information

MDPI

Article

Intelligence Amplification-Based Smart Health Record Chain for Enterprise Management System

S. Velliangiri [1], P. Karthikeyan [2], Vinayakumar Ravi [3,*], Meshari Almeshari [4] and Yasser Alzamil [4]

[1] Department of Computational Intelligence, SRM Institute of Science and Technology, Kattakulathur Campus, Chennai 603203, India; velliangiris@gmail.com
[2] Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 62102, Taiwan; nrmkarthi@gmail.com
[3] Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar 34754, Saudi Arabia
[4] Department of Diagnostic Radiology, College of Applied Medical Sciences, University of Ha'il, Ha'il 55476, Saudi Arabia; m.almeshari@uoh.edu.sa (M.A.); y.alzamil@uoh.edu.sa (Y.A.)
* Correspondence: vravi@pmu.edu.sa

Abstract: Medical service providers generate many healthcare records containing sensitive and private information about a patient's health. The patient can allow healthcare service providers to generate healthcare data, which can be stored with healthcare service providers. After some time, if the patient wants to share the healthcare records of one healthcare service provider with another, we can quickly exchange the healthcare record using our approaches. The challenges faced by healthcare service providers are healthcare record sharing, tampering, and insurance fraud. We have developed Health Record Chain for Sharing Medical Data using the modified SHA-512 algorithm. We have evaluated our methods, and our method outperforms in terms of storage cost and total time consumption for health record sharing. The proposed model takes 130 ms to share 100,000 records, 32 ms faster than traditional methods. It also resists various security attacks, as verified by an automated security protocol verification tool.

Keywords: blockchain; health record chain; medical data; hashing; smart contract

check for updates

Citation: Velliangiri, S.; Karthikeyan, P.; Ravi, V.; Almeshari, M.; Alzamil, Y. Intelligence Amplification-Based Smart Health Record Chain for Enterprise Management System. *Information* **2023**, *14*, 284. https://doi.org/10.3390/info14050284

Academic Editor: Qingchen Zhang

Received: 12 April 2023
Revised: 30 April 2023
Accepted: 9 May 2023
Published: 11 May 2023

1. Introduction

Over the years, medical facilities have undergone significant advancements. However, one major challenge faced by patients is the need to present their medical records every time they visit a doctor. These records typically comprise prior prescriptions, medical history, X-rays, MRIs, and other related documents. Managing these records is a time-consuming task [1,2], and sharing them globally is often difficult due to variations in healthcare formats and security protocols employed by different healthcare service providers. To address this issue, we propose a digital solution that eliminates the need for patients to carry physical medical files. Our solution involves utilizing blockchain technology to store patient records securely. By storing the data on a decentralized network, we can ensure that the data are distributed among several peers, making it more resilient to data breaches [3–5]. The main concept of our proposal is to leverage the benefits of blockchain technology to improve the efficiency and security of patient record management. The process for accessing and managing patient medical records on the proposed blockchain network is simple and secure. Any individual can join the network as a doctor or a patient, and when a patient visits a doctor, the doctor is granted access to save the diagnosis and medical records on the patient's record on distributed ledgers across the blockchain network. The doctor can create and edit a patient's records by signing the transaction, which is encrypted cryptographically using their private key. Each patient is uniquely identified by a patient ID, which ensures that their medical information is kept private and secure [6,7].

To ensure that hospitals and patients worldwide can communicate with each other, the proposed health record chain system utilizes a permissioned blockchain. This allows patients to have complete control over their health information and enables them to approve or withdraw access to their records from healthcare service providers. One of the main challenges in sharing healthcare records on the blockchain is ensuring user privacy. Recent advancements in blockchain technology, such as the development of permissioned blockchain networks, have addressed this issue by enabling only specific end-users to join the network [8–10]. To prevent medical errors and ensure that healthcare service providers have access to a patient's complete medical history, we have implemented a two-layered health record chain using blockchain technology. By leveraging the decentralized and encrypted nature of blockchain, we are able to enhance the security of patient data and make it difficult for unauthorized individuals to access or alter the information stored on the network. This helps prevent medical identity theft and insurance fraud, safeguarding sensitive patient data. Another advantage of blockchain-based health record sharing is the ability to enable secure and efficient data sharing between healthcare providers. Patients can grant permission for their healthcare data to be shared with specific providers, ensuring that only the necessary information is disclosed.

The decentralized nature of blockchain also eliminates the need for a central authority to manage the data, reducing the risk of data breaches and unauthorized access. To achieve this, we have implemented a private blockchain as the first layer, maintained by healthcare service providers, and a permissioned blockchain as the second layer, maintained by collective healthcare service providers. Transactions are kept in plain text, which means that attackers can steal data by gaining access to blockchain nodes or impersonating a healthcare service provider. Therefore, healthcare records on distributed ledgers must be encrypted, and control measures must be imposed to limit access to critical information [11–13].

Motivations

The motivation of the article is summarized as follows.

1. The adoption of blockchain technology in healthcare can be challenging due to the varied approaches of different institutions such as healthcare providers and insurance payers. Without a streamlined method such as a single-payer system, getting these organizations to adopt blockchain technology can be difficult, which can reduce the effectiveness of the entire system.
2. Hospitals and insurance companies may intentionally avoid sharing data due to the competitive advantage of confidentiality. Data sharing between these entities can be challenging, which can hinder the implementation of blockchain technology in healthcare.
3. The lack of effort and awareness of blockchain technology among those outside of information technology can be a barrier to its adoption, and even financial incentives may not be enough to address this issue.

Although the adoption of blockchain technology in healthcare can be challenging due to various barriers, including the varied approaches of different institutions, the competitive advantage of confidentiality, and the lack of awareness outside of information technology, there are novel solutions being developed to overcome these challenges. The multiple healthcare providers and insurers can join together on a single platform, creating a streamlined approach to adoption. Additionally, new privacy-focused blockchain technologies such as the new modified SHA-512 are being developed to address the concerns around confidentiality and data sharing. These novel solutions have the potential to overcome the current barriers to blockchain adoption in healthcare, making it more effective and secure for patients and providers. The novelty in the research paper is the proposed Health Record Chain for Sharing Medical Data, which uses a modified SHA-512 algorithm to securely store and exchange healthcare records between healthcare service providers.

The contributions of the research article are summarized as follows:

- Health record chain is a permissioned blockchain technology that allows data sharing while maintaining anonymity. A modified SHA-512 algorithm was used to create new block structures that give a complete medical history for each patient while maintaining data integrity.
- A modified hash algorithm was designed to improve execution speed while keeping the SHA-512 structure.
- The proposed solution was evaluated against state-of-the-art medical data-sharing methods using blockchain technology to assess its efficacy.

The remaining structure of this research paper is as follows. Section 2 provides an overview of previous work on using blockchain technology for health record sharing. Section 3 presents a detailed model of our proposed health record chain. Our performance assessment and security analysis of the health record chain are discussed in Section 4. Lastly, Section 5 concludes the research paper and provides potential future directions for this study area.

2. Related Works

Wang et al. proposed a novel solution for secure and energy-efficient healthcare by integrating wireless body area networks (WBANs) with blockchain technology. Their approach involves linking patients' devices via WBANs and utilizing blockchain technology for data transmission and storage. The system is designed to use hardware resources efficiently, while providing robust security and consistent performance. In another study, Wang et al. presented a medical diagnosis and treatment system that incorporates AI healthcare technology. They conducted computational experiments to assess treatment options and utilized parallel processing to facilitate timely and optimized decision-making in both real and virtual healthcare scenarios. Additionally, they constructed a consortium blockchain network connecting patients, hospitals, health bureaus, and the healthcare community, by combining blockchain technology with personal health systems (PHS). This system allows for comprehensive exchange of healthcare data, review of health records, and safeguarding of care quality.

Wang et al. reported that blockchain-empowered secure data management using the Guard Health data sharing system is used for data storage, and the Guard Health information system is used for data sharing [14,15]. A Graph Convolutional Network is constructed to identify dangerous nodes to provide a trust model to enforce security and reduce risks. According to the security analysis, the model used in this research might fulfil security criteria and outperform standard schemes in terms of efficiency according to a performance evaluation [16].

Zhao et al. combined blockchain and body sensor networks to share healthcare data efficiently. Biosensor nodes in the body sensor network provide a lightweight backup and recovery method for health blockchain keys. Biosensor nodes in the body sensor network are in charge of generating, backing up, and recovering health blockchain keys, which will improve their security. The blocks on the blockchain may be encrypted with a unique key, leading to low storage cost and excellent performance [17]. Shamshad et al. proposed an efficient authentication scheme in electronic health record management systems using blockchain. The proposed model is applied to three levels: end-user, resource, and healthcare service providers. Out of N from N 1 authorities, an identity-based signature scheme with numerous authorities can survive a collision attack. This model performs more efficiently than traditional electronic health record management systems [18].

Rajput et al. developed an emergency access control management system (EACMS) that protects the patient's health record by enforcing privacy and security regulations in an emergency. The Hyperledger Composer network, a permission blockchain system, controls EACMS. As a result, personal health record data is only accessible to known members of the blockchain, as stated by the consortium's admin peers [19]. Xu et al. proposed a blockchain approach for secure and fine-grained control of health data on a large scale. The solution uses two blockchains to prevent medical conflicts and protect against unauthorized access to users' health data and doctors' diagnoses. The encrypted data and keys are separated to allow for flexible key management.

Furthermore, consumers can remove physicians at any moment to protect their privacy. The privacy-preserving approach was shown to be efficient and practical in reality. However, the solution needed to be more appropriate for a multi-level user healthcare system [20].

Chen et al. discussed the electronic health record-sharing mechanism using blockchain-based searchable encryption. A trustworthy and confidential search scheme is established without any verification mechanism using a specified smart contract on blockchain to substitute the centralized server. The suggested system achieves justice by rewarding honest users using blockchain technology. The method appears viable and thriving based on the security analysis and performance evaluations [21]. Dagher et al. presented a blockchain framework for secure, efficient, and interoperable access to medical records while preserving patients' sensitive information. The framework employs smart contracts on an Ethereum blockchain for access management, data protection, and enhanced security through cryptographic methods [22].

Huang et al. created MedBloc, a blockchain-based healthcare record-sharing system aimed at unifying New Zealand's diverse health IT landscape and addressing issues in the existing healthcare system. MedBloc is a fully functional, patient-centered EHR solution that enables easy access and exchange of health information through a dedicated client service by patients and healthcare professionals. Patients can grant and withdraw consent using smart contracts and cryptographic methods. Healthcare providers may obtain consent and upload records to the blockchain, which are encrypted and securely kept [23]. Aruna Sri et al. reported a healthcare data management consensus algorithm. Blockchain technology is widely applied in various areas of healthcare, such as data management, medication adherence, supply chain management, claims and billing administration, and analytics. The proposed method takes fewer communication costs than traditional healthcare record management systems [24]. Yang et al. provided a viable method for exchanging medical records on the cloud while maintaining privacy. It involved employing vertical partitioning of medical datasets to categorize medical records' characteristics and examining many aspects of medical data, each with its privacy issues [25]. Roehrs et al. described Omni personal health record (OmniPHR) architecture that uses blockchain technology and the openEHR interoperability standard to connect dispersed health records. OmniPHR is a blockchain-based prototype that improves health data replication among computer nodes. Thousands of concurrent connections transferring data blocks across a network of ten super peers are used to test the performance of the OmniPHR prototype [26].

Tanwar et al. proposed an electronic healthcare record-sharing system built on a blockchain network. The immutable ledger technology ensures the system's security by preventing unauthorized modifications, eliminating the risk of a single point of failure. The system's performance was evaluated using Caliper by adjusting parameters such as block size, block verification time, and endorsement policy and implementing optimizations for metrics such as latency and throughput [27]. Sreenu et al. proposed a blockchain and IoT-based vaccine supply chain to address issues of falsified or substandard vaccines and ensure efficient and resilient vaccine management during pandemics. The system is built on the Hyperledger Fabric framework and has been evaluated to perform better than other benchmark schemes in speed and efficiency [28]. Butt et al. proposed a chain-like structure for sharing medical records, using blockchain technology and HL7 standards to create global connectivity between records. The approach focuses on making patient data available for a specific period. The proposed approach performs better than other record-sharing systems, reducing the time to read, write, delete, and revoke a record [29].

3. Proposed Methodology

The current method of storing and sharing medical records is plagued with several issues, such as high costs, data tampering, and insurance fraud. Patients often carry physical or digital copies of their medical records when seeking treatment in different regions, which can be challenging for medical service providers to accept due to the sensitive information contained within. To address these challenges, we have developed a blockchain-based medical record-sharing method that can be used across multiple regions.

Our proposed method is designed to enable medical service providers to share health records between regions without compromising data security. The current centralized approach can be vulnerable to hackers who may modify medical records to gain benefits, and our method provides a secure, efficient, and cost-effective solution to this problem. Our health record chain model integrates insurance service providers into the healthcare record chain model and enables easy sharing of medical records between healthcare service providers, patients, and insurance companies, regardless of location. This method provides a secure platform for managing sensitive medical information and ensures the easy transfer of medical records in a global environment. To better understand our proposed method, we have depicted the overview of the health record chain in Figure 1 and the healthcare record chain for integration into the existing system in Figure 2.

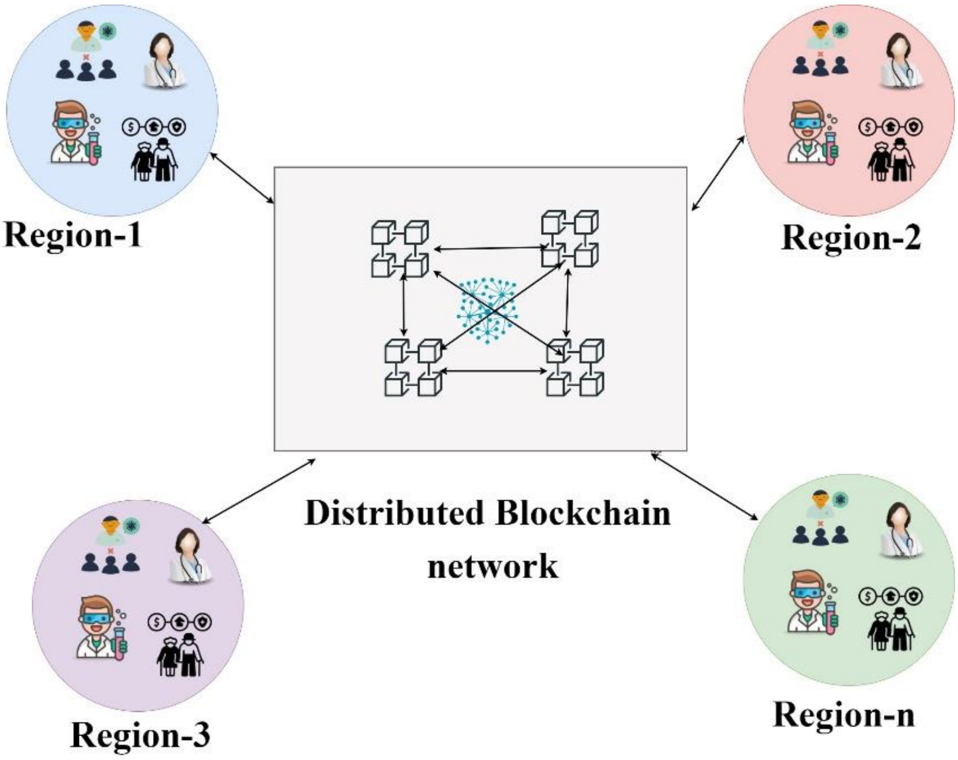


Figure 1. Overview of the health record chain for enterprise management system.

3.1. Data Generations

Data can be generated in various ways within the healthcare chain. Healthcare service providers generate a variety of data, including X-rays, MRI scans, ultrasound reports, angiography, radiography, endoscopy, as well as text, paper, numeric, image, video, digital, and multimedia data. Insurance service providers generate insurance claims details, while patients can add personal information such as name, age, address, and medical history to the health record chain. Additionally, research institutions may generate clinical trial data that can be added to the health record chain network. Table 1 outlines the read and write permissions for users in the Health Record Chain for Sharing Medical Data in a Global Environment.

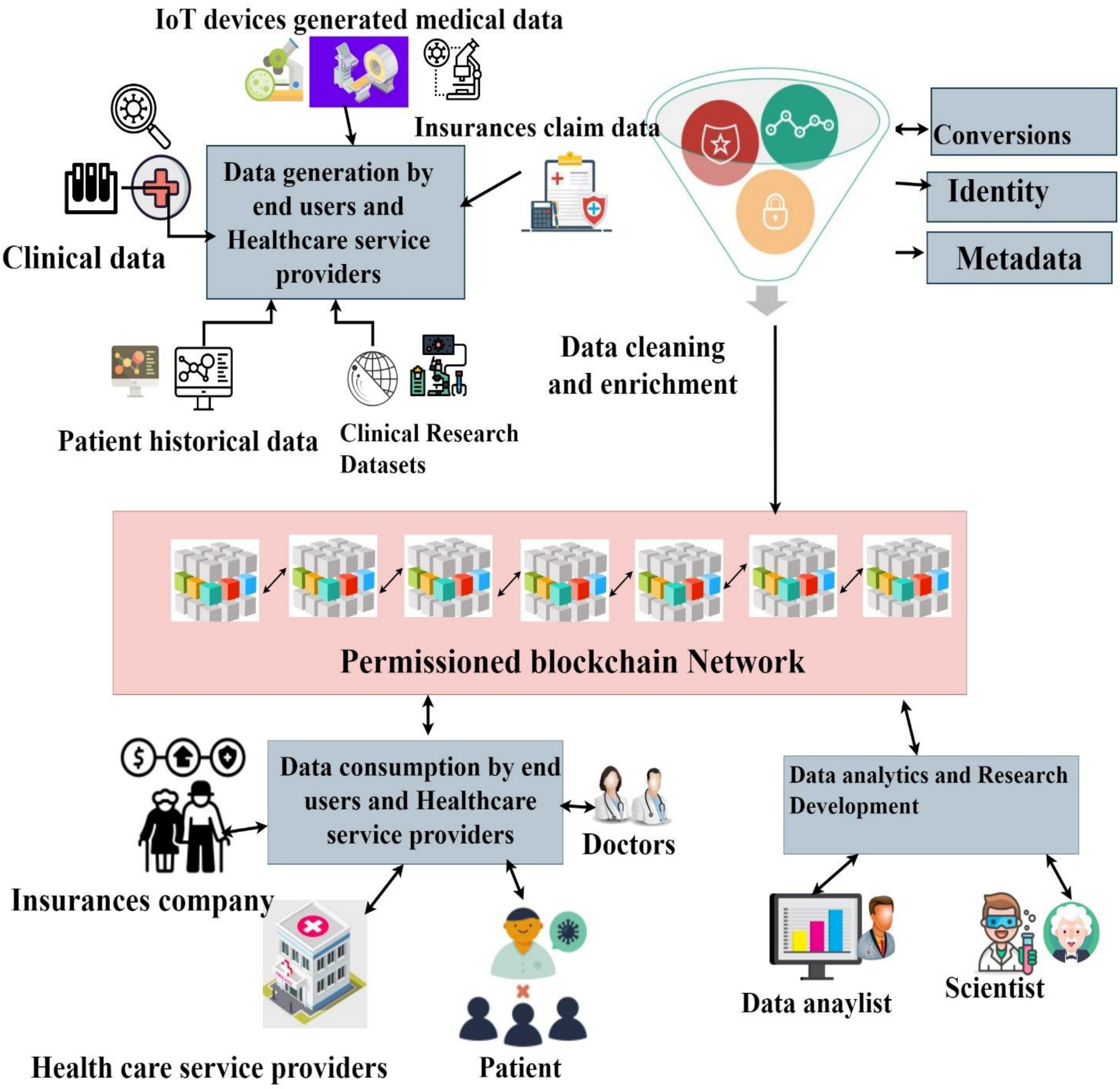

IoT devices generated medical data
Insurances claim data
Data generation by end users and Healthcare service providers
Clinical data
Patient historical data
Clinical Research Datasets
Conversions
Identity
Metadata
Data cleaning and enrichment
Permissioned blockchain Network
Data consumption by end users and Healthcare service providers
Doctors
Insurances company
Health care service providers
Patient
Data analytics and Research Development
Data anaylist
Scientist

Figure 2. Healthcare record chain for enterprise management system workflow.

3.2. Data Cleaning

In the healthcare chain, data can be collected from multiple entities and in various formats. Before adding healthcare data to the health record chain network, it should be cleaned to ensure accuracy and consistency. This can be achieved by adding timestamp information, indicating when the data were created, by whom, and for what purpose. Unwanted and noisy information should be removed from the data generated by different healthcare record sources. To ensure data security, a hash code is generated and added to all healthcare records before they are added to the health record chain network. It is important to note that data storage on the blockchain does not imply non-compliance. In fact, compliance enforcement can be made smoother and more transparent through the use of blockchain technology. Health Insurance Portability and Accountability Act (HIPAA) compliance protects patient data, ensuring that all electronically protected health information generated, received, managed, or transmitted by healthcare providers is kept confidential, secure, and available.

Table 1. Read and write permission of different users in the health record chain model.

S. No	User	Permission
1	Doctors or healthcare service providers	1. Read/Write on permissioned healthcare records 2. Request other healthcare service providers to read or change the healthcare record
2	Patient	1. Read their healthcare records 2. Permitting healthcare service providers to read and change their healthcare records.
3	Insurances service providers	1. Read/Write on permissioned electronic health records. 2. Requesting the patient to read and change the healthcare record.
4	Research institution	1. Read the permission healthcare record.

3.3. Construction of Permissioned Blockchain Network

Healthcare providers can preserve health records on the blockchain using the patient's public key. Intelligent contracts are activated when doctors, diagnostic facilities, or health insurance firms give information stored on the blockchain. Healthcare service providers, patients, insurance providers, and research institutions use the public critical medical token to create a new healthcare record block.

The created new health record block is sent to the hash algorithm which divides the message into 2048 bit, takes a securely stored object as input, and computes the hash code for the given message. The generated hash code is sent to an existing blockchain network, which uses a consensus algorithm to validate whether the given health record block is valid to add to the existing blockchain network. If any end-users request access to the health record block, transfer the requested health record to the end-users if that record is not compromised. If the health record block is compromised, that block is removed from the existing blockchain network. Figure 3 shows the hashing functions in the health record chain network.

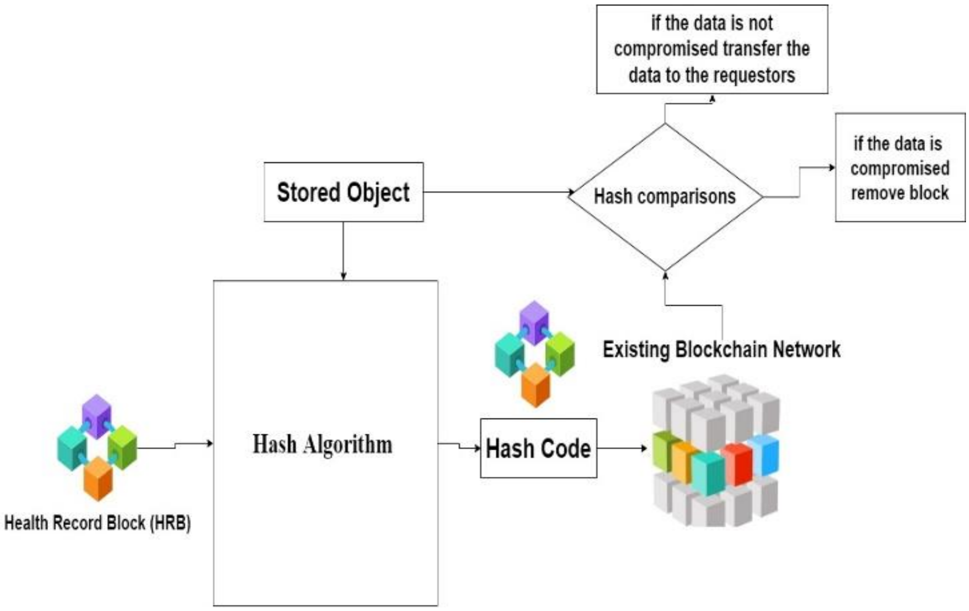

if the data is not compromised transfer the data to the requestors
Stored Object
Hash comparisons
if the data is compromised remove block
Existing Blockchain Network
Hash Algorithm
Hash Code
Health Record Block (HRB)

Figure 3. Hashing in health record chain.

3.4. Hash Value Generations

SHA-512 is unquestionably more secure than SHA-256. Although it generates a giant hash (and utilizes more rounds), more states could also make it more vulnerable. This is especially true for the output size-reducing SHA-512/224 and SHA-512/256 algorithms. As an illustration, a differential attack against SHA-512 in 2016 revealed a real-world collision on SHA-256/244's 44 rounds. A collision attack on 38-round SHA-512 has a complexity of 240.5, but a similar attack on 38-round SHA-256 has a complexity of 237. Even still, the change is less significant than one might anticipate. So we have decided to modify the SHA-512 algorithm to improve performance.

Divide the cleaned healthcare record into the fixed size of message 2048 bit with N number of blocks. A hash algorithm takes 2048 bits as input and produces 1024 bits as hashed output. The 1024-bit intermediate buffer is used to hold the intermediate result of the hash code.

3.5. Hash Code Algorithm

```
    Input: Health Record Block (HRB) is divided into M1, M2, M3, . . . . . . , MN
    Output: Hach code HN
    Intermediate Buffer can be created as IB1, IB2, IB3, IB4, . . . . . . , IB16
1.  Initialize the Initialize hash value
    h0,0 = 3A59E667F3BCC908
    h0,1 = BB67AE8584CAA73B
    h0,2 = 3C6EF733FE94F82B
    h0,3 = 546FF5387F1D36F1
    h0,4 = 98E1527FADE682D1
    h0,5 = 9B04689C2B3E6C1F
    h0,6 = 1F83D9B3FB41BD62
    h0,7 = 6F10CD19137E2908
    h0,8 = 1BFF763ABC25338C
    h0,9 = 1967250912EF23AE7
    h0,10 = 38765129EFA1298E
    h0,11 = 837839090EFEFA12
    h0,12 = 54645FEF678AD1EF
    h0,13 = 1BFF763ABC25338C
    h0,14 = 4AFF673265FEADB1
    h0,15 = 947AB4525C1AEF18
2.  Process the Health Record Block (HRB)
    For i = 1 to N
2.1. Prepare the message schedule S
    For t = 0 to 16
    St = Mi, t
    For t = 0 to 79
    St = SigmaFun (St-2) + (St-7) + SigmaFun(St-15) + St-16
2.2. Initialize the intermediate buffer
    IB1 = hi-1,0
    IB2 = hi-1,1
    IB3 = hi-1,2
    IB4 = hi-1,3
    IB5 = hi-1,4
    IB6 = hi-1,5
    IB7 = hi-1,6
    IB8 = hi-1,7
    IB10 = hi-1,9
    IB11 = hi-1,10
    IB12 = hi-1,11
    IB13 =hi-1,12
    IB14 = hi-1,13
    IB15 = hi-1,14
    IB16 = hi-1,15
2.3. Hash Code Computations
    For t = 0 to 79
    $T_1 = IB_1 + Ch (IB_2 + IB_3 + IB_4) + \sum_1^{1024} IB_4 + S_t + K_t$
    $T_2 = \sum_1^{1024} IB_1 + Maj (IB_1 + IB_2 + IB_3)$
    $IB_1 = T_1 + T_2$
    $IB_2 = IB_1$
    $IB_3 = IB_2$
    $IB_4 = IB_3$
    $IB_5 = IB_4 + T_1$
    $IB_6 = IB_5$
    $IB_7 = IB_6$
    $T_3 = IB_1+Ch (IB_{10}+ IB_{11}+ IB_{12}) + \sum_1^{1024} IB_{12} + S_t + K_t$
    $T_4 = \sum_1^{1024} IB_1 + Maj (IB_9 + IB_{10} + IB_{11})$
    $IB_9 = T_3 + T_4$
    $IB_{10} = IB_9$
    $IB_{11} = IB_{10}$
    $IB_{12} = IB_{11}$
    $IB_{13} = IB_{12} + T_3$
    $IB_{14} = IB_{13}$
    $IB_{15} = IB_{14}$
2.4. Compute the intermediate Hash value
    h0,0 = IB1 + hi-1,0
    h0,1 = IB1 + hi-1,1
    h0,2 = IB1 + hi-1,2
    h0,3 = IB1 + hi-1,3
    h0,4 = IB1 + hi-1,4
    h0,5 = IB1 + hi-1,5
    h0,6 = IB1 + hi-1,6
    h0,7 = IB1 + hi-1,7
    h0,8 = IB1 + hi-1,8
    h0,9 = IB1 + hi-1,9
    h0,10 = IB1 + hi-1,10
    h0,11 = IB1 + hi-1,11
    h0,12 = IB1 + hi-1,12
    h0,13 = IB1 + hi-1,13
    h0,14 = IB1 + hi-1,14
    h0,15 = IB1 + hi-1,15
Return (hN,0| | hN,1| | hN,2| | ... ... ... ... ... .... hN,15)
```

3.6. Data Consumption Using Smart Contract

The proposed approach involves setting up a network using Hyperledger Fabric, an open-source blockchain platform, to encrypt and store a patient's medical record as a digital asset. Access to the medical record is controlled through implemented access policies using smart contracts. Patients authorize access to their medical records through digital signatures, which authorized recipients, such as doctors or hospitals, verify before accessing the record using the proposed hash algorithm. Any updates to the medical record are recorded on the Hyperledger network, providing a transparent and permanent record of all transactions and updates. Our algorithms ensure that the medical record is secure and only accessible by authorized individuals.

Smart contracts are created in computer code and are based on user-defined parameters. Once stated criteria are satisfied, the full provisions of the contract are implemented, just like in a written paper contract. The end user can use the smart contract and access the data.

Patients: A group of patients $\{pa \in P \mid 1 \leq a \leq \infty\}$ who receive care from various medical establishments. Patients may choose how much information they want to provide according to their privacy choices.

Healthcare service providers: A set of healthcare service providers $\{HSP \in HS \mid 1 \leq b \leq \infty\}$ that offer required medical treatment to patients in P and create records detailing the treatment outcome.

Doctors: The set of doctors $\{D, l \; \forall \; 1 \leq l \leq \infty\}$ working at healthcare service providers.

Insurance agent: The set of insurance agents $\{IA, l \; \forall \; 1 \leq l \leq \infty\}$ working at insurance service providers.

Health record block is denoted as HRB. $\{HRBj \in B \mid 1 \leq j \leq n\}$

privilege-based access structure that consists of k levels {P1, P2, . . . , Lk} and their corresponding access policies {T1, T2, . . . , Tk}. The patient record is referred to as B {B1, B2, B3, . . . , BK}. The symmetric encryption key is generated for the patient {Sk1, Sk2, ... , Skk}. The healthcare record is encrypted using a symmetric encryptions algorithm using Ski.

$$\text{EBi} = \text{Symmetric\_Encryption(Ski,Bi)} \tag{1}$$

Ski is encrypted using an asymmetric public key encryption algorithm using Ti, described in an access policy for the patient.

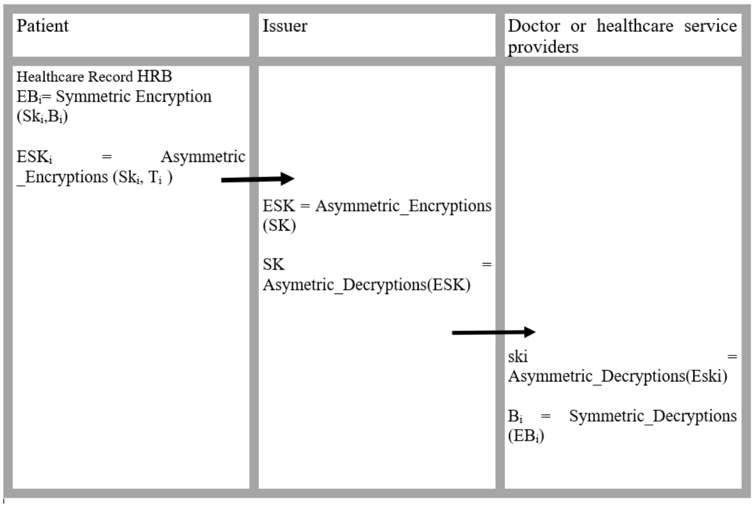
$$\text{ESKi} = \text{Asymmetric\_Encryptions(Ski,Ti)} \tag{2}$$

A patient creates a smart contract with access policies (T1, T2, . . . , Tk) and deploys it on a permissioned blockchain for access to the health record chain by end-users. During further medical treatment at another facility, the staff must have attributes (A) that match the patient's access policies to access any part of the record. A key issuer constantly monitors the blockchain and creates a private key (SK) for the end-user upon validation of a specific team member. The private key is encrypted with the end-user's public key, resulting in ESK = Asymmetric_Encryption(SK) (Equation (3)). The end-user can then acquire the private key by decrypting ESK using their private key (pr), as shown in Equation (4): SK = Asymmetric_Decryption(ESK). The patient obtains the encrypted blocks (B1, B2, B3, . . . , BK) from the health record chain and symmetric keys (Sk1, Sk2, . . . , Skk). The end-user can then decrypt the symmetric key (Eski) that belongs to level Li using the generated private key from Equation (4), such that ski = Asymmetric_Decryption(Eski) (Equation (5)). The end-user can also derive the remaining symmetric keys (ski + 1, . . . , skk) and decrypt the encrypted health record (EB1, EB2, EB3, . . . , EBK) from the healthcare chain network using Equation (6). Figure 4 illustrates the medical record sharing of the proposed efficient blockchain-based authentication approach.

$$\text{ESK} = \text{Asymmetric\_Encryptions(SK)} \tag{3}$$

$$\text{SK} = \text{Asymetric\_Decryptions(ESK)} \tag{4}$$

$$\text{ski} = \text{Asymmetric\_Decryptions(Eski)} \tag{5}$$



Patient

Healthcare Record HRB
EB_i= Symmetric Encryption (Sk_i,B_i)

ESK_i = Asymmetric _Encryptions (Sk_i, T_i)

Issuer

ESK = Asymmetric_Encryptions (SK)

SK = Asymetric_Decryptions(ESK)

Doctor or healthcare service providers

ski = Asymmetric_Decryptions(Eski)

B_i = Symmetric_Decryptions (EB_i)

Figure 4. Medical record sharing of proposed blockchain-based efficient authentication approach.

The end-users can also derive the symmetric keys ski + 1, . . . , skk. Finally, the end-users decrypt the encrypted EB1, EB2, EB3 . . . .EBK healthcare record from the healthcare chain network using Equation (6). Figure 4 shows the medical record sharing of the proposed blockchain-based efficient authentication approach.

$$\text{Bi} = \text{Symmetric\_Decryptions(EBi)} \tag{6}$$

4. Experiments

This section discusses the experimental setup, result discussion, and security investigation of the proposed model.

4.1. Experimental Setup

The health record chain proposed in this study was implemented using the Python programming language and was thoroughly tested. A single computer node with 16 GB random access memory, Ubuntu operating system, and an Intel I7 processor were used for testing purposes. The effectiveness of the proposed health record chain model was evaluated by comparing it with conventional healthcare record management systems, and simulation parameters were changed for the analysis. The Nursery dataset from the University of California, Irvine (UCI) machine learning repository (UCI, 0000), which consists of 12,960 healthcare records, each 32 kB in size, was used as a test dataset. To test the health record chain, we increased the number of healthcare records in the original dataset to 100,000. To create chameleon hash values for encrypted healthcare records, we used the chameleon hash function available on Github. Additionally, we compared the storage overhead of various systems with different numbers of healthcare records.

4.2. Result Discussion

Our method provides greater than 20%. Since they work on arbitrary-sized inputs to fixed-sized outputs, in order to witness at least one colliding pair with a 50% probability for SHA-256, they need about 2128 inputs. SHA-512 uses the value 2256. The generic birthday attack, which costs O(2n/2) with a 50% discount for an n-bit output hash function, is to blame for this. Figure 5 depicts the hash value generations of SHA-512 and our methods.

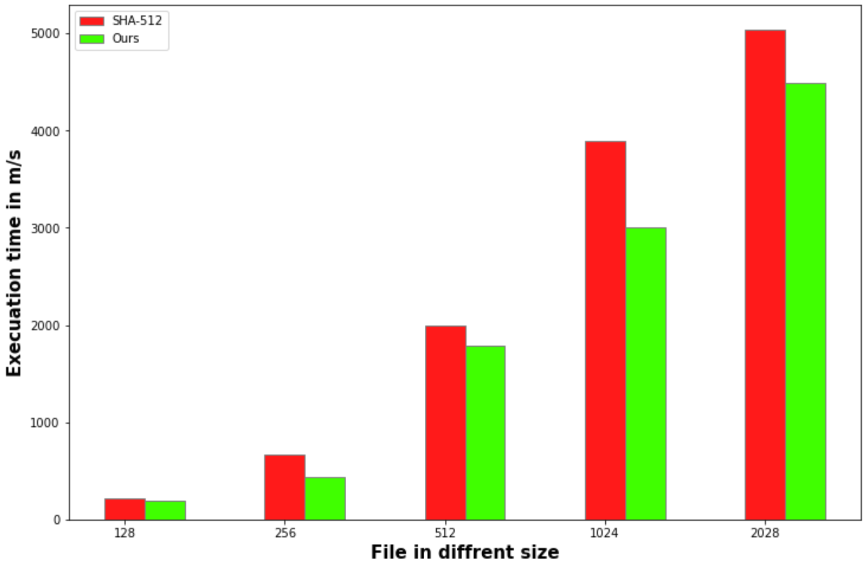


Figure 5. Hash value generation.

Figure 6 shows the overhead storage comparisons of the proposed approach and existing methods. The *X*-axis shows the number of medical records shared among the medical service providers., and the *Y*-axis shows the storage taken by the cloud service providers in MB. Aruna Sri et al. [24] used 810 MB storage for sharing 300,000 healthcare records. In contrast, Tanwar et al. [27] used significantly lower storage, 670 MB, for sharing 300,000 healthcare records. The storage of the proposed approach is 511 for sharing 300,000 healthcare records which is much lower than existing approaches because our proposed approach modifies using the hash function, which reduces the storage overhead. The storage overhead plays a vital role in sharing data in a global environment because the data need to be shared from one location to another. Our approach uses a modified hashing function and a simplified algorithm to take less storage overhead. Our approach to blockchain methods, such as sharding and pruning, can significantly reduce the storage overhead compared to a traditional blockchain. Sharding allows for the storage of the blockchain to be split into smaller pieces or shards, which can be stored on separate nodes, reducing the storage requirements for each node. Pruning allows for removing old, unneeded data from the blockchain, further reducing the storage overhead. Our proposed model requires only 500 MB to store 30,000 records, 25% less storage than traditional methods.

Our approach is more efficient regarding total consumption time for record sharing with cloud service providers, as shown in Figure 7. Aruna Sri et al. took 162 ms and 177 ms to share 100,000 and 200,000 healthcare records, while Yang et al. took even less time using a consensus mechanism with blockchain technology. Regardless of the increased number of shared records, our approach consistently requires lesser total consumption time than existing methods. As depicted in Figure 8, our approach also requires less storage cost compared to existing methods. The *X*-axis in the figure represents the different methods used in medical record sharing, while the *Y*-axis represents the cost of sharing 10 medical records. Our approach has a lower storage cost than existing methods, with Huang et al. incurring a storage cost of 51$ for sharing 10 healthcare records due to the use of heavyweight protocols. Our approach outperforms all other traditional methods because we are not using any third party for medical validity records or have no extra process to add a medical record. If any users want to add a record, they should create an account and can add their record without creating extra complications in medical record sharing. Consensus algorithms used in the traditional blockchain-based model can be time-consuming. Multiple nodes must reach a consensus before a record can be shared, leading to longer wait times. Our proposed model takes 130 ms to share 10,000 records. This is because our model is more secure as it shares with the permissioned blockchain network.

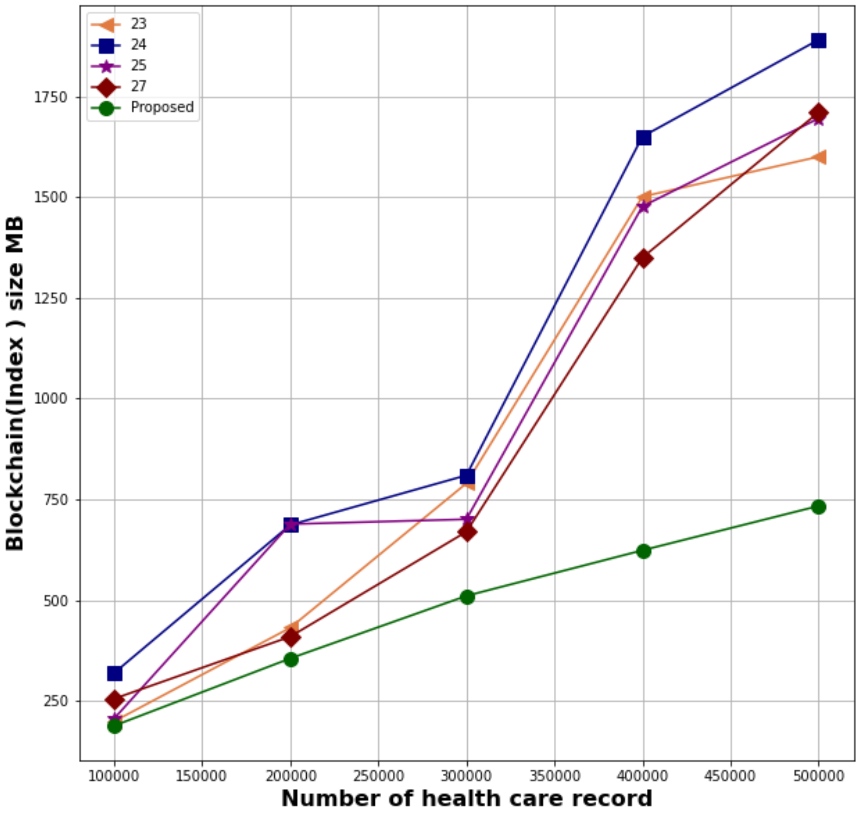


Figure 6. Storage overhead comparisons [23–25,27].

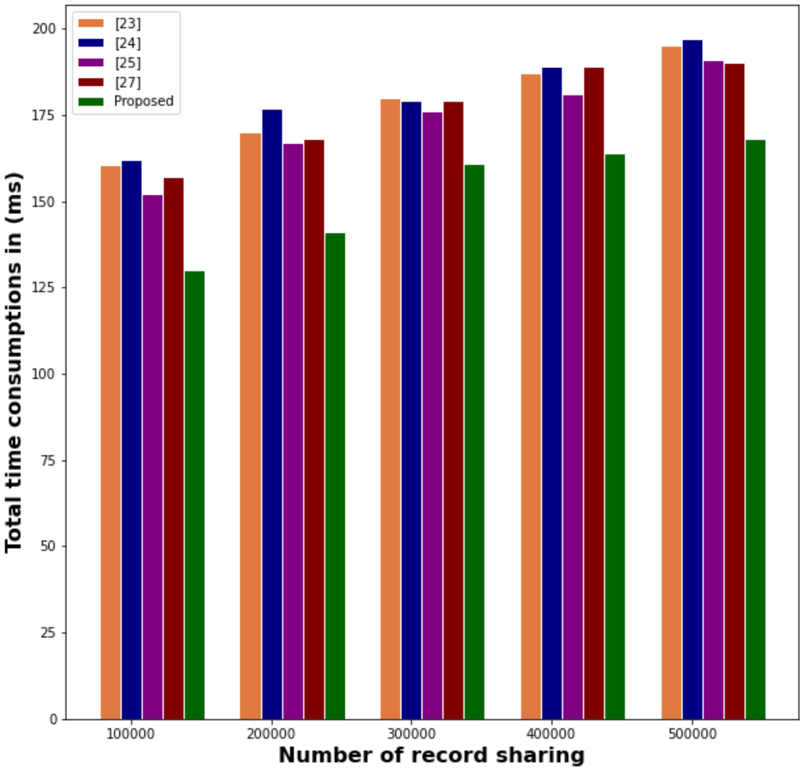


Figure 7. Total time consumption for health record sharing [23–25,27].

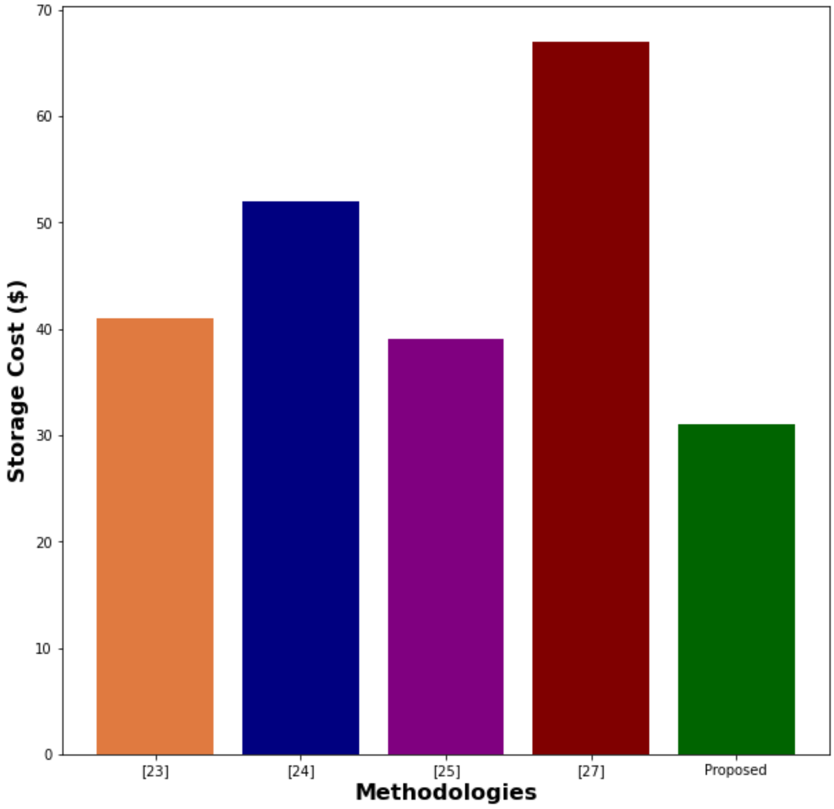
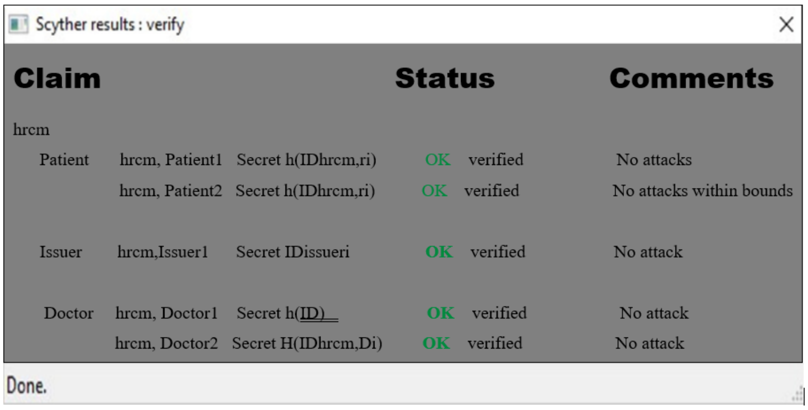


Figure 8. Storage cost analysis [23–25,27].

4.3. Security Investigation of the Proposed Model

In this section, we utilized the Scyther protocol to perform a security analysis and verify its performance against various threats. The use of security protocol analysis tools has gained significant attention in recent years, with Description Language (or SPDL programming language) being a commonly used tool. Scyther examines the protocol under scrutiny against predefined security properties that are also included in the model, enabling validation of the protocol for an unbounded or limited number of sessions. Additionally, it can use a specified role to analyze the protocol by performing a complete execution that demonstrates all aspects of the protocol role. Figure 9 illustrates the security analysis of the Scyther tool.


Scyther results : verify

Claim				Status		Comments
hrcm						
	Patient	hrcm, Patient1	Secret h(IDhrcm,ri)	OK	verified	No attacks
		hrcm, Patient2	Secret h(IDhrcm,ri)	OK	verified	No attacks within bounds
	Issuer	hrcm,Issuer1	Secret IDissueri	OK	verified	No attack
	Doctor	hrcm, Doctor1	Secret h(ID)	OK	verified	No attack
		hrcm, Doctor2	Secret H(IDhrcm,Di)	OK	verified	No attack

Done.

Figure 9. Security analysis of the Scyther tool.

Table 2 compares security attack analyses using various state-of-the-art methods with the current method. It demonstrates that the proposed solution is effective against all cyber-attacks and has forward secrecy and mutual authentication capabilities. However, many existing systems have room for improvement in forward secrecy, session key agreement, and mutual authentication. In healthcare applications, resisting impersonation and replay attacks remains a challenge.

Table 2. Attack analysis.

Methodology	Anonymity	Insider Attack	Healthcare Record Compromising Attack	Offline Password-Guessing Attack	Reply Attack
Huang et al. [23]	×	✓	✓	✓	×
Aruna Sri et al. [24]	✓	×	✓	✓	✓
Yang et al. [25]	✓	✓	×	✓	✓
Tanwar et al. [27]	✓	×	✓	✓	✓
Proposed Method	✓	✓	✓	✓	✓

Goal 1: The proposed protocol uses a two-hash code, which makes it challenging to identify user information in communication channels and protect against dynamic anonymity attacks. However, an uninvolved aggressor may still attempt to determine the characteristics of conveying clients based on their perception of the organization's traffic.

Goal 2: Our approach can tolerate internal intruders and prevent them from changing the content in healthcare record storage devices by using internal access policies.

Goal 3: The proposed protocol uses complicated arithmetic functions in hash code generation, making it challenging for hackers to compromise healthcare records by computing the hash code for a given user within polynomial time.

Goal 4: The proposed medical record-sharing method stores a hash code in the smart card, making it impossible to guess the password of patients and healthcare service providers. The offline password guessing attack is not achievable by the hackers since it is challenging to determine two boundaries simultaneously within polynomial time.

Goal 5: The proposed protocol assigns a unique hash ID and healthcare record session number to each encrypted healthcare record, which eliminates replay attacks. Any attacker attempting to gain access to the medical record present in the cloud using a replay attack will find it challenging since the medical record session-ID is inserted in each record.

Our proposed method can withstand different types of attacks, such as insider attacks, medical record compromising attacks, password guessing attacks, replay attacks and anonymity attacks. As shown in Figure 10, our proposed model has a lower security attack rate than the existing medical record-sharing protocol. Huang et al.'s [23] method has a higher security attack rate in anonymity and replay attack. The proposed method has a lower security attack rate regarding anonymity and replay attacks. Aruna Sri et al.'s [24] model leads to an insider attack if any credentials of healthcare service providers are misused. In Yang et al.'s [25] model, healthcare records can be compromised if the users' details are misused. Our proposed model compromising the healthcare record has a significantly lower rate. So, our approach can be used, especially in healthcare record sharing, in the enterprise environment. Figure 11 depicts the proposed and existing methods performance regarding different security services.

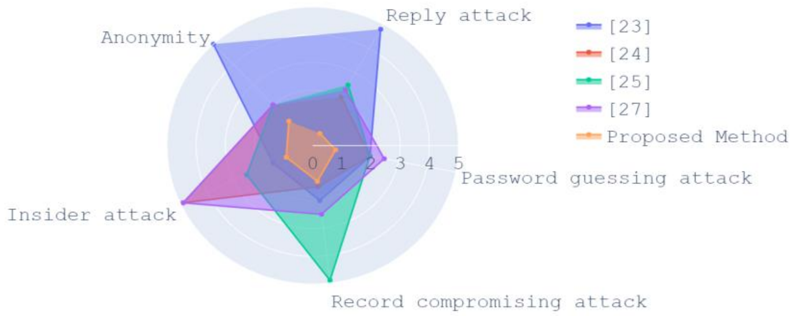


Figure 10. Proposed and existing methods performance in terms of different security attacks [23–25,27].

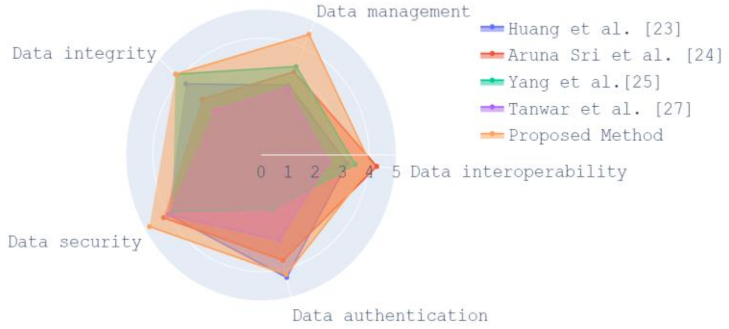


Figure 11. Proposed and existing methods performance in terms of different security services [23–25,27].

5. Conclusions

Our study has identified the security vulnerabilities associated with global medical data sharing and proposed the Health Record Chain for Sharing Medical Data as an efficient solution for enterprise systems. The proposed model for sharing medical records demonstrated efficient performance, taking only 130 ms to share 100,000 records, which is 32 ms faster than traditional methods. The model also exhibited robust resistance to various security attacks, as confirmed by an automated security protocol verification tool. These findings suggest that the proposed model offers a promising solution for secure and efficient sharing of medical records in healthcare systems. The proposed protocol was evaluated for the security of its secret parameters using the Scyther tool and demonstrated better performance than existing methods. These findings indicate that the proposed protocol has the potential to be a promising solution for promoting medical record sharing in the global environment for enterprise systems. The proposed model needs to be tested and validated for scalability with large volumes of medical data. Future research can explore ways to optimize the protocol for handling massive amounts of medical data efficiently. The proposed protocol may face challenges in terms of adoption by healthcare providers and patients. Future research can explore ways to incentivize adoption and encourage widespread use of the protocol. The proposed protocol requires a governance structure to ensure accountability, transparency, and security. Future research can explore ways to establish a governance framework that promotes trust and confidence in the protocol.

Author Contributions: Conceptualization S.V. and P.K.; Methodology, S.V. and P.K.; Software, S.V. and P.K.; Writing—original draft, S.V. and P.K.; Writing—review & editing, S.V., P.K., V.R., M.A. and Y.A.; Validation, S.V., P.K., M.A. and Y.A.; Supervision, V.R.; Resources, M.A. and Y.A.; Visualization, M.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data that support the findings of this study are openly available at https://archive.ics.uci.edu/ml/datasets/nursery (accessed on 14 January 2023).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Guo, R.; Shi, H.; Zhao, Q.; Zheng, D. Secure Attribute-Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems. *IEEE Access* **2018**, *6*, 11676–11686. [CrossRef]
2. Jabarulla, M.Y.; Lee, H.-N. A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications. *Healthcare* **2021**, *9*, 1019. [CrossRef] [PubMed]
3. Ndzimakhwe, M.; Telukdarie, A.; Munien, I.; Vermeulen, A.; Chude-Okonkwo, U.K.; Philbin, S.P. A Framework for User-Focused Electronic Health Record System Leveraging Hyperledger Fabric. *Information* **2023**, *14*, 51. [CrossRef]
4. Kumar, A.; Parihar, A.; Panda, U.; Parihar, D.S. Microfluidics-based point-of-care testing (POCT) devices in dealing with waves of COVID-19 pandemic: The emerging solution. *ACS Appl. Bio Mater.* **2022**, *5*, 2046–2068. [CrossRef]
5. Reen, G.S.; Mohandas, M.; Venkatesan, S. Decentralized patient-centric e-Health record management system using blockchain and IPFS. In Proceedings of the 2019 IEEE Conference on Information and Communication Technology, CICT 2019, Allahabad, India, 6–8 December 2019; pp. 1–7. [CrossRef]
6. Shi, S.; He, D.; Li, L.; Kumar, N.; Khan, M.K.; Choo, K.-K.R. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Comput. Secur.* **2020**, *97*, 101966. [CrossRef]
7. Zou, R.; Lv, X.; Zhao, J. SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. *Inf. Process. Manag.* **2021**, *58*, 102604. [CrossRef]
8. Guimarães, T.; Silva, H.; Peixoto, H.; Santos, M. Modular Blockchain Implementation in Intensive Medicine. *Procedia Comput. Sci.* **2020**, *170*, 1059–1064. [CrossRef]
9. Harshini, V.M.; Danai, S.; Usha, H.R.; Kounte, M.R. Health record management through blockchain technology. In Proceedings of the 2019 3rd ACM International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 1411–1415. [CrossRef]
10. Alexaki, S.; Alexandris, G.; Katos, V.; Petroulakis, N.E. Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions. In Proceedings of the 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, Spain, 17–19 September 2018; pp. 1–6. [CrossRef]
11. Wang, S.; Zhang, D.; Zhang, Y. Blockchain-Based Personal Health Records Sharing Scheme with Data Integrity Verifiable. *IEEE Access* **2019**, *7*, 102887–102901. [CrossRef]
12. Vazirani, A.A.; O'donoghue, O.; Brindley, D.; Meinert, E. Blockchain vehicles for efficient Medical Record management. *Npj Digit. Med.* **2020**, *3*, 1–5. [CrossRef]
13. Rahman, M.S.; Khalil, I.; Arachchige, P.C.M.; Bouras, A.; Yi, X. A novel architecture for tamper proof electronic health record management system using blockchain wrapper. In Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure BSCI, Co-Located with AsiaCCS 2019, New York, NY, USA, 8 July 2019; pp. 97–105. [CrossRef]
14. Wang, J.; Han, K.; Alexandridis, A.; Chen, Z.; Zilic, Z.; Pang, Y.; Jeon, G.; Piccialli, F. A blockchain-based eHealthcare system interoperating with WBANs. *Futur. Gener. Comput. Syst.* **2020**, *110*, 675–685. [CrossRef]
15. Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F.-Y. Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 942–950. [CrossRef]
16. Wang, Z.; Luo, N.; Zhou, P. GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network-enabled anomaly detection in smart healthcare. *J. Parallel Distrib. Comput.* **2020**, *142*, 1–12. [CrossRef]
17. Zhao, H.; Bai, P.; Peng, Y.; Xu, R. Efficient key management scheme for health blockchain. *CAAI Trans. Intell. Technol.* **2018**, *3*, 114–118. [CrossRef]
18. Shamshad, S.; Minahil; Mahmood, K.; Kumari, S.; Chen, C.-M. A secure blockchain-based e-health records storage and sharing scheme. *J. Inf. Secur. Appl.* **2020**, *55*, 102590. [CrossRef]
19. Rajput, A.R.; Li, Q.; Ahvanooey, M.T.; Masood, I. EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain. *IEEE Access* **2019**, *7*, 84304–84317. [CrossRef]
20. Xu, J.; Xue, K.; Li, S.; Tian, H.; Hong, J.; Hong, P.; Yu, N. Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. *IEEE Internet Things J.* **2019**, *6*, 8770–8781. [CrossRef]
21. Chen, L.; Lee, W.-K.; Chang, C.-C.; Choo, K.-K.R.; Zhang, N. Blockchain based searchable encryption for electronic health record sharing. *Futur. Gener. Comput. Syst.* **2019**, *95*, 420–429. [CrossRef]
22. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]
23. Huang, J.; Qi, Y.W.; Asghar, M.R.; Meads, A.; Tu, Y.-C. MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data. In Proceedings of the 2019 18th 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, 5–8 August 2019; pp. 594–601. [CrossRef]
24. Aruna Sri, P.A.; Bhaskari, D.L. Blockchain technology for secure medical data sharing using consensus mechanism. *Mater. Today Proc.* **2020**. [CrossRef]
25. Yang, J.-J.; Li, J.-Q.; Niu, Y. A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Futur. Gener. Comput. Syst.* **2015**, *43*, 74–86. [CrossRef]
26. Roehrs, A.; da Costa, C.A.; da Rosa Righi, R.; da Silva, V.F.; Goldim, J.R.; Schmidt, D.C. Analyzing the performance of a blockchain-based personal health record implementation. *J. Biomed. Inform.* **2019**, *92*, 103140. [CrossRef] [PubMed]

27. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2020**, *50*, 102407. [CrossRef]
28. Sreenu, M.; Gupta, N.; Jatoth, C.; Saad, A.; Alharbi, A.; Nkenyereye, L. Blockchain based secure and reliable Cyber Physical ecosystem for vaccine supply chain. *Comput. Commun.* **2022**, *191*, 173–183. [CrossRef]
29. Butt, G.Q.; Sayed, T.A.; Riaz, R.; Rizvi, S.S.; Paul, A. Secure healthcare record sharing mechanism with blockchain. *Appl. Sci.* **2022**, *12*, 2307. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.