Design of a Blockcdhain based Security Algorithm for IoT in Healthcare

Parag Rastogi*
Dept. of CSE
IFTM University
Moradabad, Uttar Pradesh, India
parag0305@gmail.com

Dr. Devendra Singh
Dept. of CSE
IFTM University
Moradabad, Uttar Pradesh, India
dev625@yahoo.com

Dr. Sarabjeet Singh Bedi
Dept. of CS & IT
MJP Rohilkhand University
Bareilly, Uttar Pradesh, India
dearbedi@gmail.com

2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 978-1-6654-3789-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICACITE53722.2022.9823466

***Abstract*— Electronic health records (EHRs) are becoming increasingly popular in healthcare organisations as a way to save costs and improve efficiency by replacing paper-based records. There are numerous advantages for patients, healthcare organisations, and healthcare professionals to having online access to patient records and transactions linked to diagnosis. However, it also poses severe privacy concerns over the patient's private data. Medical records can now be stored, accessed, and updated at any time and from any location thanks to the internet and its impact on the healthcare industry. Electronic Health Records (EHR) discrepancies and concerns about privacy and security should be addressed. The lack of consistency in EHR may have been the most serious problem, but it isn't the only one. The interoperability and privacy difficulties have already been addressed through the usage of decentralised online ledgers with blockchain-based systems. A Secure eHealth Framework based on a progressive temporal blockchain method is presented to overcome the aforementioned issues. As a result, the context-based smart contract helps to record medical data in a text format with temporal features and disseminate the data among all other peers as specified in the smart contract regulations Furthermore, the framework has the ability to address data concerns and deliver tamper-proof, secure transactions in the healthcare industry. RBAC and various system modules were put through their paces to see how well they worked with the Delegated Byzantine Fault Tolerance consensus algorithm (dBFT). The results suggest that the system is able to safely and effectively handle and disseminate EHRs.**

Keywords*—*Block chain, Smart contract, Healthcare, Delegated Byzantine Fault Tolerance consensus algorithm (dBFT)

I. INTRODUCTION

Although the technology behind blockchain may appear to be complex, it is actually quite straightforward when you get right down to it. A database, such as the blockchain, is a sort of distributed ledger technology. A database is a collection of data on a computer system that has been stored electronically. Tabular data structures are common for databases because they make searching and filtering for specific information much easier [1]. In order to store and access a little amount of information, spreadsheets are best used by one person or a small number of people. A database, on the other hand, is designed to keep a huge amount of information that can be accessed, filtered, and managed simultaneously by several users. A database server made up of powerful computers receives data from large computers. As many as tens of thousands of computers may be required to access the database at once in order for these servers to function. If a spreadsheet or database is open to the general public, it is usually owned and administered by a designated individual who has complete authority over how it runs and the data in it [2]. A possible game changer in the financial sector, blockchain is the digital record-keeping technology powering Bitcoin and other cryptocurrency networks. Faster and more cost-effective product delivery, improved product traceability, better partner coordination, and easier access to funding are just some of the ways that blockchain may enhance supply chains.

There have been major shifts in the healthcare industry as a result of the Internet of Things (IoT). Health care providers are using the Internet of Things (IoT) to connect sensors and medical devices, which generate and communicate sensitive information [3]. To keep an eye on patients' health while their doctors are away, IoT devices are being employed. The sensors and medical equipment in the healthcare IoT service system collect streams of data for use in decision support systems. Concerns concerning patient data security are raised as a result of a huge amount of information passing across the network at once [4]. As a result, the collecting of patient data while maintaining privacy (PPDC) is in high demand. Protecting the privacy of the data collector is critical in the PPDC process. Before the data is sent to the data collector, privacy-preserving procedures should be applied to the data to ensure its integrity.

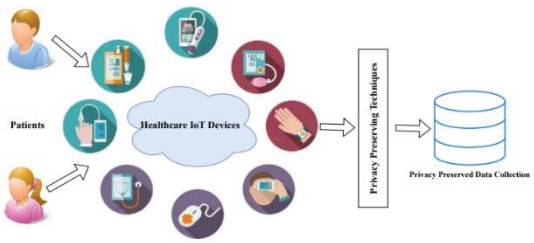

Fig. 1. Privacy Preserving Data Collection Process

Researchers' interest in publishing data while protecting their privacy has grown in recent years. Medical research, including novel therapy, early diagnosis, and accurate treatment, depends on the availability of healthcare data. Research and development teams or pharmaceutical corporations are often involved in data analytics in healthcare organisations [5]. Patients' personal information is gathered by healthcare organisations. Personal information, such as names, dates of birth, addresses, and medical records, may be included in the data gathered. These datasets provide a massive amount of information that can be used in medical research. In order to safeguard the privacy of its patients, healthcare organisations must follow established ethical and legal guidelines before disclosing patient data to other researchers or pharmaceutical corporations [6]. In order to safeguard patient privacy, healthcare organisations must change their

data in a way that does not leak personal information. It is known as anonymization to change the original data into a form that does not reveal any personally identifiable information. The data can be shared with third-party researchers in an anonymized form for data analytics. As a result, it is critical that the de-identified data still be useful [7]. In other words, the primary goal of privacy-preserving data publishing is to improve data utility while ensuring the confidentiality of the data.

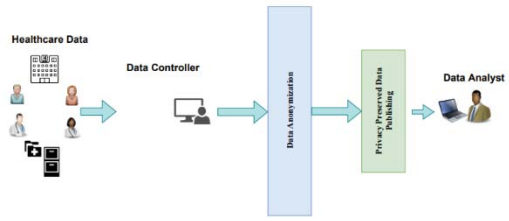

Fig. 2. Privacy Preserving Data Publishing Process

II. Background About Blockchain

[9] IoT and blockchain are two key technologies that have the potential to have a substantial impact on the communications and IT industries. Improved visibility, openness, trust, and comfort for users have been the primary goals for these technologies. To put it another way, a distributed ledger, often known as replicated log files, is at the heart of blockchain technology. The blockchain records each transaction in chronological order, with the timestamps indicating when it was made. Using cryptographic hash keys, every entry in the ledger is inextricably linked to the one before it [8]. The cryptographic hashing used to link each block to the ones before it, as well as an example blockchain architecture, are depicted in Figure 3. All transactions are recorded in a Merkle tree, with the root hash stored in the blockchain. Coinciding with this, the transactions are hashed cryptographically and stored in leaf nodes of the tree (Ha... Hc... Hd...). Child nodes' hashes are combined to form a new root hash [10]. H1, H2, etc., are all stored on the blockchain. If a single transaction on one side of the tree is modified, all of the hash values on that side of the tree will be affected. Thus, the root hash is sufficient to determine whether or not all of the transactions linked with it have been tampered with or not. The miner or ledger maintainer verifies the transactions or logs and generates a key, allowing the most recent transaction to be included in the whole ledger. All the network's nodes receive the most recent entries through this method [9]. The adversary will have a difficult time tampering with the blocks because each one contains a cryptographic hash key.

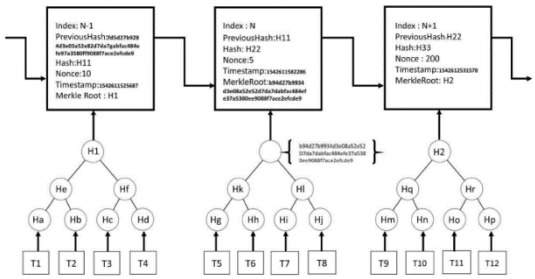

Fig. 3. Architecture of basic Block chain

IoT data can be protected by the blockchain's unique qualities, which include its ability to be tamper-proof and distributed. The miners are solely mining for their financial incentives, and they have no personal stake in any transaction [10]. The miners, on the other hand, do not know who the owners of the transactions are. As a result of the intense rivalry amongst miners, a large number of the same type of transactions are being worked on simultaneously by a large number of people. An entire transaction, from startup through submission to the distributed chain is depicted in Figure 4. There are a variety of frameworks and platforms being developed in academia and industry that facilitate the development and maintenance of blockchain. Many such platforms exist, some of which are listed here: Ripple, Ethereum, Hyper ledger fabric.

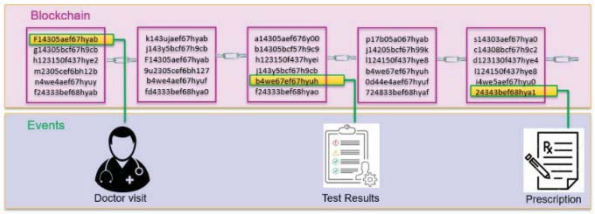

Fig. 4. Blockchain working Process

III. Block Chain Based Layered Architecture

Four layers of data sharing are employed in the proposed concept, all of which are based on blockchain technology. layers, such as the application layer, query layer, data provenance layer, and database layer, Figure 5 depicts the layers of the system.

A. Application Layer

The data can be entered by the user and retrieved from the system at a later time for analysis or any other purpose. Doctors, patients, billing, insurance, nurses, lab technicians, etc. are all users of the proposed system. The data is used for a variety of purposes by each individual user. This layer serves primarily as a conduit for information exchange between the user and the software being used.

B. Storage Layer

It is encrypted with the RSA technique and kept in the IPFS for each patient record. To ensure that only authorised individuals have access to the document, the hash value is stored on the blockchain. Despite the fact that IPFS may store any type of data, we are primarily interested in text files in this project.

C. Quary Layer

The user sends a set of queries to the system in order to retrieve data from the database. This layer's major function is to receive the user's query and return the result. The user can either see or restrict access to the record if the circumstance arises automatically. What we're calling a Temporal Hash Signature is a public key that is shared by all patients who generated a transaction at the same time, while the private key is unique for each transaction (THS). All of the Smart Contract's keys. Smart Contracts use keys and privileges to verify the identity of the user before granting access to the data.

D. Network Layer

Data can be retrieved from the current database. It is the Smart Contract that specifies the permissions that are being used. The Smart Contract keeps track of every transaction, which is then permanently saved in the blockchain for future reference. All dispersed nodes receive each result. This layer

is in charge of verifying the identity of each request made by a user and relaying the appropriate response to the verified user. It's important to disseminate data over the network so that anyone who needs it may find it.

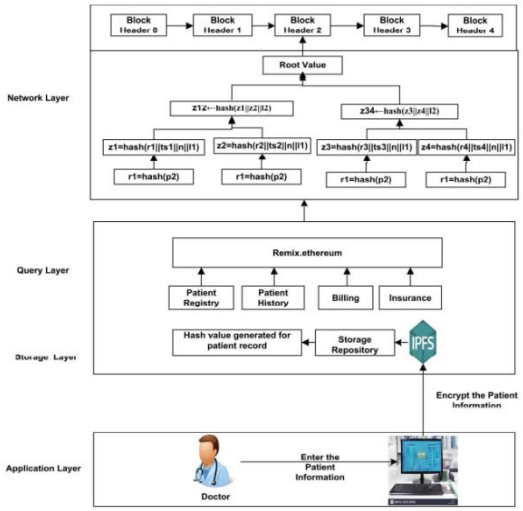

Fig. 5. Block chain based Layered Architecture

To begin with, Bitcoin's notion of Blockchain was used to inspire the development of Blockchain. Transparency and security were essential while using cryptocurrencies. However, concerns such as trust must be worked out between two parties who don't communicate with each other on a regular basis [11]. A notarized agreement between two parties that don't trust one other can be used as evidence in court if necessary. Manual agreements and legal proceedings take a lot of time and effort. Hence, smart contracts are introduced with the same motto to serve the same way, but with little paperwork and quick reaction time, and of course without a trusted third party. They are a set of codes with few ifs and buts. Smart contracts, on the other hand, are deficient in areas like scalability and performance when it comes to implementation. Smart contracts can now be implemented using a defensible logic framework that examines various combinations of logic programming languages to operate smart contracts [12]. Zero-knowledge proofs (ZKPs) are cryptographic methods that provide security and transparency in a decentralised smart contract system. Ethereum smart contracts have also been subjected to purposeful attacks in order to assess their vulnerability.

IV. Methodology

GPL, Personalized Micro Ledger, Smart Contract and Context-based Access Control are the foundational ideas of the proposed SeFra framework (CBAC). When the hash function is run, the Temporal Hash Signature (THS) is utilised to verify authenticity and compared with the result saved in the blockchain. Finally, the hash value of the blockchain's root hash. In the suggested system, the THS and the Progressive temporal blockchain are two of the most important components [13]. The mining method employed in the blockchain, and it is handled by the medical researcher to acquire the anonymized data as a reward for putting the block in the blockchain, is detailed below in Fig. 6 of the Secure framework. Traditional block-chains have two major issues: the difficulty of linking the hash chain and a powerful hash function that makes it difficult to know the input value. However, attackers can identify the pattern of input and then test with all possible data and try to decipher the content of the hash. Progressive temporal blockchain solves both of these issues.

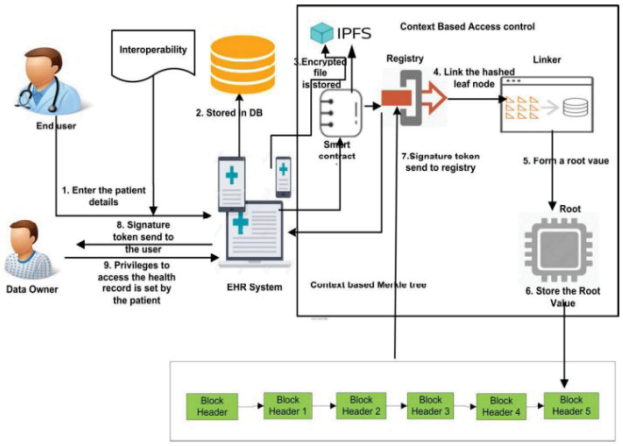

Fig. 6. health care framework based on blockchain

Figure 7 depicts the process of adding users to the health-chain network. Framework designed is role-based in which patients can register themselves and log in using their email address and password to access the platform. Network administrators will add the nodes to the blockchain once the consensus voter nodes have verified them. With the use of usernames and passwords, patients and other users will be able to access the health-chain, which will only require a minimal amount of confirmation [15]. A hashing algorithm called SHA-256 is used to encrypt the user's password for added protection. Creates a REST API that visualises and queries data stored in the CouchDB. Transactions can be processed and retrieved using the rest server's ability to create, read, update, and remove assets and participants.

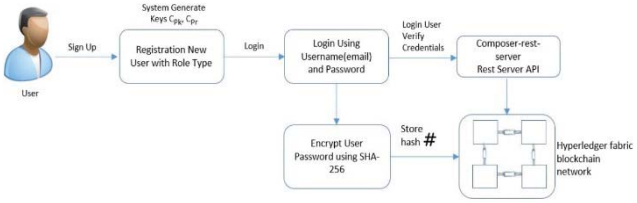

Fig. 7. Healthchain user addition

The clinician's entry into health-chain of the patient's medical history is shown in Fig. 8, which provides a step-by-step breakdown. Patients and doctors are assumed to have an approved relationship for updating health records in this method. The clinician adds medical records to the database using the internal encryption technique. Adding patient records to the health-chain can be done in two ways: To generate a new patient record, clinicians upload encrypted medical records to IPFS using their patient's public key. Then, the system builds a composite view, PCvi, that can be accessible to the clinician, or the entire data set can be shared with other clinicians.

Additionally, the system generates a unique session key (Sk) that is shared by the patient and the doctor. Encryption employing public keys of both patients and clinicians is then used to communicate encrypted session key Sk (EPpki (Sk) and ECpki (Sk)) to each other for a specific session. It will also be encrypted with the session key Sk (PCvi) and stored in IPFS

as ESk (PCvi). A secure Composite view, referred to as ESk (PCvi), is also sent to the doctor by the system.

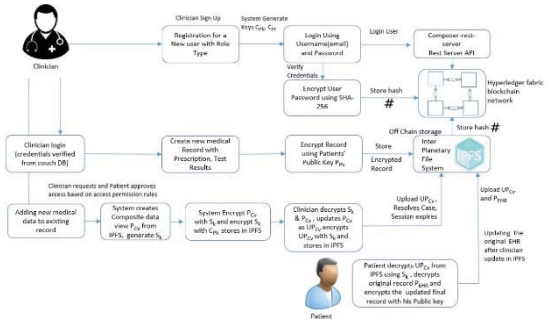

Fig. 8. Proposed Healthchain Architecture

In contrast, the dBFT mechanism uses a different approach. Transactions must be organised into batches by consensus nodes. In the jargon, a block refers to a collection of people. At the same block height, there may be thousands of blocks that are legitimate. So the dBFT method takes into account that the "client" likewise fails to ensure the final certainty of the block (that is, there is only one block for a particular block height). This is completely ignored by PBFT. Based on the PBFT, dBFT is an upgraded version of the Byzantine fault-tolerant protocol. In addition, it incorporates aspects of DPoS. The Blockchain network authorises a few nodes to act as accounting nodes by voting on the Blockchain. New blocks are created following the simplified PBFT consensus (dBFT consensus).

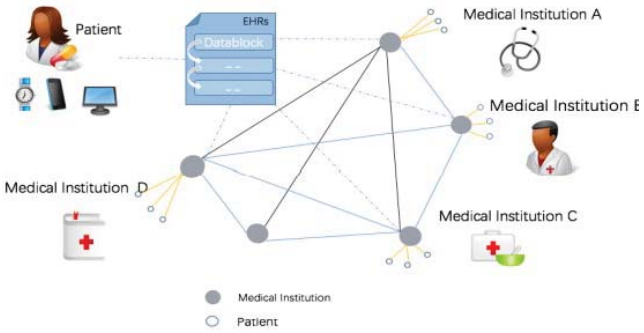

Fig. 9. Test setup for the dBFT

V. RESULTS

As shown in Figure 10, the procedure for getting a hold of an eHealth record can be found online. The doctor has asked to have decentralised network access to the patient record. Following the steps below will grant you access to your medical records. Using the patient's id and Temporal Hash Signature (THS), the doctor is requesting access to the patient's record. A Context-based Access Control (CBAC) in a Smart Contract, which verifies the patient's permission to the specific doctor, assures that the access privilege is legitimate. Once the request has been authorised, the response is sent to the CBAC in the Smart Contract, and the doctor can retrieve the information from the Smart Contract. JavaScript is used to construct the eHealth application. It begins by encrypting all of the patient's information and storing it on the IPFS network. It's termed content addressing since it generates a Hash value. Using remix.ethereum, developers may connect the front-end to the blockchain. To implement Context-based Access Control (CBAC), Smart Contracts employ the solidity language. Once this data has been processed, it has been added to the blockchain. The eHealth information is put into the Ethereum block-chain via the meta-mask. CBMT is employed in the blockchain to secure the integrity of the eHealth record.

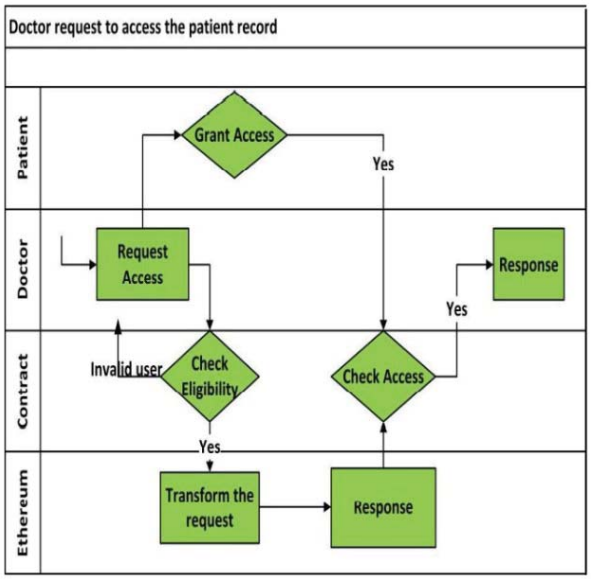

Fig. 10. Proposed accessing the eHealth Record

In the proposed work, the integrity of the eHealth record is checked, which takes less time than the current framework. Figure 11 depicts the x and y axes stated before. Records are shown on the x-axis, and verification time is shown on the y-axis in seconds. The public key for a certain record is sent to each user together with the private key and root of the PML. As a precaution, a partial check is made to guarantee that only authorised users can see the record's root value and its next level.

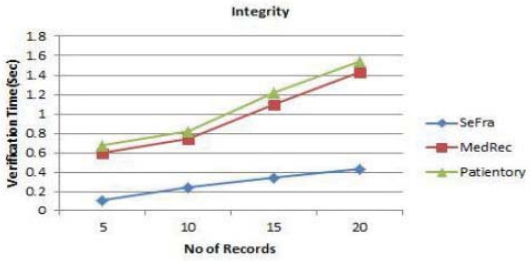

Fig. 11. Proposed Work Compared with Existing Works

Context-based Access Control (CBAC) in a Smart Contract outperforms regular Smart Contracts in terms of performance. THS is used to authenticate each user, and then the Smart Contract's CBAC is used to verify their access privileges. With THS, user authentication takes a fraction of the time it would otherwise. To access an existing transaction, the user needs to be aware of the most recent Temporal Hash Signature(THS) transaction. As a result, both the patient and the doctor save time by not having to keep track of every THS. Instead, the most recent THS must be preserved. Even though the user's THS has a legitimate signature, the system still checks the Smart Contract to see if they have access privileges that are stated in the Smart Contract. There are two methods of authentication offered in this piece of art. THS is used to verify the user's identity before granting them access to the Smart Contract. Using a private and public signing key, each transaction is secure. The time it takes to check a transaction

using the PML and without it is shown in Fig. 12 of the proposed work. The graph shows that the suggested work is superior than the current work.

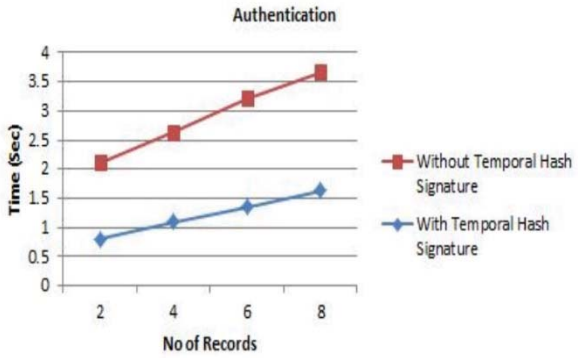

Fig. 12. Authenticate with and without Personalized Micro Ledger

For each set of test results, the dissertation employed a line chart to compare the data. Figure 13 depicts the outcomes of the comparison.

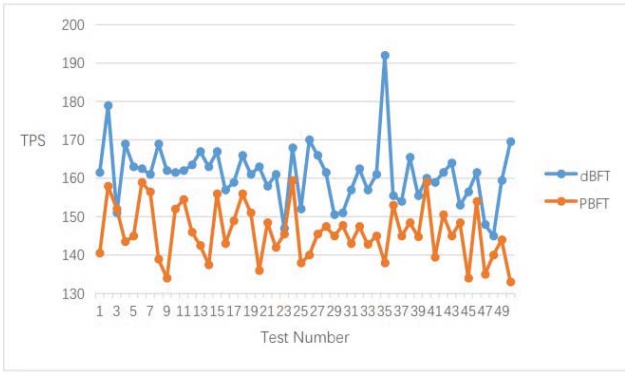

Fig. 13. Comparison for the dBFT anf PBFT test results

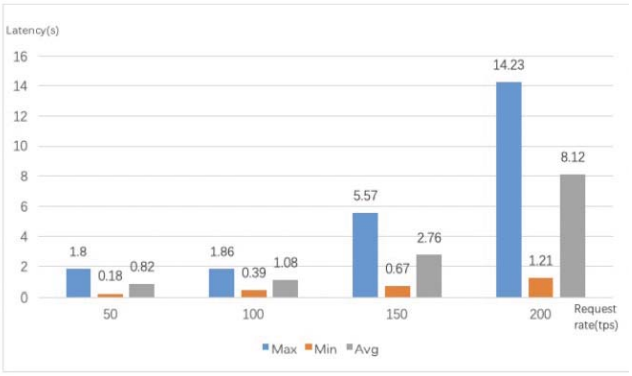

Fig. 14. latency of the dBFT algorithm at different request rates

The figure 14 shows that when the request sending rate raises, so do the system's maximum, minimum, and average latency values when the two algorithms complete account opening transactions. On the one hand, the PBFT algorithm's system latency will skyrocket as request transmission rates reach 200 TPS. In this case, the request was sent too quickly, and the system was unable to process it soon enough. It is therefore taking too long for the request to move through the system, resulting in excessive latency. A system that uses dBFT has a latency increase that can be kept within a few seconds.

VI. Conclusion

The Secure framework (SeFra), which is developed using a progressive temporal blockchain and is intended to improve the security of the electronic health record, is the focus of this proposed research. The fundamental purpose of this inquiry of data integrity and authentication, confidentiality, and auditability in eHealth systems was to increase user confidence in these systems. The proposed technique, which takes advantage of temporal features, makes interoperability easier while also dealing with scale challenges. The security of electronic health records is ensured by using context-based and temporal aspects. The temporal property was attached to each record before the records were subjected to a powerful hash function. This ensures a high level of security. For the purpose of putting the Blockchain to the test, we selected the dBFT consensus algorithm as the system's consensus mechanism.

Customers require greater transparency in product costs because what they think they are paying for is not what they are actually paying, and the supply chain, stakeholders, and the environment all require mutual trust in order to thrive. This is just one of many difficulties, but one of the most significant is that there are flaws in the blockchain technology as well as network vulnerabilities.

References

[1] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, ‘‘AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud,’’ IEEE Access, vol. 8, pp. 70604–70615, 2020.

[2] J. Indumathi et al., "Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6 HCS)," in IEEE Access, vol. 8, pp. 216856-216872, 2020, doi: 10.1109/ACCESS.2020.3040240.

[3] S. Gupta, V. Malhotra, and S. N. Singh, ‘‘Securing IoT-driven remote health care data through block chain,’’ in Advances in Data and Information Sciences (Lecture Notes in Networks and Systems), vol. 94, M. Kolhe, S. Tiwari, M. Trivedi, and K. Mishra, Eds. Singapore: Springer, 2020, pp. 47–56.

[4] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv, and S. Mumtaz, ‘‘Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV,’’ IEEE Trans. Veh. Technol., vol. 69, no. 11, pp. 13784–13795, Nov. 2020.

[5] F. Ellouze, G. Fersi, and M. Jmaiel, ‘‘Block chain for Internet of medical things: A technical review,’’ in Proc. Int. Conf. Smart Homes Health Telematics. Cham, Switzerland: Springer Jun. 2020, pp. 259–267.

[6] N. Dilawar, M. Rizwan, F. Ahmad, and S. Akram, ‘‘Blockchain: Securing Internet of medical things (IoMT),’’ Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 1, pp. 82–89, 2019.

[7] L. Xu, A. Bagula, O. Isafiade, K. Ma and T. Chiwewe, "Design of a Credible Blockchain-Based E-Health Records (CB-EHRS) Platform," 2019 ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K), 2019, pp. 1-8, doi: 10.23919/ITUK48006.2019.8995905.

[8] Leung, L. and C. Chen, E-health/m-health adoption and lifestyle improvements: Exploring the roles of technology readiness, the expectation-confirmation model, and health-related information activities. Telecommunications Policy, 2019. 43(6): p. 563-575.

[9] Ford, E., et al., Our data, our society, our health: A vision for inclusive and transparent health data science in the United Kingdom and beyond. Learning Health Systems, 2019: p. e10191.

[10] Liu, F., Y. Li, and X. Ju, Exploring Patients' Consultation Behaviors in the Online Health Community: The Role of Disease Risk. Telemedicine and e-Health, 2019. 25(3): p. 213-220.

[11] Joseph, B.K., Blockchain for Open Data–Exploring Conceptual Underpinnings and Practice, in Governance Models for Creating Public Value in Open Data Initiatives. 2019, Springer. p. 161-175.

[12] Zhao, C. and X. Meng. Research on Innovation and Development of Blockchain Technology in Financial Field. in 2019 International Conference on Pedagogy, Communication and Sociology (ICPCS 2019). 2019. Atlantis Press.

[13] L. Xia, Y. Sun, R. Swash, L. Mohjazi, L. Zhang and M. A. Imran, "Smart and Secure CAV Networks Empowered by AI-Enabled Blockchain: The Next Frontier for Intelligent Safe Driving Assessment," in IEEE Network, vol. 36, no. 1, pp. 197-204, January/February 2022, doi: 10.1109/MNET.101.2100387.

[14] Chu, X., et al. An Empirical Study on the Intention to Use Online Medical Service. in 2018 15th International Conference on Service Systems and Service Management (ICSSSM). 2018. IEEE.

[15] Tadvi, S., et al. Personal health records integrated using Android based health care system. in 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). 2017. IEEE.