Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9185731, 14 pages
https://doi.org/10.1155/2022/9185731

Research Article

On the Internet of Things, Blockchain Technology for Supply Chain Management (IoT)

Viresh Sharma,[1] Edwin Ramirez-Asis,[2] Aamir Junaid Ahmad,[3] Miguel Silva-Zapata,[4] Joseph Alvarado-Tolentino,[4] Harish Kumar,[5] and Daniel Krah[6]

[1]*Department of Mathematics, N.A.S. (P.G.) College, Meerut, India*
[2]*Faculty of Business Sciences, Universidad Señor de Sipán, Chiclayo, Peru*
[3]*Department of Computer Science and Engineering, Maulana Azad College of Engineering and Technology, Patna, Bihar, India*
[4]*Academic Department of Computer and Systems Engineering, Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Peru*
[5]*Department of Computer Science, College of Computer Science, King Khalid University, Abha, Saudi Arabia*
[6]*Tamale Technical University, Ghana*

Correspondence should be addressed to Daniel Krah; dkrah@tatu.edu.gh

Received 3 March 2022; Revised 6 April 2022; Accepted 13 April 2022; Published 10 May 2022

Academic Editor: Kalidoss Rajakani

Patient's medical records are now accessible from anywhere and at any time, thanks to the Internet and the changes it has wrought in the healthcare industry. Electronic health records were dogged by a lack of standards, but that was not the only issue. Decentralized online ledgers were already being proposed and used to solve interoperability and privacy issues when blockchain-based systems were first built. As far as technical issues go, scaling, usability, and accessibility stand out. On the one hand, it is difficult to keep secure access control measures on-chain while simultaneously keeping a wide range of medical data off-chain. Finding out who owns what and spreading access control of data is the second challenge in medical settings. Using temporal blockchain, the Secured Healthcare System (SHS) aims to address these problems (TB). As an SHS fundamental building piece, the context-based Merkle tree emphasizes privacy, enhanced integrity management, and access control methods (CBMT). For interoperability and scale control, the framework uses temporal features, HL7 criteria, and IPFS data management (IPFS). Personalized micro booklet (PML) security was found to be affected by the SHS framework, namely, on the time-based shadow notions and the contextual components of the PML (PML). Taking advantage of the architecture's enormous potential to solve the challenges of siloed data and enabling tamper-proof, secure healthcare transaction has been sought.

1. Introduction

A massive amount of health data is generated on a daily basis, and this volume continues to grow. It is challenging for healthcare practitioners to interact efficiently since the health information about each patient is distributed among a number of different organizations. Maintaining the security and privacy of a large amount of health information is a tough undertaking, particularly in today's society [1]. The problem of interoperability across numerous service providers is one that is difficult to resolve. The recovery of information and the interchange of health data may become much more difficult for patients and suppliers if monetary incentives are utilized to encourage the blocking of health information. Current technology maintains the patient's health record in a cloud-based storage system that is accessible from anywhere. Companies such as Amazon and Microsoft are using a centralized cloud to operate their operations.

Even while cloud computing offers several advantages, protecting and managing personal information is a challenging task, particularly when dealing with sensitive information such as electronic health records. Each and every individual is responsible for ensuring that a patient's electronic health record is maintained secure and private. With

a centralized cloud, privacy and security are two of the most important issues to consider.

The decentralized nature of the cloud reduces the security risks that might otherwise arise in a centralized cloud environment. There are a vast number of nodes hosting the information, which is stored in a decentralized directory that is not controlled by a single body. Increasing the amount of money spent on the storage of health information is not essential. Story, Maid Safe, File Currency, Sia coin, and other decentralized cloud systems, as well as other decentralized cloud systems, have been used to store health data [2] and other types of data. Hundreds of decentralized online books have been created to address issues like interoperability and privacy, as well as scalability, integrity, usability, and accessibility in decentralized online environments. Some of the more notable ones are as follows: one of the first challenges that the healthcare system will face is the preservation of various types of medical information, including text, video, and picture, among others, that are currently stored off-chain but will be made available in the future securely via the blockchain, such as patient records and prescriptions. Maintaining compliance with a myriad of standards while exchanging health information across many providers is the most challenging component of the process. A protocol called HL7, which is often used for sharing text files between various providers, is used in order to exchange image data between suppliers and the DICOM standard.

In the healthcare system, the first challenge is that diverse forms of medical information, such as text, video, and image, among other things, are preserved outside the chain of custody so that they may be accessed safely at a later time. Compliance with a range of standards when exchanging health data across many providers [3] is the most challenging challenge to overcome. The HL7 standard is used for the transmission of image files between healthcare providers, while the DICOM standard is utilized for the transfer of text data between healthcare organizations.

A secure e-health architecture (Sefira) is proposed in this study, which combines a progressive temporal blockchain in order to address the difficulties outlined before. This paradigm placed a strong focus on the validity and integrity of electronic health records as its central theme. In particular, the architecture is intended to preserve the electronic health record without requiring the participation of a third party. In the healthcare industry, the blockchain is used to verify the legitimacy and integrity of patient information, as well as to prevent fraud and identity theft. Sefira's most essential components are the context-based Merkle tree (CBMT) and the context-based access control (CBAC) of a Smart Contract, which are both implemented in Java. Smart Contracts have been developed to include the first of them, which is a decentralized network of electronic health data as well as information on access limitations.

As the industry continues to evolve at a rapid rate, blockchain adoption is gaining significant traction.

Many firms have begun to develop use cases, and there has been a large increase in investment in blockchain-related ventures. Although blockchain is still in the early stages of development in terms of technical maturity, the number of unique experimental adoptions and customizations is increasing all the time. Blockchain has the potential to displace an established technology and shake up the industry, or it has the potential to be a ground-breaking product that creates a completely new industry, and initial trends with the rise of cryptocurrencies have signaled that blockchain has the potential to be disruptive for the banking and financial services industries.

By removing the need to pay fees for using credit or debit cards, cryptocurrency has the potential to destabilize a centralized banking system and disrupt financial markets.

2. Related Work

The majority of the research in question suggests that a blockchain-based health architecture should be implemented. The study focuses on the integration and interoperability of electronic health records (EHRs) using blockchain technology.

Medrek is a blockchain-based decentralized healthcare system that was developed in the United Kingdom. When dealing with sensitive information, confidentiality, authentication, and data exchange are essential components. Some individuals, such as public health organizations and scientists, rely on these factors. It might perform the role of a miner, granting access to anonymized data. The notion proof is used by the Medrek [4]. In order to retain health information and a medical prototype, Medrek used the Ethereum blockchain.

Patient-centered healthcare saves money by cutting out the middleman [5]. Decentralized system that also ensures data security is what blockchain is all about! Patentor is a way for creating a patient-centered health record. The patentor Smart Contract allows you to define access privileges depending on your position. The key concerns of the patient are the integrity and interoperability of the system. Blockchain ensures that HIPAA laws and standards are followed and that they are compatible with one another.

Medi chain is a type of consensus based on evidence of labour performed in a secure environment [6]. It is a patient-centric data management system that is utilized in both the mobile app and the standard web browser, according to the company. The Linux Foundation is responsible for the upkeep of the hyperbook, which contains the health information. The RBAC-SC is primarily concerned with providing access services that are dependent on the duties of other organizations [7]. It performs checks with various authorities by using attribute-based encryption [8].

A blockchain-based exchange of health information, Blochian, is a platform that maintains a wide range of medical data [9]. Because of the mix of off-chain and on-chain checks, the system is more secure and authenticated. The blockchain contains electronic medical data, as well as personal medical records for each individual.

The primary flaw with older systems is that hackers attempt to learn the input value by providing varied input data and predicting the most probable hash result from that data. Because of the weak hash function, the collection conspires against the time of the hash chain, and it has been shown to

be a limitation on the states of the hash chains that have been authorized as cooperative evidence as a result of this.

2.1. Blockchain-Based Healthcare Organization. The quality of healthcare services varies greatly from country to country. The majority of countries do not have public services, but some do have privatized services and others do not have open access to intellectual property. These disparities highlight the difficulty of delivering healthcare to a large number of individuals. In the healthcare industry, security is a crucial issue to deal with. The use of the blockchain to protect the safety and confidentiality of critical medical information is becoming more popular. Between 2009 and 2017, a total of more than 176 million patient data were stolen [10]. The firms believe that distributed ledger technologies (DLTs) are the only method of resolving issues with medical information. Due to the fact that blockchain may be utilized as an interoperability or traditional layer, it might be beneficial for communication between systems of various types.

The blockchain is being used by the firms listed below to assist in the transformation of the management of patient data and electronic health record systems. Despite the enormous potential of blockchain technology to expand and improve the value of the healthcare system, just a few firms have begun researching it. The healthcare framework is still being developed by the majority of firms. Some organizations concentrated on patient centricity, while others concentrated on traceability of drugs, billing methods, and other aspects of business operations. The many firms each concentrated on a certain procedure. The majority of the company's healthcare infrastructure is only a prototype that was never put into operation in the real world of healthcare. In terms of interoperability, the most important consideration is that the blockchain hash must be compatible with the prior system. Blockchain healthcare startups such as Guard Time, Medrek, Roomed, Pocketbook, Factor, Stratum, and Tyrion are among the many emerging technologies in the field [11]. Table 1 depicts a high-level overview of the healthcare organization that is built on Blockchain technology.

2.1.1. Medrek. Medrek, a blockchain-based health system that manages information about patients' health, is the most widely used blockchain-based health system. The decentralized Medrek ledger stores all patient information and is utilized by the therapeutic community (doctor), patients, and medical scientists to make decisions about their care.

2.1.2. Stratum. As previously mentioned by Richard Caetano, CEO of Stratum, he aimed to produce a proof of concept in order to conduct clinical trials. Building a safe health system that can be shared across labs, clinicians, and researchers is the goal.

2.1.3. Factor. The primary goal is to build a secure means of storing health data using blockchain technology that is accessible to hospitals and other management personnel. It is possible to connect each patient's health record to a safety chip that contains patient information and allows an authorized person to access the information.

The Estonian company, KSI Blockchain Technology, has a workforce of 150 cryptographers and has developed blockchain technology. The Netherlands, the United States, the United Kingdom, and Singapore are among the countries where the guard works throughout the day. They are partners in the distribution of media and insurance. In 2017, the government of Estonia decided to implement a guard time system to secure the electronic health records of over a million Estonians. The KSI blockchain technology is being used to preserve the electronic health record [12].

2.1.4. Pocketbook. Pocketbook is an API company that provides a blockchain solution based on the Do chain protocol. When it comes to the medical services industry, the Do chain is a transmitted exchange system that operates on money and clinical information. As the hidden record for meeting chip-level blockchain requirements utilizing Intel processors, the firm makes use of the open-source Hyperledger Sawtooth from Intel, which is developed by Intel [13]. The hyperedge transaction is handled via the use of an intelligent contract.

2.1.5. Tyrion. Tyrion made use of blockchain technology in order to safeguard the patient record. Every record, as well as pharmaceuticals with an approved history of ownership, is stored in this system. The organization makes use of time signatures and credentials to ensure that the whole system runs smoothly.

2.1.6. Roomed. Roomed is a platform that blends artificial intelligence and blockchain technology to deliver health services to patients. The company gathers patient information using chatbots, wearable analytical devices, and telemedicine and then distributes that information to the health team as needed (Roomed, 2018). The Smart Contract contains information on the patient as well as access privileges.

Table 1 provides an overview of the blockchain-based healthcare organization, which is described as follows.

3. Secure Framework (Sefira) for Healthcare System

One of the primary features of the Sefira proposal framework is the use of a General Public Ledger (GPL), Personalized Micro Ledger (PML), Smart Contract, and Context Access Control (CBAC). It is possible to verify the legitimacy of a transaction using the Temporal Hash Signature (THS), which is accomplished by running the hash function and comparing the results with those stored in the blockchain. Last but not least, the root hash value on the blockchain is preserved. There are two critical components to the proposed Sefira architecture: the THS and a progressive temporal blockchain. The THS is the first of these components, and the progressive temporal blockchain is the second [14]. The Sefira framework is shown in Figure 1, which describes its operation. The mining mechanism utilized in the blockchain is processed, and the anonymized data is then used by medical researchers to compensate the blockchain storage provider for their efforts. When using standard blockchain, the most difficult obstacles are to link the hash chain to its

Table 1: Summary of blockchain-based healthcare organization.

S. no	Company	Discussion
1	Medrek	MIT project–give patients the control over their data
2	Stratum	French startup–trust panning from data falsification
1	Factor	Blockchain-based authenticity medical billing process
4	Guard time	Instant medical access, insurance
5	Pocketbook	Identity and payment optimization in the healthcare system
6	Tyrion	Global blockchain platform company with Philips's health
7	Roomed	Russian blockchain company–share the health information between providers

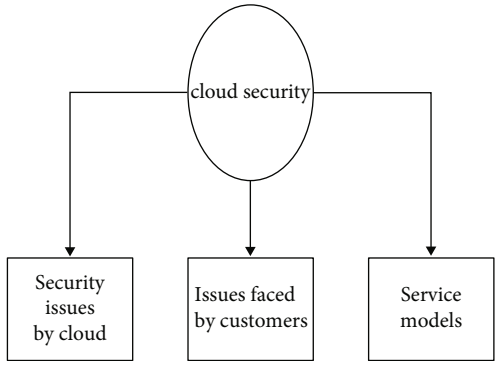

Figure 1: Secure framework (Sefira) for healthcare system.

form, and the second is a powerful hash function, which challenges to know the input value but assaults to examine the input model and test with any data in order to try to decipher the contents [15]. Both of these disadvantages are addressed by the progressive temporal blockchain (PTB). The system model of the proposed work is described in the next section.

3.1. Functionality of Sefira Framework. Because supply chain management encompasses both internal and external actors, accurate and timely information transmission is required in order to achieve increased performance in supply chain management systems.

The supply chain is the process of transporting a product from a supplier to a client, and it necessitates the proper coordination of human and mechanical input. Supply chains must increase end-to-end visibility, product tracking, fraud, regulatory compliance, delivery speed, and settlements in order to be more competitive and profitable.

It is possible to automate business rules associated with transaction processing in the supply chain by using a Smart Contract. Any collection of rules, logics, and decision criteria expressed in a programming language may be included in a Smart Contract. For example, a contract can conduct cash transfers when particular events occur (for example, the payment of a security amount in an escrow system). Because of this, Smart Contracts can be used in a variety of applications, including financial processes (such as subcurrencies, financial derivatives, savings wallets, and wills) and self-enforcing or self-directed governance applications (such as outsourced computation).

A Smart Contract is identified by an address, and the source code for the contract is maintained on a blockchain as well. Users may activate a Smart Contract by sending transactions to the contract address provided by the Smart Contract.

To be more specific, if a new transaction directed towards a Smart Contract address is recognized by the blockchain, then all participants in the mining network run the contract source code with the current state of the blockchain and the transaction payloads as inputs.

By engaging in a consensus process, the network comes to an agreement on the output and the next state of the contract, and the contract is completed. Blockchain technology, such as Ethereum, is becoming increasingly popular because it includes a full-featured Turing-complete programming language that can be used to create "contracts" that can be used to encode any arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others we have not even thought of yet, by simply writing up the logic in a few lines of code.

Although blockchain offers many exciting advantages, each use case must modify blockchain systems to meet their individual requirements in order to get the desired outcomes. For the purpose of developing a true business case, extensive research is necessary to understand the business needs of a use case as well as a cost-benefit 24 analysis. As a result, given the characteristics of this growing technology and its capacity to improve supply chain operations, there are significant exploratory possibilities to make a contribution to it. In fact, blockchain has the potential to solve supply chain difficulties because of the properties described below.

In addition, the blockchain's auditability feature may give a complete audit trail of data across the supply chain, allowing event monitoring to be performed in order to assure traceability throughout the supply chain.

Blockchain's immutability qualities may give a single time-stamped tamper-proof source of data, which can aid in the preservation of evidence of regulatory condition compliance, which is necessary to assure compliance in a supply chain.

Smart Contract: the blockchain's Smart Contract feature allows for real-time rule-based verification of multiparty confirmations, which allows for cost-effective adaptability to changes in the business environment, hence ensuring supply chain flexibility.

Stakeholder management is ensured by the use of distributed ledger technology, which enables direct connection with

a trusted digital signature-based peer-to-peer network, which reduces risk and builds confidence in the supply chain.

Despite the fact that blockchain usage in the supply chain is on the increase, it must be overlooked that the industry's acceptance of blockchain is still in its early stages. The extent to which benefits are realized must be assessed in order to guarantee that blockchain adoption and firm performance are in sync. The following are some of the possible roadblocks identified by the researchers.

Standardization of blockchain networks: blockchain networks are becoming more standardized. The high rate of development and adoption of blockchain applications by businesses across a wide range of sectors is posing hurdles to the process of standardizing blockchain technology. Within an industry, there is the possibility for several blockchain networks to be formed for the purpose of a particular application.

The number of blockchain applications is growing at an alarming rate, which will cause the standardization process to be delayed. Accordingly, the predicted benefit realization from blockchain adoption will be limited.

Latency: blockchain networks are well-known for being quick; nonetheless, it is necessary to analyze the performance of a blockchain network throughout the course of a transaction's lifespan. If transaction cycle durations are reasonable, this will result in the construction of a solid business case.

Companies may not be used to exchanging data throughout their supply chain with their partners, which may provide a challenge to collaborative efforts. To establish the requirements for Smart Contracts, all parties must participate to the process.

Data interoperability: the structure, format, and meaning of the data that each organization exchanges will have been agreed upon by the participating companies. Additionally, businesses will have to decide what information they are willing to share with others in the network and what information they want to keep private.

HL7 (seven international health levels) is a collection of principles, forms, and standards that are used to produce electronic health records in the area of electronic health records (also known as electronic medical records) (EHR). The World Health Organization established the HL7 principles and declared them to be the information technology standard for medical services as well as the recognized information technology model for human services. Although the HL7 standard was first developed in 1987, it was not formally recognized until 1994 by the American National Standards Institute. By giving instructions on how to use its standards, HL7 helps to the supply of worldwide interoperability in information technology-based healthcare. The number "7" refers to the seventh layer of the Reference Model for Open Systems Interconnections (RMOSI), which is defined as follows: OSI. Medical message interchange, decision-making, rule syntax, and the standard definition of health data and clinical records are all covered in detail in Health Level 7 (HL7) counselling resources. The HL7 guideline materials are accessible for download on the Internet.

In order to transmit an electronic health record between two healthcare providers, the HL7 standard must be used. HL7 is an international standard that is used by a wide range of healthcare providers to transport health information between software programmers and between hospitals and other healthcare facilities [16]. Specifically, it accomplishes so through making use of the healthcare system, which offers the necessary skills, norms, and standards. Resource exchange standards are among the several HL7 standards that are in use, the most notable of which being the Fast Healthcare Interoperability Resources (FHIR) standard. Figure 2 depicts an example lab report that was prepared in HL7 format for a specific patient, and Figure 3 depicts the same report in a different format.

Step by step development of blockchain-based systems is represented by a systematic design method for blockchain application development. A good grasp of business processes and compliance requirements of the use case is required throughout the procedure in order to enable decision-making throughout the procedure.

Beginning with the decision on whether to decentralize trust (authority) or not, the method proceeds to the next step.

A blockchain is more appropriate in situations where there is no need for a single trusted authority and when the dependable authority may be dispersed or partly distributed. If trust authority may be spread, then it is necessary to define the rules and specifications that govern trust authority distribution.

Aside from that, blockchain is not necessary, and solutions may be developed using standard databases instead. Because of the limitations of blockchains, the arrangement of processing and data storage between on-chain and off-chain components is of significant importance to the overall success of the system. All of this is dependent on the business needs and number of transactions for a particular use case when determining the storage and compute infrastructure necessary for a blockchain application. In Figure 2, it is necessary to do a detailed evaluation of the workload and capacity requirements. In order to predict storage and computation requirements for a use case, capacity planning is necessary.

A supply chain is made up of a variety of separate businesses that connect one end point to the other end point. Forgery is a possibility with these contract documents. When it comes to supply chain systems, one of the most pressing problems is the traceability of changing data.

The cost of current blockchain solutions is prohibitively expensive when compared to conventional database management systems, which makes them unsuitable for business usage. Many academics have pointed to this as a potential study area; however, we have not discovered any answers in the current literature in this subject.

(i) Current systems rely on faith in the human beings who are engaged in the functioning of the supply chain system; this reliance on trust must be removed

It is widely acknowledged that supply chain systems need technological transformation in order to foster confidence in the system while also providing the capacity to track down any changes that have occurred in transactional data. Despite the fact that it is impossible to cover the entire spectrum of potential blockchain applications in the supply chain management industry for the purpose of illustrating

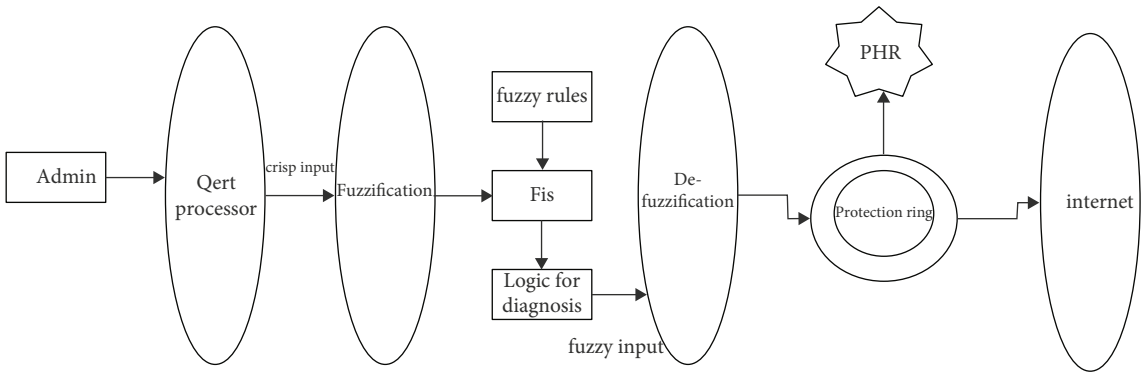

Figure 2: Sample HL7 patient record.

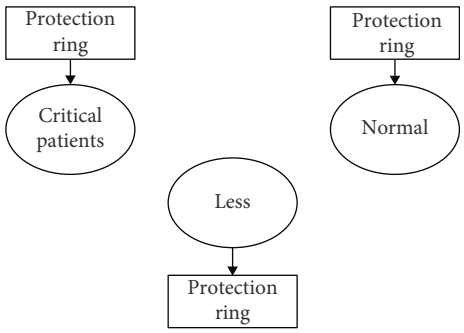

Figure 3: File sharing in IPFS.

the usefulness of blockchain, due to the fact that the applications are countless, we have chosen one specific application use case to test and demonstrate our findings.

3.2. Interplanetary File System. It is a peer-to-peer distributed file system that connects all of the other peer systems by establishing links with them. IPFS, as seen in Figure 3, is a content-addressable network that also includes distributed file storage and data interchange capabilities. Each item in the database is represented by a hash value, which is stored in the database. Additionally, it moves data inside the Git repository while also eliminating data redundancy with the help of the BitTorrent swarm by deleting redundant data from the repository.

Each record is identified by a unique fingerprint known as a cryptographic hash. It provides quick speed as well as decentralized archiving, with each file having a human-readable name (IPNS) assigned by the system. Ram, for example, might want to share a file with his friend Sam. Ram transfers the data to the IPFS storage system. The file will be deployed in the current working directory after that. After that, a hash value is created, which always begins with the letter Qi. The data has now been made accessible to the rest of the network. By using the hash value, Sam will be able to get access to the file. Rather of downloading from a central server or a single server, use a cloud-based service. A route from a distributed server may be provided by a peer. The Merkle DAG is used to establish a link between nodes in IPFS using hashes as a means of connecting them together (directed acyclic graph). The following are the benefits of using Merkle DAG to prune your trees [17].

(i) Content Addressing. Each record has a unique hash identifier

(ii) No Duplication. Each file is stored only once and cannot copy

(iii) Carefully Designed. Data has confirmed with it is a checksum, so if there is any change, then IPFS knows the data is modified

An example of a decentralized application (dApp) is a set of apps that work together to produce the desired results. The problem of centralized storage is solved by decentralized storage, which is data that is stored in a dispersed manner. When using IPFS, the material is sent from the closest peers who have a replica of the substance, reducing the burden on the single hub and increasing the user experience. Furthermore, IPFS considers constant and smooth perusing of the material, regardless of whether or not the owner of the substance is still present for consultation. The IPFS output presented in Figure 4 is an example of sample output.

3.3. Progressive Temporal Blockchain. To reach the last transaction in a progressive temporal blockchain, each transaction must rely on the subsequent next transaction in order to be successful. In order to make the transaction more secure, it produces a temporal shadow and an active hash function, which prevents hackers from determining the hash value by providing alternative input data. Before attaching the hash value to each record, the temporal shadow is appended to each record. Before hashing the transaction and adding the height of the subtree to the concatenated hash value from the child node, the length of the hash chain is approved before hashing and then hashing the transaction again. Each transaction is validated with the use of a signature on the document. The Temporal Hash Signature (THS) is utilized in this case to authenticate the user without the involvement of a third party. The presence of breaches may be recognized nearly immediately if the monitor signature changes [18].

3.4. Temporal Shadow. Allen makes the argument that there is a temporal relationship between the two incidents. When

Figure 4: Sample output of IPFS.

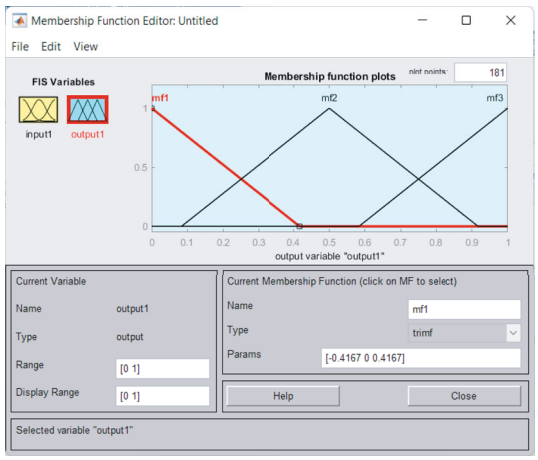

Figure 5: Layer input.

looking at the interval x and y, Allen refers to Figure 5, which shows the seven essential temporal relationships. Depending on the previous transaction, the potential sample relations of each transaction rely on the previous transaction, or the current transaction is required to start the next transaction, or two transactions might start at the same time, depending on the previous transaction.

To increase the security of a transaction in the Sefira framework, the temporal shadow is deployed. The three parameters of a nonce, the hash value of the preceding transaction, and the timestamp are used to evaluate each transaction in this context. It is dependent on the following successive transaction to complete the last transaction in order to be successful. Time-related characteristics are attached to each transaction. Time-related properties were the focus of the temporal shadow, which was cast on them. Each transaction in temporal shadow should have a timestamp applied to it, and temporal shadow should add the timestamp after attaching the hash value. The nonce value, Personalized Micro Ledger (PML) root value, and timestamp serve as the temporal shadow for the General Public Ledger (GPL). For the temporal shadow to be calculated, the PML takes into account the random number, the timestamp, and the preceding hash value. With the help of the progressive temporal blockchain, it is possible to prove the validity, integrity, and authenticity of electronic information. Figure 5 represents Allen relation.

3.5. Context-Based Merkle Tree (CBMT). The temporal shadow and progressive temporal blockchain were used to increase the security of the system. When it comes to the Sefira framework, two ledgers are maintained: one is called the General Public Ledger (GPL), and the other is called the Personalized Micro Ledger (PML) (PML). In order to aggregate all of the transactions occurring at a certain moment, the context-based Merkle tree (CBMT) is employed. The context indicates that it is dependent on the time, the place, and the identity of the speaker. Before hashing, the height of the subtree is attached to the concatenated hash value from the child node, which represents the height of the subtree.

Each and every patient transaction is recorded in the General Public Ledger (GPL). Temporal shadow, root value, and current transaction are the three components that make up the GPL. The context-based Merkle tree (CBMT) is used to ensure that the data is kept in its original form. The Merkle tree was first presented in 1979 by Ralph Merkle. In the GPL, each patient transaction is regarded to be a leaf node. Each patient transaction is saved in the block for the duration of the block's existence. Each nonleafy node is represented by a hash value of its own. The temporal shadow is attached to each transaction's hash value before it is generated and stored in the database. Before attaching the hash value to each record, the temporal shadow is appended to each record. For each transaction, the height of the subtree was appended to the concatenated hash value from the child node before hashing, and then the length of the hash chain was accepted prior to having the hash value computed. The Temporal Hash Signature (THS) infrastructure is created and confirmed without the involvement of third parties that are considered trustworthy [19]. Algorithm 1 represents the context-based Merkle tree.

3.6. Personalized Micro Ledger (PML). The Personalized Micro Ledger (PML) is a system that keeps track of each patient's individual transactions [20]. It keeps track of the subactivity that is responsible for keeping track of the health record in this ledger. Each subactivity has its own hash value, which is then combined to make a tree. The temporal shadow utilized in the PML is a kind of shadow. The generation of a temporal shadow is predicated on the time when the transaction was created [21]. This ledger is solely responsible for the maintenance of subactivity in health records such as subdata (di), nonce (n), and temporal shadow (ts). For example, the patient is suffering from health problems and has sought therapy in a hospital. A prescription is issued by the doctor, and this transaction is dependent on a number of sub transactions. The first step is to register your personal information, which is a subtransaction [22]. The next step is to schedule an appointment, which is another subtransaction. The next step is to make a payment, which is still another transaction. A PML is formed by aggregating all of the subtransactions together. The root value of the PML was provided as input for the final transaction, which is stored in the General Public Ledger (GPL).

3.7. Layers of Context-Based Merkle Tree (CBMT). Three layers were maintained to generate the Merkle tree like registry layer, linker layer, and root layer. The first layer is the registry layer, which initiates the registration request. Figure 6 represents the layers of the Merkle tree [23] .

An upper-level layer is notified by receiving the hash value of a transaction and forwarding the hash value to a registry [24]. It is the responsibility of the registry to link

Input: patient record z_i; patient public key Pa_k;
patient private key Pk_s; Doctor keys $po_{d,}$ po_{ds};
i_n nonce; st_{ir} temporal shadow; this Temporal Hash Signature (THS);
height of the tree l_i; sub activity hash value i_s; p_{romote} sub activity root value;
Output: Transaction deployed in the blockchain
Begin:
Step1: for (i1; i < n; i++)
p_iSig((ps_{dk}) encrypt(rec_i,pk_{pk})) //Doctor encrypt the record p_i $r_i$hash(p_i)
Step 2: ts_ihash(t_i&&n_i&&p_{rooti}) //Registry server receives the hash of records and forwards it to the linker server.
$y_i$hash(s_i&&ts_i&&l_i)
General ledger $z_i$hash(r_i&&ts_i&&l_i)
Step 1: Linker convert the hash of value into trees and forward to the next higher-level server
$z_i$hash(r_i && ts_i && l_i)
Step 4: Root hash value stored in the Calendar database.
$calZ_{root}$
Step 5: The patient set access privilege in the Smart Contract.
Step 6: The bytecode of a Smart Contract deployed in the blockchain.
Step 7: Finally it is stored in the blockchain, and the signature token sent patient -> ths_i
End for
End

Algorithm 1: Context-based Merkle tree (CBMT).

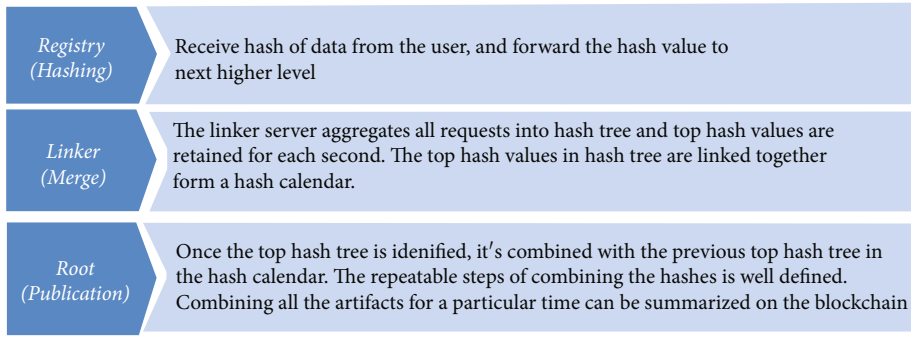

Figure 6: Layers of context-based Merkle tree (CBMT).

the hashes of transactions and pass the information to the next level linker.

Finally, the root hash value contains the top hash value that was previously saved in the root hash value. Temporal Hash Signature (THS) is a digital signature that is produced and delivered to the registry through an aggregator. These are the three layers of the Merkle tree that are seen in Figure 6 [25].

3.7.1. Registry. The end-user submits the hash of data to the registry, which then connects the hash of data and transfers it to a higher level of hierarchy in the organization. Each patient's health information is hashed using the SHA256 technique, and the hash result is sent to a higher tier of the system for processing [26].

3.7.2. Linker. The linker layer gets the hash value from the lower level layer and creates a connection between the hash of value and the original value. The signature token is generated without the need of any keys in this case. The hash value is sent to the parent node by the approved child node and stored in the parent node [27]. The linker creates a connection between all of the hash values entered by the user. The same procedure was followed again and again until the final result was obtained.

3.7.3. Root Layer (Also Known as the Root Layer of a Tree). The linker layer gets the hash value from the aggregator, as well as all of the root values from the subtree aggregate, and stores them in the root layer of the tree structure. The temporal shadow that is created for each transaction is done so without the assistance of trustworthy third parties [28]. It is possible to produce Temporal Hash Signatures (THS) for authentication reasons and have them validated without the requirement for trusted third parties.

3.8. Temporal Hash Signature (THS). The suggested works are designed to address the shortcomings of the current

work. The rationale for using the Temporal Hash Signature (THS) is that it ensures correct authentication when accessing an eHealth record. The authorized user must use the THS token to authenticate himself or herself. It is necessary for a patient to properly save the THS token in order to get access to their health record, and a doctor may access the patient's information after they have received the signature token from the user [29]. In previous systems, the doctor must remember a specific THS in order to access the patient record; however, in the proposed work, the doctor may access any record simply by providing the most recent THS to the system.

The Smart Contract keeps track of all signatures; all it does is compare the most recent hash signature to the most valuable hash signature, and if the hash signatures match, it grants access to the record, with the privileges being verified in the Smart Contract. Despite the fact that the user possesses the THS, privilege is checked in the Smart Contract because, regrettably, a hacker may get the THS but not the privilege to access the record and, as a result, could not access the record if the privilege was not checked [30].

3.9. Context-Based Access Control (CBAC) in Smart Contract. Each record has its own temporal context tag, which makes it easier to find information. By using the temporal context tag, health records may be retrieved by specifying a specific time period such as a year, month, week, or day. In the next step, the access privileges for each patient record are defined in a Smart Contract. Depending on the privileges assigned by the Smart Contract, the authorized user is granted access to the eHealth data set out. The CBMT Smart Contract is maintained on the blockchain in progressive temporal time. The CBAC in Smart Contract is responsible for maintaining four contracts, including a patient contract, patient history, an insurance contract, and a billing contract, among other things. They will not be able to modify a contract after it has been recorded on the blockchain. This method of access is quick, low-cost, and highly secure. In this case, access restriction is not only determined by the user's credentials but also by the time and place of the event.

3.10. Layered Architecture of SHS. The suggested approach consists of four levels, each of which is utilized to transfer data among various service providers via the usage of blockchain technology. The layers are divided into four categories: the application layer, the query layer, the data provenance layer, and the database layer. The SHS system is divided into layers, as seen in Figure 7. The secure system is implemented using JavaScript. The user can enter the details and also retrieve the data from the system for research or another purpose. In the posed system, the user is doctors, patients, billing, insurance, nurses, lab technician, etc. Each user accesses the data for different purposes. This layer mainly used as a communication interface between user and application. Figure 7 represents the layer.

In the IPFS, each patient record is encrypted using the RSA technique and kept in a secure location. The hash value that was created was submitted to the blockchain, which allowed for safe access control to the record to be established. The benefit of using IPFS is that it may store any kind of data, including text, images, videos, and other types of media. However, in the proposed work, we will just examine text files.

3.10.1. Query Layer (Also Known as the Query Layer). The user wishes to access data from the database, and as a result, the user sends a series of queries to the system, which the system then executes. The query layer's principal function is to accept a request from the user and to respond to the request by sending the result to the user. Automatically occurring conditions enable the user to either see or prohibit access to a certain record based on their existence. This is referred to as a Temporal Hash Signature since the public key is the same for every patient who created the transaction at a certain time, while the private key is distinct for each transaction, as opposed to a digital signature (THS). The Smart Contract contains all of the keys that are needed. If a user requests access to data, the Smart Contract verifies that the user is who he or she claims to be with the aid of keys and privileges.

It enables users to have access to information stored in an existing database. The Smart Contract was created in order to describe the rights. Each transaction is indexed in the Smart Contract and safely kept on the blockchain, which is a distributed ledger. Each result is delivered to all of the nodes that are dispersed. This layer is in charge of validating each user request and sending the response to the user who has successfully authenticated. The information should be shared primarily inside the network, so that anybody who has the appropriate privileges may view the record. The procedures must be followed while processing patient records.

The patient records are produced and kept on a distributed network with thousands of nodes, which allows for greater efficiency. The blockchain contains the hash value of the patient's identification. Because each file is tied to the previous hash value, it is difficult to change the patient's record by altering the hash value. In addition to the generalised public ledger (GPL), it also maintains the Personalized Micro Ledger (PML) (PML). GPL maintains all patient health records, and each file is connected to the one that came before it in order to protect the integrity of the electronic health records system. The PML, on the other hand, has the customized patient record, which contains the microlevel information on the specific patient. In order to maintain the integrity of the health record, each patient record is connected to the previous records, as well as having a temporal shadow attached to the end of the record. The Smart Contract is kept up to date in exchange for an access permission. Role-based access control grants access to the health data to the authenticated user depending on the access privileges granted to that user. Authentication in a Smart Contract is accomplished via the use of context-based access control (CBAC), according to the suggested approach. Context-based access control (CBAC) in Smart Contracts comprises information about the ownership of records, the rights granted to those records, and the integrity of the data. Breach detection is virtually instantaneous as long as the monitor's signature does not change.

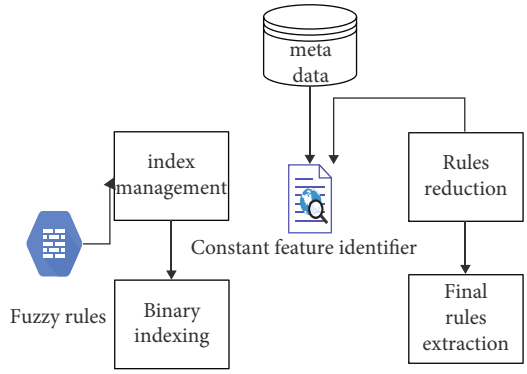

Figure 7: Layered architecture of SeFr.

The following are steps to take while uploading a file.

(1) During the registration procedure, the patient provides the SHS system with his or her public key. The RSA technique is used by the doctor to encrypt the patient's health information using the patient's public key in order to ensure the information's security

(2) All of the patient's information is saved locally for future reference. The IPFS network stores the encrypted patient health records, allowing for access to the information from any location at any time

(3) The SHA256 method with temporal shadow is used by electronic health record systems to turn the list of encrypted patient records into a hash of documents, which is translated into fixed-length associated with time using the SHA256 algorithm

(4) The registry server gets the hash of records; before transferring each record to a higher level of abstraction, each transaction is appended with a temporal shadow, and then the hashed value is sent to the linker server

(5) The linker organizes the hash of value into trees and then forwards the information to the next higher level server. For each round, the global hash tree is generated by the linker servers in a hierarchical fashion

(6) The root server is located at the very top of the linker hierarchy. The Calendar database contains the hash value for the root node

(7) A signature token is constructed using the top hash value as a starting point and a leaf hash value as an ending point. Each transaction is hashed and built into a Merkle tree, with the root value of the tree being saved in the block header of the block

(8) The Smart Contract is stored on the blockchain, and it enables the patient to choose who has access to his or her data and under what circumstances

(9) The Temporal Hash Signature (THS) token generated by the user registry server is delivered to the user registry server

To get a copy of the file, click here.

(1) The doctor asks access to the patient's information by providing a valid patient identification number

(2) The request is sent to the blockchain for processing. Before anything else, the user is prompted to input the signature token

(3) The user submits a Temporal Hash Signature (THS), and the registry verifies that the signature is valid

(4) The access privileges are validated in the context-based access control (CBAC) in the Smart Contract at the next level of authentication, and the authorized user is granted access to the data at that level of authentication

(5) The encrypted health record is decrypted with the help of the user-patient private key, which is sent to the doctor by phone by the patient and doctor

3.10.2. Implementation of the SHS System. The creation of the SHS framework application makes use of the JavaScript programming language. Consultations with a doctor are offered, and a prescription record is accessible for patients to check. In order to decode the prescription file, an encrypted version of it was uploaded to the IPFS network and subsequently decrypted. Medical records are encrypted by their physicians with the use of their public keys, and the patient may decrypt their records with the help of their own private keys, which they have given. An encrypted duplicate of the record is stored on the IPFS network. The hash value of the file that was created is referred to as the content address in this context. This was done before the hash value was formed, thereby creating a temporal shadow. The letter Qm is always used to indicate that the hash value is being used. In the section below, you can see the hash value of the file that has been stored on the Ethereum blockchain.

The Ethereum is a web-based integrated development environment for the Ethereum blockchain that was developed by the Ethereum Foundation. The connection between the front and the blockchain is established via the usage of this protocol. Ethereum makes use of the Solidity programming language, which is also utilized to set access permissions in the Smart Contract. Solidity is a programming language that was developed by the Ethereum Foundation. According to the instructions, the user installed the metamask in his or her browser in order to deploy the transaction on the Ethereum blockchain, and the transaction was successfully deployed. This research was conducted out with the assistance of the Ethereum and metamask integrated development environment, which was created to aid in the deployment of healthcare-related information systems. It is necessary for this application to operate effectively for the user to have the metamask plugin installed in their browser.

It contains three various types of datasets, including, for example, 100 patient records, 10,000 patient records, and 100,000 patient records, among other things. The doctor encrypts the patient's health record using the patient public

key, and the patient private key is used to decode it. The doctor encrypts the patient's health record using the patient public key. Once the encrypted health record has been created, it is hashed and stored in the IPFS folder where it may be accessed. An application of a temporal shadow to the equation was performed before generating the hash values. When a patient's record contains subactivities such as registration, appointment, and payment, the root value of a hashed file, which was supplied as input for the General Public Ledger, was used to hash each of the subactivities (GPL). The degree of security provided for medical records has been increased. Aside from that, it is impossible to track them down to their original source of information In order to develop a Smart Contract, Solidity is the programming language that is used. The hashed data is transmitted to the Smart Contract, and the byte code for the health record is generated. The Smart Contract is then placed on the blockchain with the aid of the remix.ethereum online tool, which is available on the Ethereum platform. A Smart Contract compiler provides an application binary interface that is utilized by the application to communicate with the Smart Contract database. In order to activate the access privilege on the blockchain, blockchain takes use of the application binary interface and executes the contract, which are both provided by the blockchain. A user-created metamask is used to deploy transactions on the Ethereum blockchain, which is used to sign transactions.

The SHS framework includes a number of different stakeholders. The dashboard of the SHS has a distinct login for each person who needs to use the system. The many stakeholders include the doctor, the patient, the nurse, the administrative staff, billing, and insurance. Doctors may submit patient information into the SHS eHealth systems if the doctor has been validated by the system. Figure 8 shows the interface to collect patient details.

After retrieving the relevant information from the database and entering the symptoms of the patient depicted in Figure 9, the doctor is ready to start treating the patient. If the patient wishes to retrieve his or her eHealth information history in the future, he or she may do so by logging in with the patient login and retrieving the information. THS (Temporal Hash Signature) and context-based access control (CBAC) are used in Smart Contracts to verify that the authentication is successful.

The doctor enters the symptoms of the patient and gives the prescription; then, the pdf file is generated for the record. Based on the symptoms, the medicine is provided by the doctor. This record is created as a pdf file, and it is shown in Figure 9.

The pdf file is encrypted with the RSA algorithm, and it is stored in the Interplanetary File System. Once the encrypted data stored in a decentralized network, then the file is hashed with the SHA256 algorithm, and the hash value is generated for the record. Always hash value starts with Qm. The hash value used for the future access of the file is shown in Figure 10.

3.11. Result Analysis. The integrity of the eHealth record is checked in the proposed work, which takes less time compared with the existing framework. Figure 11 is mentioned with x- and y-axes. The x-axis refers to the number of the records, and the y-axis indicates verification time, which measured in terms of the seconds.

Figure 8: Interface to collect patient details.

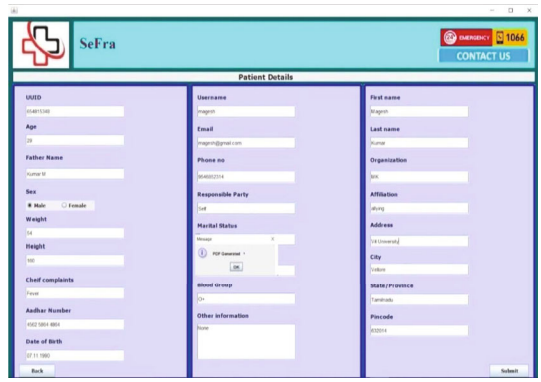

Figure 9: GUI to generate the patient record.

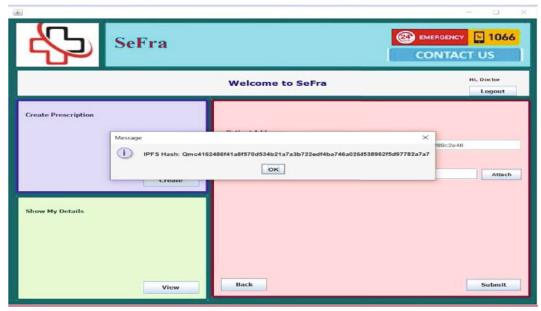

Figure 10: IPFS hash generation.

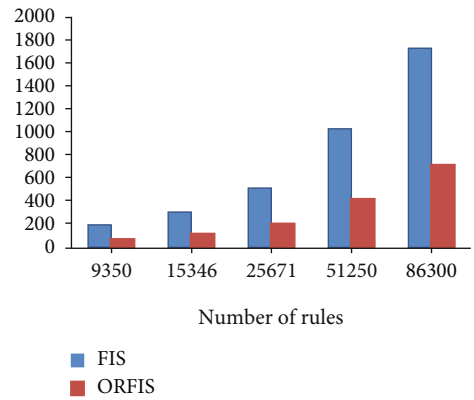

Figure 11: Proposed work compared with existing works.

Table 2: Comparison of different blockchain eHealth framework.

	MedRec (Ekblaw et al., 2016)	Patientory (McFarlane et al., 2017)	Medibloc (Vallies, 2017)	Medichain (Rouhani et al., 2018)	SHS (Charanya, 2019)
Blockchain	Permission	ETH (permission)	QTUM (public)	ETH	Permission
Private blockchain	Yes	Yes	No	Yes	Yes
Standard	HL7	HIPAA	HIPAA	JSON	HL7
Consensus	Proof of work	Proof of work	Proof of stake	Proof of work	Proof of work
Block time	19 sec	17 sec	Minutes	20 sec	16 sec
Smart Contract	Code solidity	Solidity	Go	Solidity	Code (solidity)
Patient control	Full control	No information	Patient control	Patient and doctor control	Patient control
Focus	Patient care, research	Telemedicine	Patient care, doctor, and researcher	Telemedicine, researcher	Patient care, researcher, insurance, and billing
Rewards	Anonymized data	No	No	No	Anonymized Data

Each user receives the private key and root of the PML as to the public key for the particular record. The system checks the root value of the PML and the next level of the tree, and partial checking is done to ensure the authorized user access of the record.

The main aim is to verify the context-based Merkle tree (CBMT) to check the integrity of the record. The integrity of the file quickly was verified with a CBMT. The integrity of the transaction was efficiently checked with less time with the help of PML. The Personalized Micro Ledger (PML) was not maintained in the existing system. So the verification time of the transaction is high in the existing system. Table 2 explains the comparative analysis of the proposed system with the existing system. The patient-centric healthcare system, like MedRec, Patientory, Medibloc, and Medichain, compared with the proposed system. In the proposed work, each transaction is hashed with temporal properties. These techniques provide more security to the healthcare record, and Personalized Micro Ledger (PML) was used, which reduces the verification time of the record. So the proposed system is more secure when compared with the existing works.

3.11.1. Conclusions and Discussions. The suggested approach provides a solution to the security vulnerabilities that have been identified. SHS addresses the following security issues in accordance with the proposed approach.

3.11.2. Confidentiality. The term "confidentiality" refers to the fact that an unauthorized user will not be able to access health information. Double security measures are used in this instance. A patient's health information is encrypted and saved in the IPFS in the first instance, and its hash value is considered as its addressing in the second instance. Second, in order to improve the security of the health record, the hash value of the content addressing is stored in the blockchain as a hash value. As a result, the health information is better protected.

3.11.3. Integrity. For a hacker, it is impossible to modify the hash value of a single block without also affecting the hash value of every other block in the system. Because of the nature of blockchain, every change in one block will result in an automatic change in the next block. The temporal shadow method is used in the suggested system in order to increase the overall security of the system. Before attaching the hash value to each record, the temporal shadow is appended to each record. Before hashing, the height of the subtree is attached to the connected hash, which serves as an incentive from the child node. In addition, the length of the hash chain is accepted before hashing, which is an incentive from the parent node. As a result, temporal shadow serves as a secure hash function for data [31].

3.11.4. Authentication. First and foremost, the Smart Contract establishes the access privileges for each patient data. Authorized users are permitted to access the information based on the access privileges granted to them. The context-based access control (CBAC) in Smart Contracts is a four-contract system that uses context-based access control. Access control is based not just on the user's credentials but also on the time and location of the request, resulting in high levels of security. A Temporal Hash Signature (THS), which is an extra security measure, is implemented. With the assistance of THS, each patient's health record was checked. The authentication process is completed without the assistance of a third party. A breach may be noticed rather readily if there are any substantial changes in the environment. If someone attempts to access the data, the system first verifies the access privileges set out in the Smart Contract, after which it requests that the user input the THS; if both requirements are met, the system enables access to the data.

3.11.5. Interoperability. The decentralization of blockchain technology is used in the proposed work. In no way does this suggest that an interoperability problem with a human services framework built on the blockchain will be eliminated. The HL7 standard is used in the proposed system to facilitate the exchange of information between various service providers. Each service provider will utilize a distinct system,

but they will all be required to follow the same set of rules in order to maintain interoperability.

4. Conclusion

The proposed study developed a safe eHealth framework using progressive temporal blockchain technology, which increases the security of the system overall. The information is entered in the HL7 standard, which enables for simple access to health data across various healthcare practitioners. A Smart Contract that incorporates context-based access control (CBAC) grants access to historical health information to authorized users who have successfully authenticated themselves in the system. In the progressive temporal blockchain, a hash of health data is preserved for future reference. This method is tamper-proof; once a health record has been saved, it is difficult to make changes to the data. The researcher will take on the role of a data miner and will be compensated with anonymized data. The Temporal Hash Signature (THS) is used in the Smart Contract to authenticate the user and to validate the rights of the user. The specifics of context-based Merkle tree (CBMT) for integrity and context-based access control (CBAC) in a Smart Contract for authentication are covered in more depth in the following chapters.

Data Availability

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of Interest

All authors declared that they do not have any conflict of interest.

Acknowledgments

The authors extend their gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through the research groups program under grant number R. G. P. 1/85/42.

References

[1] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare:"MedRec" prototype for electronic health records and medical research data," *Proceedings of IEEE open & big data conference*, vol. 13, 2016, p. 13, 2016.

[2] C. McFarlane and O. Söderström, "On alternative smart cities: from a technology-intensive to a knowledge-intensive smart urbanism," *City*, vol. 21, no. 3-4, pp. 312–328, 2017.

[3] J. Hu and S. Liu, "Responsive polymers for detection and sensing applications: current status and future developments," *Macromolecules*, vol. 43, no. 20, pp. 8315–8330, 2010.

[4] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.

[5] A. S. Rajawat, P. Bedi, S. B. Goyal et al., "Fog big data analysis for IoT sensor application using fusion deep learning," *Mathematical Problems in Engineering*, vol. 2021, Article ID 6876688, 16 pages, 2021.

[6] G. Khambra and P. Shukla, "Novel machine learning applications on fly ash based concrete: an overview," *Materials Today: Proceedings*, pp. 2214–7853, 2021.

[7] B. D. Rouhani, M. S. Riazi, and F. Koushanfar, "Deepsecure: scalable provably-secure deep learning," in *Proceedings of the 55th Annual Design Automation Conference*, pp. 1–6, New York, NY, USA, 2018.

[8] N. Cruz, C. A. Bustos, M. G. Aguayo, A. Cloutier, and R. Castillo, "Impact of the chemical composition of Pinus radiata wood on its physical and mechanical properties following thermo-hygromechanical densification," *BioResources*, vol. 13, no. 2, pp. 2268–2282, 2018.

[9] N. K. Rathore, N. K. Jain, P. K. Shukla, U. S. Rawat, and R. Dubey, "Image forgery detection using singular value decomposition with some attacks," *National Academy Science Letters*, vol. 44, no. 4, pp. 331–338, 2021.

[10] Y. Guo, G. Xu, X. Yang et al., "Significantly enhanced and precisely modeled thermal conductivity in polyimide nanocomposites with chemically modified graphene via in situ polymerization and electrospinning-hot press technology," *Journal of Materials Chemistry C*, vol. 6, no. 12, pp. 3004–3015, 2018.

[11] J. Jiang, J. Pi, and J. Cai, "The advancing of zinc oxide nanoparticles for biomedical applications," *Bioinorganic Chemistry and Applications*, vol. 2018, 18 pages, 2018.

[12] M. K. Ahirwar, P. K. Shukla, and R. Singhai, "CBO-IE: a data mining approach for healthcare IoT dataset using chaotic biogeography-based optimization and information entropy," *Scientific Programming*, vol. 2021, Article ID 8715668, 14 pages, 2021.

[13] L. Tan and J. Jiang, *Digital Signal Processing: Fundamentals and Applications*, Academic Press, 2018.

[14] A. S. Rajawat, P. Bedi, S. B. Goyal et al., "Securing 5G-IoT device connectivity and coverage using Boltzmann machine keys generation," *Mathematical Problems in Engineering*, vol. 2021, no. 7, Article ID 2330049, p. 10, 2021.

[15] M. Sathya, M. Jeyaselvi, L. Krishnasamy et al., "A novel, efficient, and secure anomaly detection technique using DWU-ODBN for IoT-enabled multimedia communication systems," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 4989410, 12 pages, 2021.

[16] J. H. Wayne, M. M. Butts, W. J. Casper, and T. D. Allen, "In search of balance: a conceptual and empirical integration of multiple meanings of work–family balance," *Personnel Psychology*, vol. 70, no. 1, pp. 167–210, 2017.

[17] A. Khare, R. Gupta, and P. K. Shukla, "Improving the protection of wireless sensor network using a black hole optimization algorithm (BHOA) on best feasible node capture attack," in *IoT and Analytics for Sensor Networks*, vol. 244 of *Lecture Notes in Networks and Systems*, pp. 333–343, Singapore, 2022.

[18] A. S. Rajawat, P. Bedi, S. B. Goyal et al., "Fog big data analysis for IoT sensor application using fusion deep learning," *Mathematical Problems in Engineering*, vol. 2021, Article ID 8091363, p. 16, 2021.

[19] M. Kaur, D. Singh, V. Kumar, B. B. Gupta, and A. A. Abd El-Latif, "Secure and energy efficient-based E-health care framework for green Internet of Things," *in IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1223–1231, 2021.

[20] D. Samburaj, "UK trials blockchain-based social welfare payments," *CryptoCoins News*, vol. 7, 2016.

[21] W. Suberg, "We don't need blockchain: R3 consortium after $59 million research," *The Cointelegraph*, 2017.

[22] T. D. Diwan, S. Choubey, H. S. Hota et al., "Feature entropy estimation (FEE) for malicious IoT traffic and detection using machine learning," *Mobile Information Systems*, vol. 2021, Article ID 8091363, 13 pages, 2021.

[23] N. Emmadi and H. Narumanchi, "Reinforcing immutability of permissioned blockchains with keyless signatures' infrastructure," in *Proceedings of the 18th international conference on distributed computing and networking*, pp. 1–6, New York, NY, USA, 2017.

[24] T. D. Diwan, S. Choubey, H. S. Hota et al., "Feature entropy estimation (FEE) for malicious IoT traffic and detection using machine learning," *Mobile Information Systems*, vol. 2021, Article ID 8091363, p. 13, 2021.

[25] N. Heess, D. Tb, S. Sriram et al., "Emergence of locomotion behaviours in rich environments," 2017, http://arxiv.org/abs/1707.02286.

[26] G. J. Katuwal, S. Pandey, M. Hennessey, and B. Lamichhane, *Utilizing blockchain technologies in manufacturing and logistics management*, IGI Global, Hershey, PA, 2022.

[27] O. N. Allen and E. K. Allen, *The Leguminosae, a source book of characteristics, uses, and nodulation*, Univ of Wisconsin Press, 1981.

[28] S. Joshi, S. Stalin, P. K. Shukla et al., "Unified authentication and access control for future mobile communication-based lightweight IoT systems using blockchain," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 8621230, 12 pages, 2021.

[29] N. Jain, S. Rathore, and P. K. Shukla, "Designing efficient optimum reduced order IIR filter for smoothening EEG motion artifacts signals," *Design Engineering*, vol. 2021, no. 6, pp. 5080–5101, 2021.

[30] J. Mahatpure, M. Motwani, and P. K. Shukla, "An electronic prescription system powered by speech recognition, natural language processing and blockchain technology," *International Journal of Scientific & Technology Research*, vol. 8, no. 8, pp. 1454–1462, 2019.

[31] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H. -N. Lee, "Systematic review of security vulnerabilities in Ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022.