcare data. Second, the lifespan of medical wireless sensor networks is modified for data management and optimization through the use of a distributed layered hierarchy. As a result, network resources are enhanced, and trust in the peer-to-peer (P2P) setting made possible by blockchain technology is increased. Third, the proposed BHIIoT encrypts data using the NuCypher threshold re-encryption method to protect shared resources, which are blocks stored in an immutable blockchain storage system. For instance, chain codes are used in distributed e-healthcare applications to automate transaction tracing, index data distribution, logging, and authentication in order to stop illegal conduct. In [25], the quality issues that is currently present with blockchain technology implementation. Additionally, it specifies terminologies related to smart contracts in industries, public, private, hybrid, and consortia blockchains, as well as the properties that are necessary, including autonomy, transparency, immutability, data integrity, and security.

A blockchain-based decentralized authentication and access control protocol for EHS is described by Xiang et al. [26]. By addressing the more important privacy and security issues related to medical data, this protocol makes it possible for consumers and medical service providers to collaborate effectively and safely share resources. To enhance the negotiation process, a multiweighted subjective logic-based practical Byzantine fault-tolerant (PBFT) negotiation mechanism is used. Ultimately, we show that our solution is resilient to known security threats by employing BAN logic to establish the dependability of the systems-security safeguards. The authors in [27] suggest a blockchain consortium with preselected users. Here, public key encryption with keyword search (PEKS) technology is utilized to ensure data security, access management, privacy preservation, and secure search. The security proof indicates that there is no discernible difference between our suggested strategy and the keyword guessing attack. The suggested scheme outperforms other relevant schemes, according to the results of the comparative simulations and performance analysis.

Shamshad et al. [28] propose a novel blockchain-based EHR sharing system that preserves privacy and security and enables better diagnosis and effective treatment in TMIS. First, the consensus, data structures, and procedures of two different types of blockchains the consortium blockchain and the private blockchain are developed. While consortium blockchain keeps the safe indexes of EHRs, private blockchain manages EHR maintenance. Our protocol's security study confirms that it meets all security objectives by avoiding a number of security threats. The authors in [29] suggest an IoT authenticated group key agreement system based on blockchain technology. In the proposed protocol, a new entity known as the device manager is introduced. This entity serves as a bridge to connect blockchain networks and Internet of Things devices. Security research shows how resistant the suggested protocol is to different types of assaults.

Singh and Das [30] in order to increase access control over medical data, a lightweight two factor authentication approach (TFAS) that incorporates user authorization, device, user, and data authentication is recommended. This two-stage authentication verification process begins with human and device authentication utilising PUF and fuzzy extractor; the second stage employs user authorization and data authentication based on blockchain. In addition to ensuring the scalability and expansion of the blockchain-based IoMT network, it uses a cluster of servers that are interplanetary file systems enabled by smart contracts.

Table 1 provides a summary of healthcare data management mechanisms in blockchain technology.

3. Proposed Methodology

In terms of revenue and data, healthcare is the industry with the biggest boom. Security is the need of the hour for too many electronic health reports. There was a need to use blockchain technologies to make this sensitive information more secure. Because of its specific distributed deceptive and privacy-proof characteristics, it becomes famous. However, owing to the authentication challenges of the IoT Based blockchain framework, eHealth programmes use blockchain technologies face certain security threats. Worse, medical institutions have computerised health records, which creates privacy concerns. Bitcoin's blockchain technology is indestructible because it is decentralized, encrypted, faith-based, and maintained through mutual collaboration. It is characterised by data exchangeability and data integrity. The effective, safe, modified policy attribute-based encryption (MKP-ABE) is implemented in this paper to ensure secure and secure sharing of electronic health records through blockchain hyperleader. Figure 1 displays the model system of the proposed architecture.

Table 1: A comparison of blockchain technology's medical record management for the healthcare industry.

References	Blockchain technology	Merits	Demerits	Type of medical data
Castaldo and Cinque [31]	Private blockchain (proof-of ownership)	Secure sharing of information for healthcare and enhanced auditing procedures	The cross-border interchange of e-health data are restricted to Europe	EHR
Yue et al. [32]	Private blockchain	Blockchain-based artificial intelligence system for healthcare data sharing privacy control	The suggested method was not scalable, and there was no guarantee that the data would be available (sharing of E-health data is limited)	EHR and PHR
Patel [33]	Proof-of-Stake	Decentralized and secure medical imaging data sharing	Interoperability and privacy concerns are not taken into account by the suggested solution	Medical image records
Hussain et al. [34]	Hash enabled blockchain platform	Sharing of medical records for administrative, clinical, and scientific reasons	Confidentiality and access control are ignored	EHR
Genestier et al. [35]	Hyperledger platform	Consent management is used in electronic health systems to manage and share personal data	There is no access control and no thorough permission procedure at all	EMR
Omar et al. [36]	Consortium blockchain	Sharing medical records with strong security via paired encryption and signatures	The suggested remedy lacks complete automation and functionality	Medical records
Babu et al. [37]	Health records' security	Improved healthcare applications' scalability, flexibility, security, and accessibility	Blockchain-based security solutions have greater costs and need to comply with regulations	Hyperledger fabric
Tiwari et al. [38]	Secure issue of IoT-based health monitoring system	Transactional data availability, security, integrity, and storage concerns	Performance measurements are not used to evaluate the suggested method	Hyperledger fabric
Pelekoudas-Oikonomou et al. [39]	Examines the edge learning and IMoT devices	Numerous aspects, including face mask recognition, fever detection, and patient cough sound analysis at home, were examined	The suggested solution's accuracy in using actual subjects is not tested	Hyperledger Fabric and Ethereum

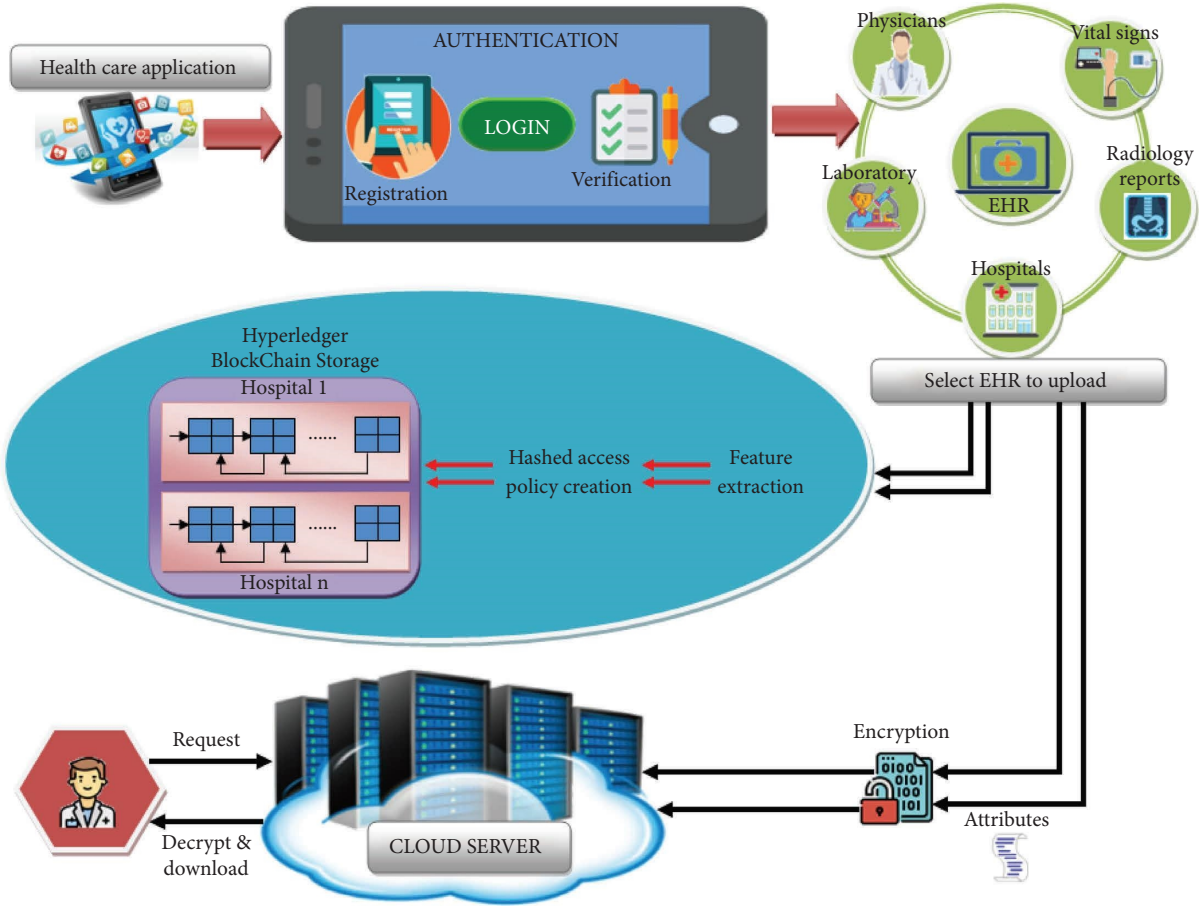

Figure 1: The architecture of the system model.

3.1. Authentication Phase. The first phase of the proposed secure sharing of EHR using blockchain technology is authentication. Authentication is the process of verification or testing to make sure that the user is who he claims to be. It is an important step in providing access to authorized patients. This phase mainly consists of three steps, registration, namely, login and verification.

3.1.1. Patient Registration. Throughout the initial stage of the patient registration procedure, the user is responsible for entering the patient's information. The health assistant is in charge of inputting the patient's information into the database, which includes the patient's name, age, username, gender, password, address, hospital ID, patient ID and doctor name, among other things. These particulars will be saved in the database. The patient details are mathematically represented as follows:

$$\vec{A}_{r(p)} = \{\vec{a}_1, \vec{a}_2, \vec{a}_3, \ldots\ldots\ldots\ldots\ldots\ldots \vec{a}_n\}, \quad (1)$$

where $\vec{A}_{r(p)}$ signifies the patient details set and a_n indicates the n information about the patients, such as age, sex, name, and patient ID.

3.1.2. Optimized Key Generation. After filling in the patient details, in this step, the optimized key generation process is done. The randomly generated key value is less secured for the data encryption and decryption process. So, the keys are generated optimally to provide highly secure during the encryption and decryption process. Getting the modified salp swarm optimization (MSSO) algorithm, the main values are optimally chosen here. The Modified Salp Swarm Optimization (MSSO) algorithm is an improved iteration of the Salp Swarm Optimization (SSO) algorithm that draws inspiration from the swarming characteristics observed in marine salps. In order to tackle optimization problems, this metaheuristic algorithm is based on the imitation of the collective behaviour of these organisms. MSSO implements alterations and enhancements to the conventional SSO with the objective of bolstering the rate of convergence, capabilities for exploration, and capabilities for exploitation. A notable improvement entails the integration of adaptive strategies or hybridization with alternative algorithms to strengthen its capability to address intricate and multidimensional optimization problems. MSSO generally entails the generation of a population of salp agents, in which each agent modifies its position in the search space iteratively in accordance with a predetermined set of rules. The regulations comprise motion protocols that emulate the swimming patterns of salps, as well as approaches for revising positions in light of regional and international data. The enhanced functionalities incorporated in MSSO are designed to rectify the deficiencies identified in the initial SSO, thereby

guaranteeing improved convergence towards optimal solutions in a wide range of problem domains, including finance, machine learning and logistics [40, 41].

MSSO has been successfully used in a large variety of optimization problems and is among the most effective metaheuristic optimization algorithms. However, there are still problems such as low convergence and lower performance. Salp swarm is an invertebrate that lives predominantly in the Southern Ocean and swings forward by absorbing water. They generally form a salp swarm chain in the deep water, which is divided into two parts: leaders and followers. Individuals at the top of the group chain are referred to as leaders, while the rest are referred to as followers. The group's purpose is for followers to move in unison under the supervision of leaders, constantly updating their locations and finding and developing better food sources in the search environment. The MSSO algorithm is used to increase convergence performance in global search and local search as well as to improve the quality of the main generation efficiency optimized. Below are step-by-step illustrations of the MSSO process. To pick an optimum key attribute, the following processes are used. Introduced in the computational model used to replicate the swarming action of MSSO:

Step 1: First, initialize the salp population randomly, which is represented in the following equation:

$$(\mathrm{Bp})_k'' = \mathrm{Ran}(\ldots)\ \left(Cu_k - Cl_k\right) + Cl_k, \forall k \in \text{No.of.variables}, \tag{2}$$

where $(\mathrm{BP})_k''$ signifies the initial position of the salps, $\mathrm{Ran}(\ldots)$ indicates the random number between 0 and 1, Cu_k and Cl_k signify the upper limit and lower limit of the k^{th} dimension, respectively.

Step 2: Next, change the head salp location according to the gap between the salp and the source of food. To increase the search ability, the upgrade strategy for head salp is modified instead of the average as a weighted number of best positions.

$$(\mathrm{Hs})_k^1 = \begin{cases} Zw_1 * Da_k + e_1\left(\left(Cu_k - Cl_k\right)\ e_2 + Cl_k\right)\ e_3 \geq 0, \\ Zw_2 * Da_k - e_1\left(\left(Cu_k - Cl_k\right)\ e_2 + Cl_k\right)\ e_3 \geq 0, \end{cases} \tag{3}$$

where $(\mathrm{Hs})_k^1$ denotes the position of the leader, Zw_1 and Zw_2 indicate the weight values, Da_k indicates the position of the target food in the k^{th} dimensions, e_1, e_2, and e_3 signify the random coefficients between 0 and 1. The coefficient e_1 is the essential parameter because it provides a balance between exploration and exploitation capabilities. It is mathematically expressed as follows:

$$e_1 = 2\ e^{-(4f/F)}, \tag{4}$$

where F signifies the maximum iterations and f indicates the current iteration.

Step 3: Then, update the position of the follower using the following equation:

$$(\mathrm{Hs})_k^i = \frac{1}{2\ \left(Zw_1 + Zw_2\right)}\left(Zw_2 * (Hs)_k^i + Zw_1 * (Hs)_k^{i-1}\right), \tag{5}$$

$$Zw_1 = \widehat{G}_1 * \widehat{G}_2, Zw_2 = \widehat{G}_1 * \widehat{G}_3, \tag{6}$$

where $i \geq 2$, $(\mathrm{Hs})_k^i$ denotes the position of the i^{th} follower at the k^{th} dimension, and $\widehat{G}_1$, $\widehat{G}_2$, and $\widehat{G}_3$ represent the coefficient vectors. Based on this coefficient vector, the weight is calculated. This strategic update for weighted roles strikes a compromise between search engine discovery and extraction capacities. It also improves the pace of convergence, contributing to better SSO efficiency. Finally, evaluate the fitness of every salp that is maximizing the objective function. It is expressed as follows:

$$\mathrm{Opt}_{\mathrm{val}} = \arg\max\left(\sum_{k=0}^{i} (HS)_k\right). \tag{7}$$

The operation of the method ends only if the highest number of variations is completed and the optimal fitness benefit structure is selected as optimum. This will analyse the optimized meaning for the primary value. Based on the optimal prime value the method selects the public key (I_{Pub}) and private key (I_{Pri}). These keys are also used in extra dispensation. The pseudocode for the MSSO algorithm is presented in Algorithm 1.

3.1.3. Login. In order to be confirmed, the patient must provide the authentication information provided by the hospital administration when accessing the system. At the beginning of the login process, the patient must input both their login information and password. The ID for the

```
Set the salp population Hsi (i = 1, 2, ..., n) as Cu and Cl
While (end condition is not accomplished)
Compute the fitness of each search agent equation (7)
Da = the best search agent
Modify Zwi by equation (4)
  For every salp (HSi)
    If (I = 1)
      Modify the position of the leading salp
    Else
      Modify the position of the follower salp by equation (5)
    End
  End
  Amend the salps based on the upper and lower bounds of variables
End Return Da
```

Algorithm 1: Pseudocode of the MSSO algorithm.

hospital and the ID for the patient should then be given. The best version of the patient's private key must be provided as a last obligation ($I_{\Pr i}$).

3.1.4. Verification. The system will go on to the verification stage after the patient logs in, where it will check the patient's login, password, and private key against the database. The system will determine that the patient has already been registered with the cloud server associated with the hospital if all of the information including the Username, password, and key is determined to match. You will have to go through the registration process once more in such instance.

3.1.5. Admin Login Page. On the admin login screen, logged-in users can access their accounts by providing their username and password. The system can then be accessed by the admin. Furthermore, the administrator grants read/write access to the database to other practitioners or institutions. The admin module gives the following permission to the patient or other institutions such as view option, edit option, delete option, and update option. An example of these permissions could be given in the tabular form as in Table 2.

3.2. Secure Upload Phase. After successfully completing the authentication process, select which EHR files needs to be uploaded. All primary health administrative documentation for the treatment professional comprises the submitted EHR file, including records, progress notices, issues and prescriptions, essential symptoms, previous medical background, vaccines, laboratory results, and radiology studies. Also, it is file formats, including folders (.doc), graphic (.jpeg, .png), and excel (.xlsx). It has various file formats. These uploading data is mathematically expressed as follows:

$$\left(J_{ud}''\right)_b = \{j_1'', j_2'', j_3'', \ldots\ldots\ldots\ldots\ldots\ldots, j_n''\}, \quad (8)$$

where $(j_{ud}'')_b$ indicates the uploaded EHR file and j_n'' represents the n amount of information in the EHR files. After that, upload these files are securely to the blockchain storage and cloud server, the following steps are used.

Table 2: Accessibility of patient or other institutions.

Module name	View	Edit	Delete	Update
Module accessibility				
Patient details	☑	☑	☐	☑
Doctor details	☑	☑	☑	☑
Consulting details	☑	☑	☑	☑
Fix appointment	☑	☑	☑	☑
Pharmacy	☑	☐	☐	☑
Lab details	☑	☐	☐	☑

3.2.1. Feature Extraction. This is the first step of the secure upload phase. From the uploaded EHR file, some important features are extracted in this step. The extraction of features includes reducing the number of resources needed for a vast number of details. The name of the file, absolute path, file type, file size, parent folder and free space is secret, executable, accessible, readable, and main features are derived from EHR data $(j_{ud}'')_b$, as are available, hash code, time, time-recovery, and time. Mathematically, it is expressed as follows:

$$KF_l'' = \{kf_1'', kf_2'', kf_3'', \ldots\ldots\ldots\ldots\ldots\ldots, kf_n''\}, \quad (9)$$

where KF_l'' signifies the extracted feature set and kf_n'' indicates the n number of features extracted from the EHR file.

3.2.2. Hashed Access Policy Creation. After feature extraction, the hashed access policy for the extracted features will be developed using the Whirlpool Hash (WH) algorithm. Whirlpool iterates a compression mechanism based on a specialised 512 bit block cypher with a 512 bit key. Wide Trail guides the round function and key scheduling. The function structure, which is not platform-specific, benefits 8 bit and 64 bit Whirlpool implementations. Whirlpool employed a randomly generated substitution box (S-box), the internal structure of which made hardware implementation challenging. Any linear combination of input bits and the hash result cannot be securely connected, even the hash output itself. This is because the hash approach is

one-way. Whirlpool is immune to differential attacks because it is impossible to predict which bits of the hash output will change when input bits are altered. As a result, it is difficult for an attacker to decide which bits of the hash result to change. In this algorithm, the extracted features are converted into hash code. Based on this hash code, for future authentication, the access policy is being created [42–44]. The algorithmic procedures of the Whirlpool hash algorithm are explained below.

First, given an extracting feature set (KF_l'') as message consisting of a sequence of blocks $o_1, o_2, o_3, \cdots\cdots\cdots\cdots o_k$, the whirlpool hash function is described as follows:

$$\begin{aligned} W_0 &= \text{initialvalue},\\ W_{\text{itere}} &= E\left(W_{\text{iter}-1}, o_{\text{iter}}\right) \oplus W_{\text{iter}-1} \oplus o_{\text{iter}} = \text{center value},\\ W_k &= \text{hashcodevaluefortheextratedfeatures}, \end{aligned} \tag{10}$$

Each iteration's encryption key input displays the interim hash $W_{\text{iter}-1}$ value of the last iteration is the present message block o_{iter} and the plaintext. "The output for this iteration (W_{iter}) consists of the bitwise XOR of the current message block, the intermediate hash value from the previous iteration, and the output from the block cipher X." Figure 2 shows the process of hashcode created for the extracted feature.

Step 1: Append padding bits

The message is padded by appending a single "1" bit followed by the required number of "0" bits.

Step 2: Append length (L)

The message is attached with a block of 256 bits. This block is handled as a 256 bit integer (most relevant first byte) and consists of the first message bit duration (before the padding). The consequences of the first two steps produce a message containing 512 bits of integer. The extended message here is displayed as the 512 bit block series $o_1, o_2, o_3, \ldots\ldots\ldots\ldots o_k$, so increasing the total length of the enlarged message is $t \times 512$ bits.

Step 3: Initialize the hash matrix

The intermediate and final effects of the hash function are stored in a byte 8×8 matrix. The matrix is starting as a 0 bit matrix.

Step 4: Message processing

Messages are interpreted one block of 1024 bits at a time from structured input. The block cypher X is the core of this algorithm.

Step 5: Output

The final 512 bit Hash value of the extracted feature is determined after each block of 1024 bits has gone through the message processing stage (KF_l'') is obtained. The final hash value is denoted as W_k. Based on this final hash value, the access tree is constructed. The doctors or other institutions are able to decrypt if and only if the data attributes satisfy their access structure. This hashed access policy (Q_m) is considered as a secret key for further processing to improve the security level.

3.2.3. Hyperledger Blockchain Storage. The resulting Hash Code was subsequently entered in the Hyperledger Fabric blockchain in order to satisfy the credibility, availability and privacy criteria at each time of the transaction. Here, a single blockchain is generated for each hospital. During this function, the device consults multiple hospitals, which is Hyperledger blockchain. It requires data transaction blocks. An algorithm named minerals' work evidence for a stable, tamper-resistant agreement between any nodes in the network verifies and adds the blocks to the blockchain. Each block includes chronologic order hash of its preceding block, timestamp, nonce and preceding hash value. The platform's cryptographical hash algorithm ensures that connected blocks are immune and that blockchain data cannot be altered, although allowed users are still searching for such EHRs in the blockchain. The Hyperledger blockchain's organisational structure is depicted in Figure 3.

3.2.4. Encrypt EHR File Using MKP-ABE. In this phase, the uploaded EHR file $(j_{ud}'')_b$ is encrypted by using the Modified Key Policy Attribute-Based Encryption (MKP-ABE) algorithm and the encrypted file will be stored in a cloud server. Key Policy Attribute-based Encryption (KP-ABE) is a public key that supports fine-grained decryption access control. Only the ciphertext may be decrypted with attributes satisfying the control structure. To enhance the security level of the conventional KP-ABE, the proposed system uses a secret key (i.e., hashed access policy), so the term is called MKP-ABE. The MKP-ABE scheme consists of the following steps:

(a) Setup: This algorithm takes the security parameter ϖ and a universe description of attributes $(J_{\text{ud}}'')_b = \{j_1'', j_2'', j_3'', \cdots\cdots\cdots\cdots\cdots\cdots, j_n''\}$ as a starting point for the creation of a master secret key $\widetilde{I}_{msk}$ and some public parameter as P_{var}.

(b) Key Generation: In this key generation step, the system will take the optimized public and private key of the patient, which is already generated in the optimized key generation phase (Section 3.1.2).

(c) Encryption: This algorithm takes as input $(J_{\text{ud}}'')_b = \{j_1'', j_2'', j_3'', \cdots\cdots\cdots\cdots\cdots\cdots, j_n''\}$, public parameter ($\varpi$), hashed access policy (Q_m), and patient private key ($\widetilde{I}_{\text{pri}}$). It output the ciphertext**.** Mathematically, it is expressed as follows:

$$E\ \left(J_{ud}''\right)_b = \left(J_{ud}''\right)_b + \left(\varpi * I_{pri}''\right)\ *\ Q_m. \tag{11}$$

(d) Decryption: Finally (4), the decryption process is carried out; here, the authenticated user can retrieve the file from the cloud server. Given a ciphertext $E(J_{ud}'')_b$, patient public key ($\widetilde{I}_{\text{pub}}''$) and secret key

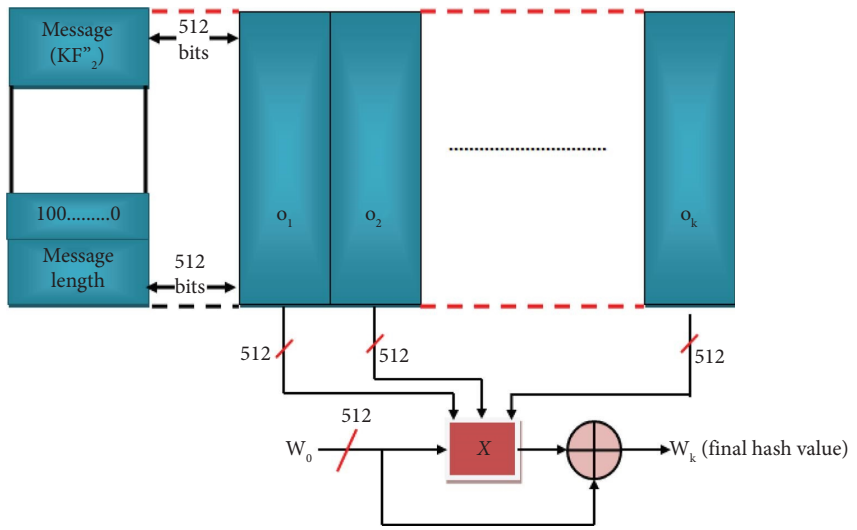

Figure 2: Whirlpool algorithm-based hash code creation for the extracted feature.

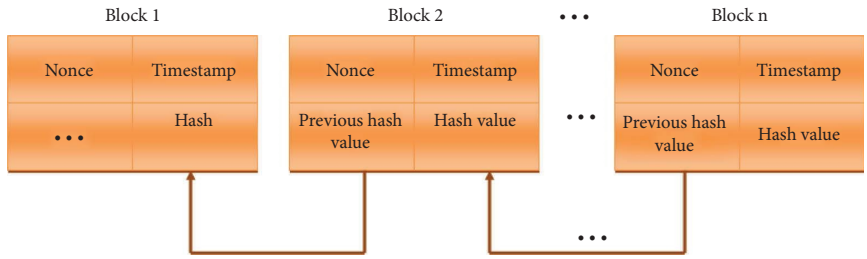

Figure 3: The Hyperledger blockchain storage structure.

(hashed access policy) Q_m, it produces the decrypted original file as follows:

$$\left(J_{ud}^{''}\right)_b = \frac{\left(E\ \left(J_{ud}^{''}\right)_b *\ I_{\text{pub}}^{''}\right)}{Q_m}, \tag{12}$$

where $\left(J_{ud}^{''}\right)_b$ denotes the original document. This way the data receiver retrieves the encrypted data from the cloud server. The receiver receives a document with a secure authentication scheme.

3.3. Secure Download Phase. This procedure enables hospital clinicians to safely retrieve patient data. If the doctor requests the file from the Cloud Server, the system will check the Hashed Access Policy before delivering it to the doctor. If the inquiring user has the correct Hashed Access Code, the system decides that they own the file containing the keys to decode the encrypted PHR file. This system allows the targeted user to decrypt the file using the decryption keys. The doctor can read, write, and cancel authorization. If the hasher access policy does not match, the system will refuse to download.

4. Results and Discussion

The effectiveness of the envisioned secure exchange of electronic health records utilising Hyperledger blockchain was evaluated using assessment techniques in this performance analysis section. In this part, examples from comparative research and recent test results are used to further illustrate the effectiveness of the suggested strategy. A software programme was used to build the proposed architecture (JAVA). The part that follows talks about the comparative analysis [45].

For our framework, Hyperledger (permissioned blockchain) is a better fit than Ethereum (permissionless blockchain) for the following two reasons: It can be difficult because of a permissionless blockchain, which allows anyone to join the network anonymously and without permission. Regarding an electronic medical record system, each member of the network must have their identity known. Hyperledger is a permissioned Blockchain network with identifiers for each participant; therefore, it makes sense to use it.

Patient medical data are susceptible to security breaches. Because everyone on the network participates in Ethereum's consensus process, material recorded on the distributed ledger that requires a higher level of anonymity can be accessed by all users. The privacy problems of patient medical data are addressed by Hyperledger's permissioned Blockchain, which only permits nodes approved by authorities to read such data [46].

The main issue that permissionless Blockchain networks like Ethereum are experiencing is privacy. When it comes to maintaining and operating the health system, it

Table 3: Experimental methodology for evaluating the Efficient Secure Sharing of EHR.

Aspect	Description	Rationale
Setup	Simulated or prototype environment that mimics real-world scenarios using IoT devices that provide EHR data	Mimics real-world deployment to assess practicality and functionality of the system
Metrics	Throughput and transaction speed: This metric measure the rates at which transactions are processed Scalability: The ability of a system to manage increasing data volumes. Security measures: Assesses the efficacy of security protocols Interoperability: The ease with which IoT devices communicate with one another Privacy Compliance: Ensures that regulations are followed	Throughput and transaction speed are critical for determining system efficiency Scalability is critical for accommodating expanding data volumes Security measures: Safeguards sensitive EHR data Interoperability is essential for efficient data exchange Privacy Compliance: Ensures that regulations are followed
Rationale	Metrics for analysing system efficiency, security, scalability, interoperability, and regulatory compliance	In healthcare contexts, comprehensive review assures the system's practicability, security, and regulatory compliance

Table 4: Demonstrate the performance of the proposed MKP-ABE with the existent methods in terms of encryption time and decryption time.

Metrics	File size (MB)	Proposed MKP-ABE	KP-ABE	ECC	RSA	AES
Encryption time	5	362	701	912	1242	1538
	10	1202	1552	1853	2112	2448
	15	2053	2428	2869	3228	3634
	20	2473	3004	3457	3871	4248
	25	4008	4569	4865	5364	5701
Decryption time	5	403	843	1107	1378	1689
	10	1325	1644	2027	2286	2612
	15	2101	2558	3016	3382	3776
	20	2624	3146	3588	4015	4411
	25	4138	4701	5025	5501	5976

makes sense to safeguard data from unauthorized individuals, protecting the system's overall privacy as depicted in Table 3.

4.1. Performance Analysis. Compared to the classical Key Policy Attribute-Dependent Encryption (KP-ABE), Elliptic Curve Cryptography (ECC), Rivest–Shamir–Adelman (RSA) and Advanced Encryption Standard (AES), the performance of the suggested MKP-ABE is presented in the performance analysis portion. The analysis can obtain the results by varying parameters like file size ranges from 10 to 50. The observations are seen with respect to the period of success encryption, decryption time, encryption memory use, decryption memory use, upload time, and download time. The following table verifies the relationship based on the encryption and decryption times.

Table 4 and Figure 4 depict the performance of the proposed MKP-ABE with the traditional KP-ABE, ECC, RSA, and AES algorithms. Encryption and decryption times were used in this comparison as performance metrics. Concerning the encryption time metric, for file size 5 mb, the existent AES method takes 1538 ms time to encrypt the data, which is higher than the recommended ones. Also, the existent KP-ABE, ECC, and RSA algorithms take the encryption time of 701 ms, 912 ms, and 1242 ms, respectively. The proposed MKP-ABE, on the other hand, encrypts files faster than current approaches. The proposed technique is similar to how it takes less time to encrypt data for a smaller file size (10 to 25). In terms of decryption time, the suggested MKP-ABE takes 4138 ms to decrypt data from a 25 mb file, but the existent KP-ABE, ECC, RSA, and AES take decryption time of 4701 ms, 5025 ms, 5501 ms, and 5976 ms time, respectively, which is higher when compared to the suggested one. For file size 5 mb to 20 mb, the proposed one takes less time to decrypt the data than the conventional methods. Thus, the discussion reveals that the suggested one attains better performance than the traditional techniques.

Figure 5 contrasts the proposed MKP-ABE with the conventional KP-ABE, ECC, RSA, and AES in terms of security level analysis. The conventional AES hence performs worse than the suggested one. Furthermore, the suggested method performs better than conventional KP-ABE, ECC, and RSA. For example, the proposed MKP-ABE provides 98.76% security, but the conventional KP-ABE, ECC, RSA, and AES provide security of 94.56%, 93.21%, 91.29%, and 89.98%. The discussion therefore shows that, in terms of high-level performance, the proposed system outperforms the baseline KP-BE, ECC, RSA, and AES.

Figure 6 shows, based on memory use during encryption and decryption, how well the suggested MKP-ABE performs in comparison to the current security methods, such as KP-ABE, ECC, RSA, and AES. The amount of RAM allocated for encryption and decryption is specified. A file size between 5 and 25 megabytes is required for the performance. Figure 6(a) demonstrates that the proposed MKP-ABE uses less memory for encryption than conventional methods (5133475 kb for a 5 mb file). While encrypting data, however, current encryption techniques like KP-ABE, ECC, RSA, and AES use far more RAM. Figure 6(b) analysis led to the conclusion that the proposed technique performed better than the alternatives. For example, for file size 5 mb, the proposed MKP-ABE takes memory usage of 5221775 kb, but the existent KP-ABE, ECC, RSA, and AES occupy the memory of 5532321 kb, 5833761 kb, 6222786 kb, and 6877865 kb, respectively. Similarly, all remaining 10 to 25 MB file sizes necessitate higher performance from the recommended MKP-ABE. This discussion preserves the anonymity of the access controls while requiring less computational cost than current alternatives.

Figure 7 depicts the performance of the proposed MKP-ABE algorithm in terms of two performance indicators, namely upload time and download time. The proposed one performs remarkably well, according to the study of the presented figure. The proposed approach, for instance, uploads files up to 5 mb in 9447 ms and downloads them in 8813 ms. The proposed one also requires 11221 milliseconds to upload and 10814 milliseconds to retrieve a 10 MB file. For remaining file sizes ranging from 15 MB to 25 MB, the suggested method necessitates quicker upload and download times. Thus, the discussion shows that the proposed method achieves better performance.

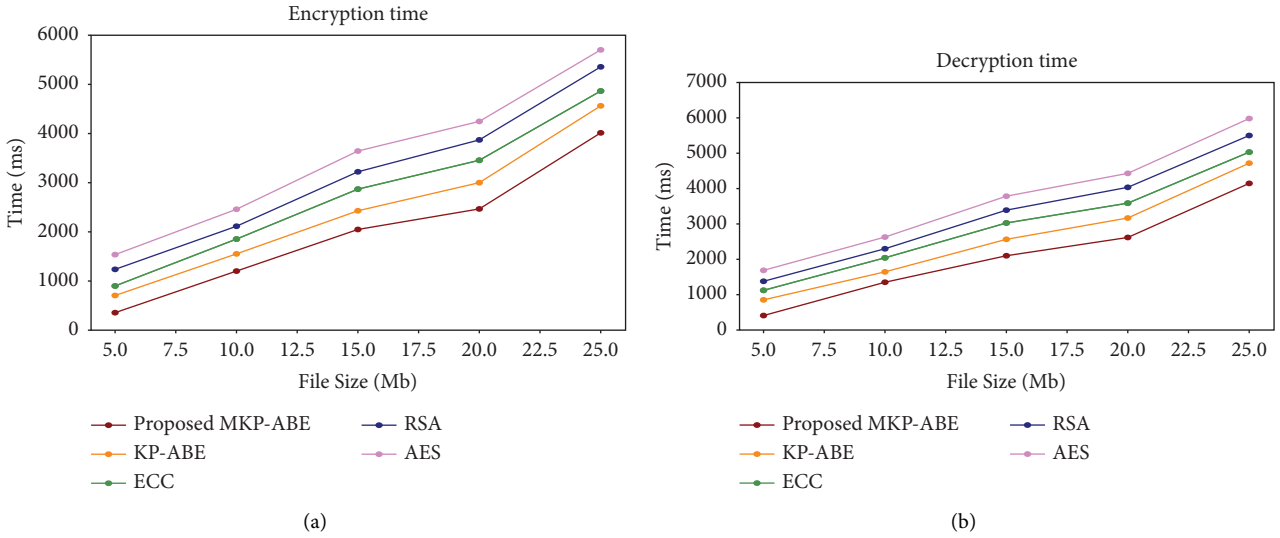

Figure 4: Comparative analysis of the proposed MKP-ABE with the traditional methods in terms of (a) Encryption time and (b) Decryption time.

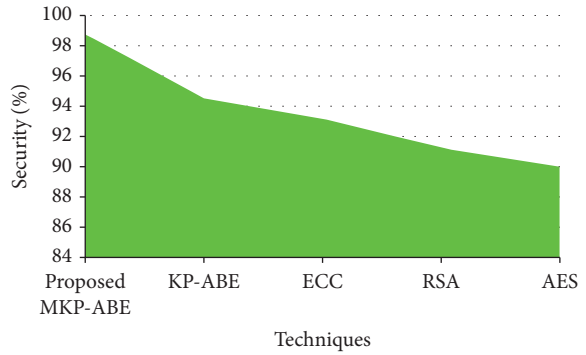

Figure 5: Security level analysis of the proposed method.

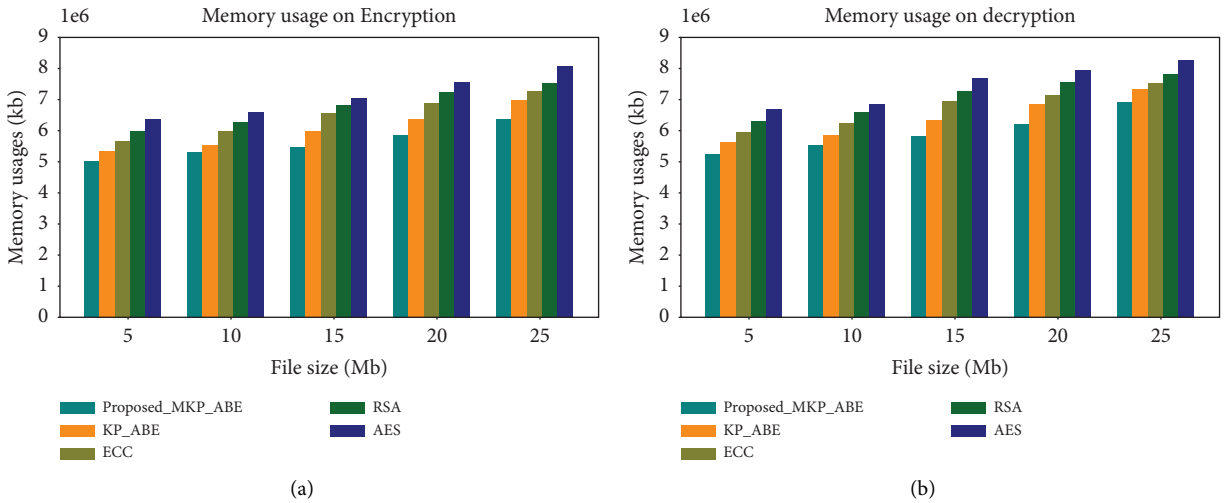

Figure 6: (a) Memory usage on encryption and (b) Memory usage on the decryption performance comparison.

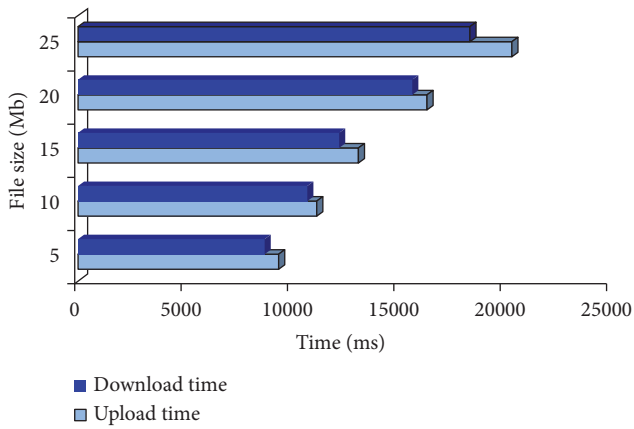

Figure 7: The proposed method's download and upload times.

5. Conclusions

Blockchain technology provides great potential for the application of digital healthcare systems. Access control for EHR is problematic, though. EHR transactions need to be kept on distributed storage on the blockchain due to their enormous number. In this article, the method recommended an effective protected exchange of electronic health data utilising the IoT-based MKP-ABE algorithm. For data collection and transformation in the healthcare domain, the approach suggested is highly responsive. The framework suggested consists of three main phases: authorization, secure upload, and stable download. The suggested system is therefore stronger than traditional models, depending on the remaining metrics. The proposed IoT mechanism achieves a high degree of success through the experimental effects analysis as opposed to traditional methods, and the protection analysis indicated that the proposed system is viable and effective and often works in a more flexible manner. The proposed Modified Key Policy Attribute-Based Encryption performs better for the remaining 10 to 25 mb file sizes. This IoT framework compares MKP-ABE to various efficiency indicators, such as encryption, decryption period, protection level analysis and encrypted memory use, resource use on decryption, upload time, and transfer time, which are present in the KP-ABE, ECC, RSA, and AES. In this case, the IoT device indicated requires 4008 ms for data encryption and 4138 ms for data decryption. Limitations and challenges with the suggested system are First off, blockchain technology has scalability problems despite providing strong security due to its decentralized structure and use of cryptography. The blockchain might find it difficult to manage the strain as the number of health records rises, which could have an effect on the performance and speed of data transactions. Moreover, there are new challenges in assuring the security and legitimacy of data from several sources when IoT devices are integrated into the blockchain network. Different IoT systems and devices may not work together properly, which could result in compatibility problems, vulnerabilities, and inconsistent data.

In future to build a test EHR organization on the Hyperledger Fabric platform in the near future. We hope this will make a strong case for other nations to start implementing it and will have a important impact on smaller countries like North Macedonia.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] M. Usman and U. Qamar, "Secure electronic medical records storage and sharing using blockchain technology," *Procedia Computer Science*, vol. 174, pp. 321–327, 2020.

[2] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, Article ID 102407, 2020.

[3] P. Morgan, "Blockchain technology: principles and applications in medical imaging," *Journal of Digital Imaging*, vol. 23, pp. 1–9, 2020.

[4] B. Jaishankar, S. Vishwakarma, P. Mohan, A. Kumar Singh Pundir, I. Patel, and N. Arulkumar, "Blockchain for securing healthcare data using squirrel search optimization algorithm," *Intelligent Automation & Soft Computing*, vol. 32, no. 3, pp. 1815–1829, 2022.

[5] S. Neelakandan, "Large scale optimization to minimize network traffic using mapreduce in big data applications," *Energy Information and Commuincation (ICCPEIC)*, vol. 25, 2016.

[6] D. Tith, H. Suzuki, W. M. A. B. Wijesundara, N. Taira, T. Obi, and N. Ohyama, "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. 0 3–12, 2020.

[7] J. Huang, W. Yuan, M. R. Asghar, A. Meads, and Y.-C. Tu, "MedBloc: a Blockchain-based secure EHR system for sharing and accessing medical data," in *Proceedings of the In18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering*, TrustCom/BigDataSE, Rotorua, New Zealand, June 2019.

[8] Y. Sharma and B. Balamurugan, "Preserving the privacy of electronic health records using blockchain," *Procedia Computer Science*, vol. 173, pp. 171–180, 2020.

[9] P. Meier, J. H. Beinke, C. Fitte, and T. Frank, "Generating design knowledge for blockchain-based access control to personal health records," *Information Systems and E-Business Management*, 2020.

[10] T. Alshalali, K. M'Bale, and D. Josyula, "Security and privacy of electronic health records sharing using hyperledger fabric," in *Proceedings of the IEEE International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 760–763, Las Vegas, NV, USA, July 2018.

[11] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[12] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018.

[13] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: a blockchain-based framework for privacy-preserving and secure data sharing in smart cities," *Computers & Security*, vol. 88, Article ID 101653, 2020.

[14] A. A. Diro, N. Chilamkurti, and Y. Nam, "Analysis of lightweight encryption scheme for fog-to-things communication," *IEEE Access*, vol. 6, pp. 26820–26830, 2018.

[15] M. Bayat and Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 56, pp. 1–29, 2020.

[16] T. T. Thwin and S. Vasupongayya, "Blockchain-based access control model to preserve privacy for personal health record systems," *Security and Communication Networks*, vol. 2019, Article ID 8315614, 15 pages, 2019.

[17] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *Journal of Medical Systems*, vol. 42, no. 8, p. 152, 2018.

[18] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[19] A. Mubarakali, "Healthcare services monitoring in cloud using secure and robust healthcare-based blockchain (SRHB) Approach," *Mobile Networks and Applications*, vol. 45, 2020.

[20] Y. Cao, Y. Sun, and J. Min, "RETRACTED: hybrid blockchain–based privacy-preserving electronic medical records sharing scheme across medical information control system," *Measurement and Control*, vol. 53, no. 7-8, pp. 1286–1299, 2020.

[21] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[22] A. A. Laghari, A. A. Khan, R. Alkanhel, H. Elmannai, and S. Bourouis, "Lightweight-BIoV: blockchain distributed ledger technology (BDLT) for internet of vehicles (IoVs)," *Electronics*, vol. 12, no. 3, p. 677, 2023.

[23] Siddique, W. Ahmed, A. Khan Jumani, and A. A. Laghari, "Introduction to internet of things with flavor of blockchain technology," *Like health care, supply chain management, etc.● Covers consensus algorithms like PAROX, RAFT, etc. and their applications This book is primarily aimed at graduates and researchers in computer science and IT*, vol. 12, 2022.

[24] A. A. Khan, S. Bourouis, M. M. Kamruzzaman et al., "Data security in healthcare industrial internet of things with blockchain," *IEEE Sensors Journal*, vol. 23, no. 20, pp. 25144–25151, 2023.

[25] A. K. Jumani and A. A. Laghari, "Blockchain and big data: supportive aid for daily life," *Security Issues and Privacy Concerns in Industry 4*, 2021.

[26] X. Xiang, J. Cao, and W. Fan, "Decentralized authentication and access control protocol for blockchain-based e-health systems," *Journal of Network and Computer Applications*, vol. 207, Article ID 103512, 2022.

[27] M. Banik and S. Kumar, "Blockchain-based public key encryption with keyword search for medical data sharing in cloud environment," *Journal of Information Security and Applications*, vol. 78, Article ID 103626, 2023.

[28] S. Shamshad, K. M. Minahil, S. Kumari, and C.-M. Chen, "A secure blockchain-based e-health records storage and sharing scheme," *Journal of Information Security and Applications*, vol. 55, Article ID 102590, 2020.

[29] C. M. Chen, X. Deng, W. Gan, J. Chen, and S. K. H. Islam, "A secure blockchain-based group key agreement protocol for IoT," *The Journal of Supercomputing*, vol. 77, no. 8, pp. 9046–9068, 2021.

[30] N. Singh and A. K. T. F. A. S. Das, "TFAS: two factor authentication scheme for blockchain enabled IoMT using PUF and fuzzy extractor," *The Journal of Supercomputing*, vol. 80, no. 1, pp. 865–914, 2023.

[31] L. Castaldo and V. Cinque, "Blockchain-based logging for the cross-border exchange of e-health data in Europe," in *International ISCIS Security Workshop*, Springer, Berlin, Germany, 2018.

[32] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, p. 218, 2016.

[33] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informatics Journal*, vol. 25, no. 4, pp. 1398–1411, 2019.

[34] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. Tavares, and V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cognitive Systems Research*, vol. 52, pp. 1–11, 2018.

[35] P. Genestier, S. Zouarhi, P. Limeux, D. Excoffier, and A. Prola, "Blockchain for consent management in the e-health environment: a nugget for privacy and security challenges," *Journal of the International Society for Telemedicine and eHealth*, vol. 5, 2017.

[36] A. A. Omar, M. Z. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Generation Computer Systems*, vol. 95, pp. 511–521, 2019.

[37] E. S. Babu, B. V. R. N. Yadav, A. K. Nikhath, S. R. Nayak, and W. Alnumay, "Medi blocks: secure exchanging of electronic health records (Ehrs) using trust-based blockchain network with privacy concerns," *Cluster Computing*, vol. 26, no. 4, pp. 2217–2244, 2022.

[38] S. Tiwari, N. Dhanda, and H. Dev, "A real time secured medical management system based on blockchain and internet of things," *Measurement: Sensors*, vol. 25, Article ID 100630, 2023.

[39] F. Pelekoudas-Oikonomou, G. Zachos, M. Papaioannou et al., "Blockchain-based security mechanisms for IOMT edge networks in Iomt-based healthcare monitoring systems," *Sensors*, vol. 22, no. 7, p. 2449, 2022.

[40] J. Rene Beulah, L. Prathiba, G. L. N Murthy, E. Fantin Irudaya Raj, and N. Arulkumar, "Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model," *International Journal of Modeling, Simulation, and Scientific Computing*, vol. 14.

[41] S. Bhargava, K. Mohan, N. R. Robert, and S. Upadhye, "Optimal stacked sparse autoencoder based traffic flow prediction in intelligent transportation systems," *Studies in Systems, Decision and Control*, vol. 412, 2022.

[42] K. Kumar Singamaneni, C. Pretty Diana Cyril, S. Neelakandan, and S. Velmurugan, "Automated speech-based evaluation of mild cognitive impairment and Alzheimer's disease detection using with deep belief network model," *International Journal of Healthcare Management*, vol. 45, 2022.

[43] P. Mohan, S. Veerappampalayam Easwaramoorthy, N. Subramani, M. Subramanian, and S. Meckanzi, "Handcrafted deep-feature-based brain tumor detection and classification using MRI images," *Electronics*, vol. 11, no. 24, p. 4178, 2022.

[44] M. Gangathimmappa, N. Subramani, V. Sambath, R. A. M. Ramanujam, N. Sammeta, and M. Marimuthu, "Deep learning enabled cross-lingual search with metaheuristic web-based query optimization model for multi-document summarization," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 2, 2022.

[45] S. Mary Rexcy Asha, S. Neelakandan, M. Prakash, B. Geetha, S. Mary Rexcy Asha, and M. K. Roberts, "Artificial humming bird with data science enabled stability prediction model for smart grids," *Sustainable Computing: Informatics and Systems*, vol. 36, Article ID 100821, 2022.

[46] P. Ezhumalai, D. Paulraj, P. Ezhumalai, and M. Prakash, "A Deep Learning Modified Neural Network (DLMNN) based proficient sentiment analysis technique on Twitter data," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 47, pp. 1–20, 2022.