Published by
NIGERIAN SOCIETY OF PHYSICAL SCIENCES
Available online @ https://journal.nsps.org.ng/index.php/jnsps

J. Nig. Soc. Phys. Sci. 5 (2023) 992

Journal of the Nigerian Society of Physical Sciences

Secure Health Information System with Blockchain Technology

A. E. Ibor[a,*], E. B. Edim[a], A. A. Ojugo[b]

[a] *Department of Computer Science, University of Calabar, Calabar, Nigeria*
[b] *Department of Computer Science, Federal University of Petroleum Resources, Effurun, Nigeria*

Abstract

This paper focuses on highlighting the problems that are associated with the absence of privacy and security of medical records in a healthcare system. It seeks to bridge the gap between the currently used security protocols in the management of health information, and encryption algorithms that should be used. Extant health information systems have always been developed with conventional databases. With all the privileges to read, write and execute assigned to the administrator, who has centralised control over all medical records, there is the likelihood of the misuse, distortion and loss of such records in the event that the administrator becomes compromised or inadvertent system failure. To solve this problem, the use of decentralised and distributed databases becomes paramount. Blockchain technology has recently received much attention due to its ability to permit a peer-to-peer network with distributed databases that can be stored locally on each node in the network. Subsequently, all updates on records in a database are communicated to all participating parties, hence addressing the problem of centralised control. In this paper, we propose a health information system on a blockchain to create a trust-free system for both health personnel and patients. From the results obtained, we achieved the decentralisation of the medical records' database to enhance the security and privacy of data on the modeled peer-to-peer network.

DOI:10.46481/jnsps.2023.992

Keywords: blockchain, health information system, distributed databases, encryption algorithms, medical records

Article History :
Received: 16 August 2022
Received in revised form: 06 November 2022
Accepted for publication: 06 November 2022
Published: 29 April 2023

Communicated by: Tolulope Latunde (Ph.D.)

1. Introduction

Computers have been employed in the delivery of healthcare services and their usage has been helpful in enhancing operational efficiency and clinical services. However, the current paradigm shift in the healthcare industry brings to light the challenges of maintaining the integrity of medical records. With the advancement in information and communication technology, healthcare delivery has come with new formats and structures – from evidence-based medicine to e-medicine and remote e-health services [1]. Similarly, the application and use of computer-based solutions in healthcare is witnessing new dimensions, thus, giving room to novel security flaws. These emerging security flaws require effective defence mechanisms to contain likely unauthorised access, modification and distortion of medical records.

The World Health Organisation defined a Health Information System (HIS) as a system that is able to capture, store, manage, and transmit health-related information. In this sense, achieving a functional HIS is paramount in enhancing

*Corresponding author tel. no: +2348154213807
Email address: ayei.ibor@unical.edu.ng (A. E. Ibor)

the storage and retrieval of medical records. According to [2–4], a typical HIS must allow for the effective collection, processing, reporting, and use of health-related data across different health-based units. Current approaches to health information systems rely mostly on centralised databases with administrative control and policies, as well as authoritative access. In this case, changes and updates are only effected by an administrator or super user, and any other person to which such rights and privileges are assigned. This nontransparent transaction policy creates room for the possibility to distort records and compromise the integrity of classified medical data.

In recent times, the emergence of disruptive technologies such as the blockchain provides the capacity of managing distributed databases, which can be updated and locally stored across all nodes in the network. According to [5], the blockchain is a distributed database of records (or public ledger) of all transactions, which are executed and shared among participating parties. Similarly, [6] argued that in a blockchain, transparency is inherent, thus, permitting that updates on records are only possible when a majority of the participants reach a consensus. New insights into the expansion of HIS show that it has the potentials to increase the accessibility to medical records [7–9]. However, the use of conventional and centralised databases limit such possibilities as authentication credentials are granted from a central point. In the event of a failure of the database, loss of records becomes inevitable, in which case, the operations of the target system will be truncated in real time. These limitations necessitate the need for a decentralised database that is difficult to compromise in terms of data integrity, confidentiality and availability.

Current implementations of the blockchain enable the use of a public ledger, which consists of the information of all the participants and transactions on the blockchain [6–10]. The information captured as well as the digital transactions that have ever been executed on the blockchain can be recorded and shared across the peer-to-peer blockchain network. Similarly, [11] asserted that users can validate transactions, and also have identical copies of these transactions on their local machines. In this way, health information can be securely stored, updated and transmitted without unauthorised modification. Furthermore, it is easier to track all updates as the information stored in the blockchain database is always complete and includes all records of transactions from the point of origin of the transactions.

Health information requires a high level of accuracy at all times as minor changes in such data can lead to very unpleasant results with a plethora of consequences. With the blockchain network being able to perform periodic self-updates, it helps to deliver a self-reviewing system that is computationally infeasible and expensive to compromise. Transactions stored cannot be erased without the consensus of all participating parties. In this sense, it will be feasible to store and track medical records irrespective of the location of the Health Maintenance Organisation (HMO), patients, nurses, doctors, and other health personnel. In addition, patients' past illnesses, which are recorded on the blockchain can be useful for the proper treatment of patients in contrast to systems that run on a centralised database with limited access and the possibility of central point of failure.

To address the problem of authoritative access and centralised control of the database of medical records, this paper proposes a secure system for managing medical records using the blockchain technology. The use of the blockchain provides distributed access to the database of medical records to forestall the problem of single pint of failure. In the same sense, it becomes impossible to modify the stored medical records without the consensus of the participating parties, thus making the storage and transmission of medical records an entirely transparent process. To implement the blockchain, we used Python, GO, Docker Engine, interplanetary file system (IPFS), and other technologies with significant results obtained from rigorous experimentation. The rest of the paper is organised as follows; the review of the related literature is discussed in section 2. In section 3, the materials and method are discussed while the results and discussion are presented in section 4. Finally, the conclusion with future research direction is given in section 5.

2. Review of Related Literature

A detailed analysis of the existing healthcare information systems is provided in [12]. The authors argued that computerisation is significant in realising an efficient HIS. Similarly, they investigated the security of medical records and were able to give the design of a computerised system used by the National Heath Management Information System (NHMIS). The implemented system was able to allow the safekeeping of patients' records with basic components of running an effective and productive hospital. This notwithstanding, the system ran on a local server database that served as the repository for all medical data including queries and reports.

In [4], the evolution of HIS is highlighted. Areas of interest include the migration from paper-based to computer-based processing and storage, the availability of global and regional HIS, the use of health-related data for effective healthcare planning, and the deployment of technology for health monitoring. These aspects of HISs have witnessed tremendous improvements alongside an increase in health-related data. It is therefore pertinent to have a robust mechanism through which the escalating amount of medical records can be effectively stored, queried, reported and transmitted. Furthermore, [3] highlighted the design and implementation of a HIS, and discussed the possibilities of improving its structure through the use of a comprehensive, integrated and decentralised system.

Similarly, [13] assert that the tendency to manually reconcile medical data among clinics, hospitals, laboratories, pharmacies and insurance companies has not been a successful process. This is due to the fact that no single list of the disparate locations housing patients' data exists, and at the

same time, it is difficult to ascertain the order of data entry to determine the records, which predate the others. In other words, determining the medications a patient is actually taking using antecedents of prescriptions may be unclear. In the same sense, every electronic health record uses different workflows to store data so that it becomes unclear who recorded what and when.

In [14], MedRec is proposed. MedRec is a decentralised record management systems using blockchain technology. The proposed system is able to give patients a log of their comprehensive, accessible and credible medical history. MedRec allows participants to be informed of their medical history including any form of modifications on these records.

It is argued in [15] that the use of blockchain can be helpful to tackle the lagging in HIS, which runs on local server databases. This is a fact as patients whose medical records are managed by HIS running on a local server database have limited privileges to such data. Consequently, the administrator may alter these records or deny patients access to same.

There are several attempts by malicious users to compromise the security of medical records. Cyberattacks such as SQL injection [16], which targets the data aggregated on the database over time are very common. To this effect, the use of various disruptive technologies such as the blockchain, artificial intelligence, and internet of things for protecting medical records from human errors and cyberattacks is discussed in [17]. The different application areas of these technologies were also highlighted in this work including their security-related concerns. Specifically, the authors identified the use of blockchain-based trust models in the implementation of data management in the healthcare sector to optimise the process flow and reduce the operational costs.

The authors in [18] argued that the blockchain facilitates the use of a decentralised and distributed environment devoid of a central authority. Since the transactions on a blockchain are both secure and trustworthy, its use in healthcare for realising patient-centric approach to healthcare systems and maintaining accurate electronic healthcare records is crucial. From their findings, the authors agreed that the use of blockchain technology in healthcare allows for the sharing of data, the accurate management of health records, and access control. In the same sense, the use of lightweight blockchain architecture for the management of healthcare data is proposed in [19]. The approach is able to reduce the computational and communication overhead of Bitcoin network using clusters, where each copy of the ledger is maintained per cluster. Each cluster consists of network participants that are able to use canal for secure and confidential transactions. Their approach was also targeted at eliminating the problems of traditional client-server and cloud-based systems deployed in managing healthcare data. Some of these problems include single point of failure, centralised data control, inherent system vulnerabilities, and data privacy.

Consequently, the benefits of using blockchain for healthcare are highlighted in [20]. Some of these include distributed ledger, decentralised storage, authentication, security and immutability. The authors posited that the application of blockchain in healthcare improves data sharing capabilities, integrity, availability and authentication. In other words, the blockchain will allow patients to have control and ownership of the sharing of their medical data in a secure environment. Besides, [21] identified electronic health records and personal health records as the most targeted areas that rely on blockchain technology. They claimed that access control, interoperability, and data integrity are issues that the use of the blockchain in healthcare has helped to improve.

One significant feature of the blockchain remains that it cannot be easily compromised [22]. When a block is created, a one-time hash is generated. This hash is unique to the blockchain and is generated using the values of the features of each block. Changes to values in the block invalidate the hash as well as the block making the blockchain unbreakable as illustrated in Figure 1.

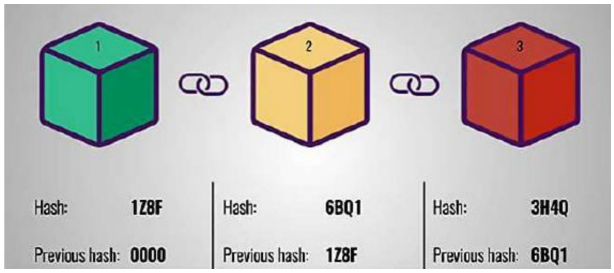

Figure 1: An Illustration of the Blockchain

As shown in Figure 1, putting information in the blockchain creates a block that contains the present and previous hashes. The first block is known as the genesis block, and has the present hash and previous hash. The second block is then created and the hash of this block is linked with the genesis block, and so on.

In this sense, [15] asserted that the use of blockchain innovation allows a verified HIS to resolve certain issues, for example, moderate access to medical information, framework interoperability, improved quality of medical data, and trust-free transactions. In addition, the significant advantages of the usage of blockchain in the security of medical records are highlighted in [13, 22–25]. These include:

i. Distributed Database: Each patient on a blockchain can access the entire database from its origin and be able to confirm the records of his/her information or data straightforwardly, without a middle person.

ii. Peer-to-Peer Transmission: Communication happens legitimately between nodes rather than through a focal hub. Every node stores and advances data to every other node.

iii. Transparency with Pseudonymity: Every transaction and its related components are obvious to anybody with access

to the blockchain. Every node, or client, on the blockchain has a unique identifier of 30 or more alphanumeric code that distinguishes it. Clients can stay unknown or give confirmation of their identities to other people. All transactions happen between blockchain addresses.

iv. Irreversibility of Records: Once a transaction is entered in the database and the records are refreshed, the records cannot be adjusted, in light of the fact that they are connected to each record that preceded them (subsequently the expression "chain"). Different computational algorithms and methodologies are used to guarantee that the chronicle on the database is lasting, sequentially ordered, and accessible to all others on the system.

Other advantages of using blockchain technology include the use of smart contracts for computational logic, scalability, and the infeasibility of a single user compromising the entire blockchain [26–30]. From the literature, the inherent problems of centralised and authoritative databases can be addressed by the use of the blockchain. Some of these problems include:

i. Standalone System: This requires authoritative access and mostly not suitable for large scale networks.
ii. Cloud based Systems: It may be cheap to implement but may not have the appropriate mechanism for allowing secured transparent transactions. It can also lead to data loss and theft in the event of espionage or system failure.

Therefore, it is envisaged that the use of blockchain will help to resolve the highlighted issues since it is a peer-to-peer network where each participant has the database stored locally in each of the nodes in the blockchain network. Changes to stored records are transparent to all participants and no participant can authoritatively make a change without the consent of others.

3. Materials and Method

In this section, the design of the proposed system is discussed. The design highlights details of the functionality of the system in terms of data storage, transmission, access and retrieval for all relevant parties.

3.1. Method

The blockchain is developed by creating a secure and transparent environment for medical records. Using a 3-tier architecture, the blockchain serves as the underlying database for the storage and authentication of medical records. The client side of the 3-tier ensures the transmission of data to the blockchain's network. These data is processed at the logic layer, which interfaces with the blockchain to determine the integrity or otherwise of the medical record using the hash code of each block. These hash codes are used to keep the medical records safe in the blockchain. The hash codes are generated by mapping a variable length input such as a patient record to a fixed length output. This fixed length output is the hash value of the record, and will change when the block of information holding the medical record is changed.

The blockchain network is a decentralised structure with peer-to-peer nodes. These nodes inspect and authenticate the validity of any new transaction such as a storage or retrieval request. This request is then fulfilled though distributed consensus by different validating nodes. Moreover, no single validating node can have centralised control of the blockchain, making it difficult for medical records to be corrupted, distorted, stolen or compromised. The architecture of the proposed system is shown in Figure 2.

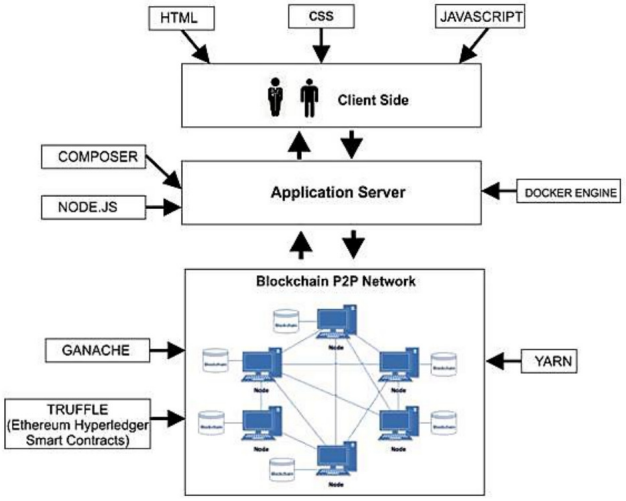

Figure 2: Architecture of a Secured HIS with blockchain technology

In the 3-tier architecture as shown in Figure 2, there is a client side, application server and the blockchain database, in which the server-side procedures, data memory access, data storage and user interface (UI) are created and kept up as autonomous modules on isolated stages.

The 3-tier design permits any of the three layers to be redesigned or supplanted freely. The UI is actualised on a workstation and utilises a standard graphical user interface with various modules running on the application server. The three layers in the 3-tier architecture are as follows:

i. Client Side: This is the first tier and shows data identified with services accessible on the desktop application. This layer speaks with different layers by sending results to the peer-to-peer network and different layers in the system. It is a platform that enables the client to interact with the system. The client side was built on Hypertext Markup Language (HTML), Cascading Style Sheet (CSS) and JavaScript.
ii. Application Server: This is the second, which is additionally called the business logic or logic layer. This layer controls application usefulness by performing comprehensive processing. This layer was built on node.js, composer, and Docker engine.
iii. Blockchain Database: This is the last tier of the architecture. This layer houses the database servers where data

is stored and recovered. Information in this tier is kept free of application servers or business logic. This layer was built on ganache, yarn and truffle (Ethereum Hyperledger Smart Contracts).

3.2. Activity Diagram

An activity diagram represents a series of actions or flow of control in a system similar to flowchart or a data flow diagram [31]. The activities modeled can be sequential and concurrent. Figure 3 shows the activities performed by each entity/class of the system and these activities are discussed thus:

i. The health personnel and patient attempt to login by entering their respective usernames and passwords, and await authorisation from the blockchain database. If the username and password is invalid it aborts the operation but if valid the users (health personnel and patient) gains access into the system and are assigned individual privileges.
ii. The health personnel views patients' medical history, diagnose, run tests on the patient and then upload the medical results into the system. The blockchain encrypts the medical result and shares to multiple participants in the network for consensus.
iii. The patient views the medical result uploaded by the heath personnel and can request for modification in biodata. The request is sent to the blockchain database and propagated across the network for subsequent approval or decline of the request. If the request is approved the changes are effected otherwise the operation is aborted. One participant cannot make changes without the cosensus of other participants in the network, otherwise the data is said to be compromised.

4. Experimental Results and Discussion

An implementation of the architecture of the proposed systems is given in this section. Several experiments were conducted to test the developed application for realising distributed access to medical data based on the design of Figures 2 and 3. The application used is built using existing technologies such as node.js, truffle smart contract, inter-planetary.

4.1. Testbed of the Experiments

The proposed system was implemented on a Windows machine running Windows 10 64-bit operating system, x64-based processor with 4GB RAM and Intel ® Core i3 6100U CPU @2.30 GHz 2.30GHz.

4.2. Software Components

An implementation of the architecture of the proposed systems is given in this section. The software used is built using existing technologies such as node.js, truffle smart contract, inter-planetary file system, Docker engine. With the implementation of the blockchain, medical records were cryptographically stored on a peer to peer network. The components used in building the software are as follows:

i. HTML: is the standard markup language for creating web pages. It describes the structure and elements of a web page.
ii. *CSS*: It is a style sheet language used for describing the presentation of a document written in a markup language like HTML.
iii. JavaScript: JavaScript, often abbreviated as JS, is a high-level, interpreted programming language that conforms to the ECMAScript specification.
iv. Python: Python is an interpreted, high-level, general-purpose programming language. Python has a design philosophy that emphasises code readability, notably using significant whitespace. It provides constructs that enable clear programming on both small and large scales.
v. GO: Go is a statically typed, compiled programming language that is syntactically similar to C, but with memory safety, garbage collection, structural typing, and CSP-style concurrency.
vi. Yarn (extension yarn.lock): In order to get consistent installs across machines, Yarn needs more information than the dependencies you configure in your package.json . Yarn needs to store exactly which versions of each dependency were installed. To do this Yarn uses a yarn.lock file in the root of your project.
vii. Docker Engine: It is the underlying client-server technology that builds and runs containers using Docker's components and services. Docker Engine supports the tasks and workflows involved to build, ship and run container-based applications.
viii. Electron.js: Formerly known as Atom Shell is an open-source framework developed and maintained by GitHub. Electron allows for the development of desktop GUI applications using front and back end components originally developed for web applications: Node.js runtime for the backend and Chromium for the frontend. Electron is the main GUI framework behind several notable open-source projects including Atom, Visual Studio Code, and Light Table.
ix. InterPlanetary File System (IPFS): InterPlanetary File System (IPFS) is a protocol and network designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system. IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files. IPFS could be seen as a single BitTorrent swarm, exchanging objects within one Git repository. In other words, IPFS provides a high-throughput, content-addressed block storage model, with content-addressed hyperlinks.

4.3. Results and Discussion

This section discusses the results of the experiments conducted to validate the efficacy of the proposed system. At the initial stage, a folder is created and populated with any category of health records either for the health personnel

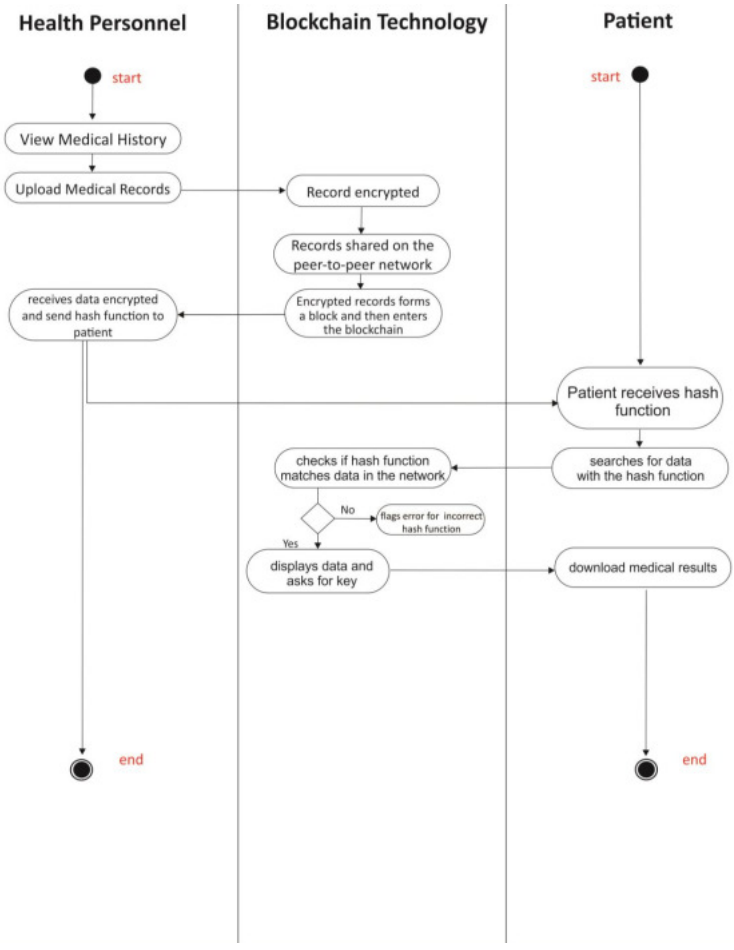

Figure 3: The Activity Diagram of the Proposed System

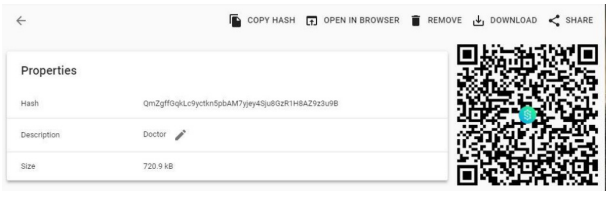

Figure 4: Encrypted Folder of Health Personnel

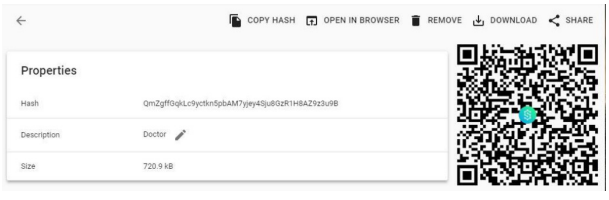

Figure 5: Encrypted Patient's Folder

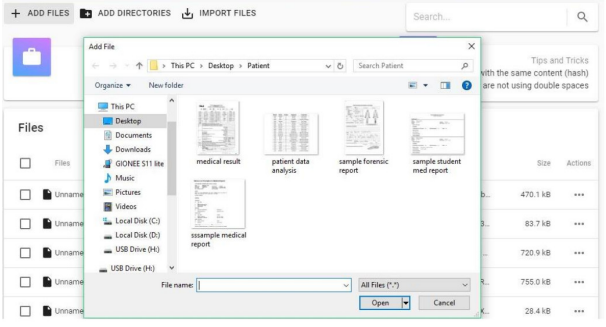

Figure 6: Adding File to the Encrypted Folders

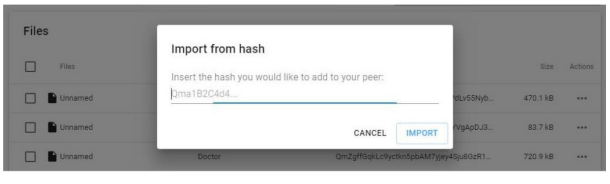

Figure 7: Importing Files with Hash Value

(doctor, nurse etc.) or the patient. This folder is then encrypted, for which a hash value is generated. The generated hash value as shown in Figure 4 can be used to perform such operations as the copying and sharing of the folder across the peer-to-peer network. Both the health personnel such as the doctors and the nurses, and the patients can participate in the viewing of the shared folder. The folder at the same time can be opened in a browser to view the records stored in it including the ability to download it to a local machine.

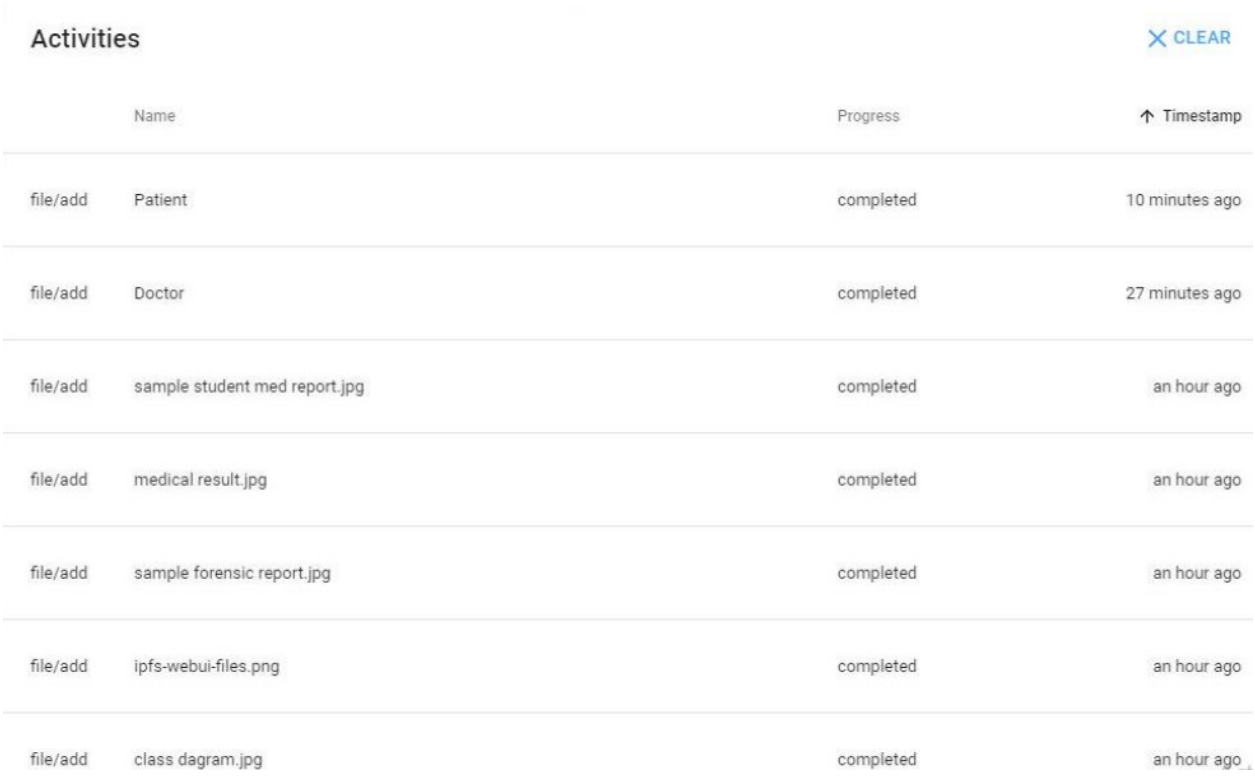

Figure 8: Activities on the Blockchain

Similarly, a patient's folder undergoes the same process as shown in Figure 5.

In the next stage, files are added to the created and encrypted folders for each entity participating in the blockchain. The added files are encrypted and hash values assigned to them to protect the integrity of their contents. This process is depicted in Figure 6.

Files can then be imported across the network and stored locally using the hash value earlier created for each file as illustrated in Figure 7. In this way, health personnel and patients have access to the health records transparently, and modifications to files are flagged when the hash values change.

All transactions (activities) in the blockchain by the different participating parties as well as the processes on data are also transparent and available to all nodes in the blockchain. Sample transactions are depicted in Figure 8.

Furthermore, we can view the total amount of data stored by multiple nodes participating in the network as well as the number of nodes connected to the blockchain per unit time. This number increases as more nodes participate in the blockchain (see Figure 9). In this sense, it is possible to maintain a transparent and distributed database of health records, which are cryptographically secure and immutable over time.

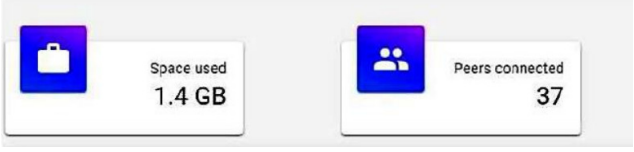

Figure 9: Used space and Peers Connected to the Blockchain network

5. Conclusion

The proposed system runs on a peer-to-peer network to eradicate the actions of a middle man or administrator. Interaction between the patient and health personnel, including having access to medical records shapes a crucial piece of the focal activities underlying health information systems. The proposed system was able to achieve the decentralisation of the medical records database to enhance the security and privacy of data on the modeled peer-to-peer network. The encryption of patients' data across the IPFS and the relevance of a public/private key pair to share, upload and download data on the blockchain network had an added advantage of the security and privacy of medical records. The proposed system was designed to aid health management organisations in the storage and retrieval of medical records. The system is modeled to tackle problems arising from data integrity, data security and the manipulations of medical records, which have been the major challenges in extant health information systems. Since the

blockchain is a public ledger that provides the information of all the participants and all digital transactions that have ever been executed, it helps to negate the relevance of authoritative access to a database of medical data. In this sense, the proposed system will bring about an accurate and efficient way of transferring medical records from health personnel to the patients without instances of record manipulation. For future work, we intend to provide a large scale implementation of this work on a district-wide basis to ascertain its resilience in real time.

Acknowledgment

The authors appreciate the handling editor and the reviewers for their valuable comments that improved the quality of this paper.

References

[1] K. A. Wager, F. W. Lee, & J. P. Glaser, *Health care information systems: a practical approach for health care management*, John Wiley & Sons, (2017).

[2] B. Chaudhry, J. Wang, S. Wu, M. Maglione, W. Mojica, E. Roth, ... & P. G. Shekelle, "Systematic review: impact of health information technology on quality, efficiency, and costs of medical care", Annals of internal medicine **144** (2006) 742.

[3] C. N. Chaulagai, C. M. Moyo, J. Koot, H. B. Moyo, T. C. Sambakunsi, F. M. Khunga, & P. D. Naphini, "Design and implementation of a health management information system in Malawi: issues, innovations and results", Health policy and planning **20** (2005) 375.

[4] R. Haux, "Health information systems–past, present, future", International journal of medical informatics **75** (2006) 268.

[5] M. Crosby, P. Pattanayak, S. Verma & V. Kalyanaraman, "Blockchain technology: Beyond Bitcoin", Applied Innovation **2** (2016) 71.

[6] M. Iansiti & K. R. Lakhani, "The truth about blockchain", Harvard Business Review **95** (2017) 118.

[7] J. Tan (Ed.), *E-health care information systems: an introduction for students and professionals*, John Wiley & Sons, (2005).

[8] L. Poissant, J. Pereira, R. Tamblyn, & Y. Kawasumi, "The impact of electronic health records on time efficiency of physicians and nurses: a systematic review", Journal of the American Medical Informatics Association **12** (2005) 505.

[9] R. Heeks, "Health information systems: Failure, success and improvisation", International journal of medical informatics **75** (2006) 125.

[10] G. Zyskind & O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data", In 2015 IEEE Security and Privacy Workshops (2015) 180.

[11] A. E. Ibor, O. A. Ofem, & J. N. Obidinnu, "A Conceptual Framework for Augmenting the Security of Digitized Academic Records in Nigerian Tertiary Institutions using Blockchain Technology", International Journal of Information Security, Privacy and Digital Forensics **2** (2018) 4.

[12] O. J. Ayangbekun & O. E. Ameenah, "Comparative analysis of existing health information systems for the development of Nigerian health sector", International Journal of Innovative Research in Computer and Communication Engineering **2** (2014) 4981.

[13] J. D. Halamka & A. Ekblaw, "The potential for blockchain to transform electronic health records", Harvard Business Review **3** (2017) 2.

[14] A. Azaria, A. Ekblaw, T. Vieira, & A. Lippman, "Medrec: Using blockchain for medical data access and permission management", In 2016 2nd International Conference on Open and Big Data (OBD) (2016) 25.

[15] A. Ekblaw, A. Azaria, J. D. Halamka, & A. Lippman, "A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data", In Proceedings of IEEE open & big data conference **13** (2016) 13.

[16] S. M. Shagari, D. Gabi, N. M. Dankolo, & N. N. Gana, "Countermeasure to Structured Query Language Injection Attack for Web Applications using Hybrid Logistic Regression Technique", Journal of the Nigerian Society of Physical Sciences **4** (2022) 832.

[17] S. K. Jagatheesaperumal, P. Mishra, N. Moustafa, & R. Chauhan, "A holistic survey on the use of emerging technologies to provision secure healthcare solutions", *Computers and Electrical Engineering* **99** (2022) 107691.

[18] M. Hölbl, M. Kompara, A. Kamisalic, & L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare", Symmetry **10** (2018) 470.

[19] L. Ismail, H. Materwala, & S. Zeadally, "Lightweight blockchain for healthcare", *IEEE Access*, **7** (2019) 149935.

[20] T. McGhin, K. K. R. Choo, C. Z. Liu, & D. He, "Blockchain in healthcare applications: Research challenges and opportunities", Journal of Network and Computer Applications **135** (2019) 62.

[21] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, & A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review", International Journal of Medical Informatics, **134** (2020) 104040.

[22] D. Efanov & P. Roschin, "The all-pervasiveness of the blockchain technology", Procedia computer science **123** (2018) 116.

[23] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, & F. Wang, "Secure and trustable electronic medical records sharing using blockchain", In AMIA Annual Symposium Proceedings American Medical Informatics Association **2017** (2017) 650.

[24] S. Angraal, H. M. Krumholz, & W. L. Schulz, "Blockchain technology: applications in health care", Circulation: Cardiovascular Quality and Outcomes **10** (2017) e003800, https://doi.org/10.1161/CIRCOUTCOMES.117.003800.

[25] T. T. Kuo, H. E. Kim, & L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedicaland health care applications", Journal of the American Medical Informatics Association **24** (2017) 1211.

[26] M. Wohrer & U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity", In 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE) **2018** (2018) 2.

[27] P. McCorry, S. F. Shahandashti, & F. Hao, "A smart contract for boardroom voting with maximum voter privacy", In International Conference on Financial Cryptography and Data Security (2017) 357.

[28] O. Ojo, M. K. Kareem, S. Odunuyi, & C. Ugwunna, "An Internet-of-Things based Real-time Monitoring System for Smart Classroom", Journal of the Nigerian Society of Physical Sciences **4** (2022) 297.

[29] X. Li, P. Jiang, T. Chen, X. Luo, & Q. Wen, "A survey on the security of blockchain systems", Future Generation Computer Systems **107** (2020) 841.

[30] C. K. Frantz & M. Nowostawski, "From institutions to code: Towards automated generation of smart contracts", In 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W) (2016) 210.

[31] J. Rumbaugh, I. Jacobson, & G. Booch, *Unified modeling language reference manual*, Pearson Higher Education, (2004).