International Journal of Computer Sciences and Engineering
Vol.**12**, Issue.**5**, pp.**28-34**, May **2024**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Article

Secured Framework for Electronic Medical Record Protection and Exchange Using Blockchain Technology

David Ademola Oyemade[1*], James Kolapo Oladele[2]

[1,2]Dept. of Computer Science, Federal University of Petroleum Resources, Effurun, Nigeria

**Corresponding Author: oyemade.david@fupre.edu.ng*

Received: 18/Mar/2024; **Accepted**: 20/Apr/2024; **Published**: 31/May/2024. **DOI**: https://doi.org/10.26438/ijcse/v12i5.2834

Abstract: The adoption of blockchains to effectively manage medical services is fast becoming popular for professional use and in patient-centered applications. Electronic medical records are highly sensitive with user-privacy data online with clinical services that relate to patients' diagnosis and treatments. The features of these medical records necessitate their availability, accessibility, agility, confidentiality and security. These have been demystified with the birth of the blockchain technology that seeks to proffer platforms and application services devoted to dependability and reliability amongst other features. Thus, we propose a blockchain health information framework for healthcare facilities. Our ensemble yields a permissioned blockchain using a hyper-fabric ledger. Using this state of technology on a peer-to-peer blockchain with various actors to include patient, practitioners and other users playing the roles of the creation, retrieval and storage of medical data for a patient to aid interoperability, our ensemble produce a query response time of 0.56 secs and https response time of 0.42 secs for 2500-users, and 0.78 secs and 0.63 secs respectively for 7500-users.

Keywords: Blockchain Technology, Electronic Medical Records, Data Security and Privacy, Interoperability

1. Introduction

Electronic medical records (EMRs) have revolutionised the standards of health records and transformed the health industry in the area of easy and seamless access to patients' medical records [1, 2]. However, the possibility of the manipulation of stored patients' data through the conventional storage approach still creates serious concerns about the security and privacy of patients' information. The healthcare environment is quite complex because multiple stakeholders are involved in complex and sensitive interactions with patients' data [3]. This can lead to privacy challenges, data insecurity, and operational inefficiencies. Trusted access to medical data is a critical process that must be made simpler, fast, and cost-effective.

EMRs are stored electronically and are extremely sensitive. Patients' personal information that includes details of diagnosis, prescriptions, drugs' administration and treatment requires frequent sharing among medical officials. Automating EMR has as its focal goal the issue of referrals to medical practitioners in other facilities for the purpose of cooperating with participatory health providers. Some of these providers with digital devices having the capability of data collection and insights generation, adopt the model of collaborations between medical practitioners and patients. Protecting the privacy of medical records is mandatory [4].

Low interoperability is common among many contemporary healthcare systems and providers. However, patients are not bound to specific clinics or medical consultants [5]. They are free to visit a doctor or be referred from a clinic, in which case, sharing the patient's historical medical information is necessary for better treatment. In addition to the issue of care coordination across healthcare centres, EMRs of a medical facility is not always available to another facility [6]. Furthermore, patients do not have control of their medical record and in some instances, data is tampered with, stolen, or shared without their consent [7]. A challenge in medical data exchange is interoperability [8]. Many health institutions use proprietary databases structured to be accessed only by their systems without permitting interoperability with others [9]. Patients must repeat their health history at every appointment, causing the loss of time and accuracy. At the same time, health records could have technical issues, due to the maintenance of standards for different purposes.

1.1 Blockchain Technology

Blockchain is a sophisticated data structure in which growing records are stored in blocks. There are four elements of the blocks. These are nformation, current block hash, previous block hash, and timestamp. Therefore, by design, every new data block that is added to the blockchain is connected to every other block. The use of a hash value makes it unchangeable; all workflow records are time-stamped, giving them identity, and copies are transferred to every participating network node. This ensures that data integrity is automatically maintained between endpoints [10, 11].

1.2 Blockchain Types

There are three types of blockchain in the market, based on application and consensus algorithms. These are public, private and consortium blockchains.

In public blockchain, the network can be joined by anyone for access to the block data. It uses public Distributed Ledger Technology (DLT), where anyone with internet connectivity can join to become an authorized miner for block mining. Nonetheless, in public blockchain networks, the identity address of the user is generated using a pseudo anonymous hash value. The address of a user is exposed to all but the activity of the user is hidden. Mining of blocks and examination of transactions can be done by a user after joining the network. For this kind of blockchain, successful miners enjoy financial incentives for helping to solve Proof-of-Work (PoW). Bitcoin [12], Ethereum (public), and Litecoin are examples of this type of blockchain. Because of the interaction costs, also known as transaction fees, imposed by public blockchains, users will always be paid for uploading or downloading documents, like electronic health records. Besides, public blockchain is designed in a way that any anonymous user can join the chain anytime. However, for blocks' addition, public blockchain is slow. Therefore, it is not ideal or recommended for EHRs management.

Private blockchain has similar operation and algorithms with public one but with a difference in its purpose and it is a restrictive or permissioned blockchain. Its operation is restricted to a closed, dispersed and centralized network and governed by access control rules. Private blockchain is used within an organization where one or more nodes control which node can perform transactions, act as miners or perform smart contracts. A TTP organization controls the aspects of its permissions, authorization and security. It is used for supply chain management and electronic voting and data preservation. Hyperledger Fabric [13] and Ripple [14] are top-notch illustrations of private blockchains. A private blockchain network cannot be joined by anybody without an invitation from approved staff members. It also adds blocks faster and consumes less power compared to the public blockchain. For this reason, managing EHRs on a private blockchain is recommended.

The consortium or hybrid boIckchain can be denoted as partly centralized and partly decentralized. it is not used by a single organization; rather, it is expanded in several organizations rather than being used by a single one. For accessibility, a group of nodes or a member must have previously registered. Legal activity by a single organization in a consortium blockchain is only possible with the consent of other organizations. An illegal activity is thereby prevented. The entire idea behind consortium blockchain was to let businesses to work together for operations' enhancement. Hyperledger Fabric, Quorum and Corda are examples of consortium blockchain.

This research paper addresses these drawbacks around interoperability, security, and privacy of EMRs. Enhanced interoperability standards can facilitate seamless data exchange between heterogeneous sources and cloud systems of an EMR systems. The remaining part of this paper is organized as follows: related works are discussed in section 2 while the methodology is discussed in section 3. Results and discussion are presented in section 4. The conclusion is given in section 5.

2. Related Works

In this section, previous works on blockchain and electronic medical records are discussed.

Saeed Banaeian Far and Maryam Rajabzadeh Asaar [15] proposed a blockchain framework to replace central authority with anonymous authority starting with a proposition that central authority cannot be trusted. The framework incorporates virtual blockchain protocol with embedded permission to eliminate the central authority.

Anton Wahrstatter, Sajjad Khan and Davor Svetinovic [16] introduced and developed a smart contract platform for decentralized federated learning and implemented with Ethereum blockchain. The primary objective of the system was to increase users trust in a decentralized blockchain system.

Awatef Salem Balobaid, Yasamin Hamza Alagrash, Ali Hussein Fadel and Jamal N. Hasoon [17] proposed a system that stores students names in blocks and replaces the conventional audit trail with a cryptographically secured equivalent. The system used deoxyribonucleic acid sequences and a chaotic system to simplify and strengthen the blockchain authorization process.

Arvind Panwar, Vishal Bhatnagar, Manju Khari, Ahmad Waleed Salehi and Gaurav Gupta [18] proposed a framework for managing personal health records that makes use of blockchain technology and IBM cloud data lakes for efficient healthcare administration. While the framework concentrated on increasing throughput and latency, they posited that the conventional blockchain approach typically reduces latency.

Honglei Li , Xiao Yang , Hongxin Wang, Wujia Wei and Weilian Xue [8] adopted Interplanetary file systems (IPFS) and blockchain technology to propose a blockchain-based, controlled, and secured EHR sharing program. The file system allows medical facilities to interchange and stores large-size EHR files while the blockchain-based abstract systems manages access to the EHR.

Ji Woong Kim, Su Jin Kim, Won Chul Cha and Taerim Kim [6] proposed a system which prevents data fabrication and falsification by transferring the section relevant to the patient's personal information off-chain and storing encrypted data on-chain. With thirty individuals participating, the application's usability was indicated by the system usability score of 74.0. Individuals with prior experience with blockchain demonstrated trust in the platform, whereas others without such experience desired an alternative method for safeguarding their data.

G. Verma, N. Pathak and N. Sharma [19] proposed a cloud environment framework which uses the blockchain for Electronic Health Data (EHD) management. It offers a secured cloud data storage and access with the use of Ethereum smart contracts, searchable Attribute-Based Encryption (ABE), and Amazon Web Services (AWS).

Sarath Sabu, H.M. Ramalingam, M Vishaka and, H.R. Swapna, Swaraj Hegde [20] noted the numerous privacy and security problems that existed with the current Internet of Things (IoT) and health record data sharing platforms and address this with the InterPlanetary File System (IPFS) and blockchain technologies.

M. J. H. Faruk, H. Shahriar, M. Valero, S. Sneha, S. I. Ahamed and M. Rahman [4] observed that customary methods for gathering, storing, and processing EHR data are centralized and associated with the risk of single point of failure which exposes the systems to numerous information breaches that jeopardize their availability and dependability. Consequently, they proposed a blockchain approach for remote patient monitoring using two of the primary blockchain frameworks.

D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne [22] proposed a system that integrates blockchain with cloud of things, offering creative ways to solve problems relating to decentralization and data security, while leveraging on its elasticity and scalability functionalities to boost blockchain operations efficiency.

R. Sangeetha, B. Harshini, A.Shanmugapriya and T.K.P. Rajagopal [22] proposed a system which keeps the patients' medical history on file in the blockchain block of data, with the Metamask used for information storage. The patients' data is encrypted using the SHA-256 technique, which converts it all into a single line of 256-bit encrypted text that will be kept in the block at etherscan.

In this paper, we proposes a blockchain framework for electronic medical record protection for improved interoperability and security, using hyper fabric ledger. This is the contribution of our paper.

3. Methodology

A blockchain is a distributed transaction ledger. It can be perceived as a distributed database in which a linear collection of data elements represents the blocks and are linked together to form a chain and secured by cryptographic primitives [23]. Each block's hash pointer is connected to the next. Hacking a blockchain requires hacking every block in the chain. This makes the system difficult to hack. Blocks are provably immutable first. This is made feasible because every block carries a hash, or numerical digest of its contents that can be used to confirm the accuracy of the transactions that it contains. Next, a block's hash depends on the hash of the block that came before it. As a result, altering the hash of any block practically makes the entire blockchain history unchangeable. Cryptographically linked blocks are shown in figure 1.

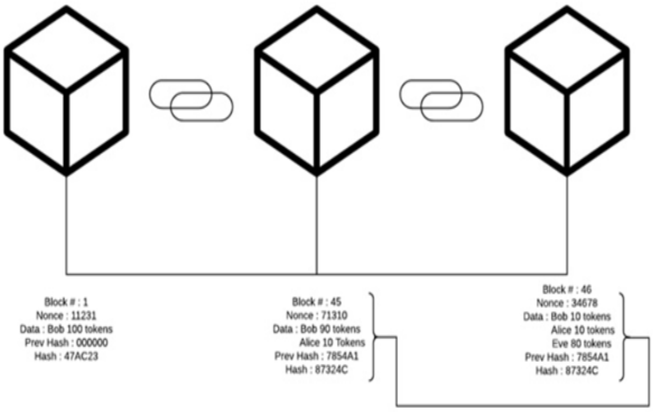


Figure 1. Cryptographically Linked Blocks [24]

The blockchain's size grows as the transactions' number increases. In addition, the transaction's order and time recorded are documented in the blocks. Every block has a timestamp, transaction data, and a cryptographic hash pointing to the block before it. Each computing resource can be thought of as a singleton state machine capable of cryptographically-secured transaction-based state transitions. Ethereum is the first company to attempt a complete implementation of this concept. It incorporates a storage capacity to support on-chain state and a Turing-complete instruction set to enable smart contract programming onto the blockchain [25, 26].

3.1 The Existing System

An electronic health record system without blockchain technology was examined and adopted as the existing system. Potential advantages of the suggested cloud-based HER system in the current investigation include cost savings, infrastructure consolidation, and consistent access to patient records (Abayomi-Alli et al., 2014). However, some issues such as security, interoperability, and privacy weaknesses were identified as drawbacks of the existing system and this could hinder effective adoption across healthcare organizations. Specifically, robust semantic interoperability protocols beyond a basic interface layer is absent and this could prevent smooth data integration between diverse hospital systems connecting to the cloud repository. Additionally, the reliance on simple username and password authentication exposes vulnerabilities to brute force attacks. The system also lacks end-to-end encryption mechanisms to protect health information confidentiality as well as granular privacy access controls and auditing to track appropriate data access according to policies (Abayomi-Alli et al., 2014). Figure 2 shows the data flow in the existing system and the connection of a systems of hospitals in a network with the authentication server and control database.

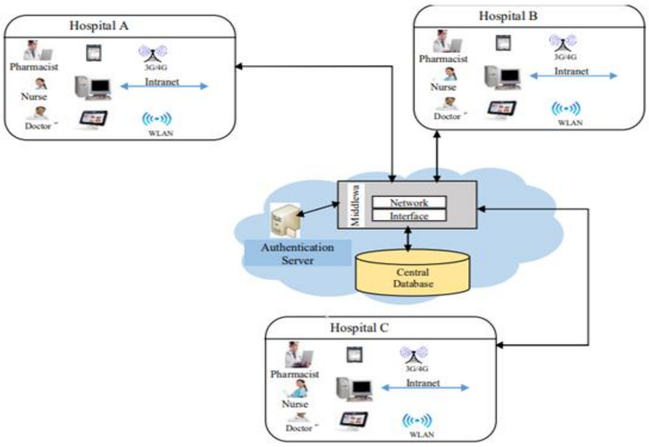


Figure 2. Data Flow of the Existing System [27]

Some of the weaknesses of the existing system include absence of the implementation of end to end encryption of the patients' data, lack of privacy control and usage auditing, and unclear ownership model of the data.

3.2 The Proposed Electronic Medical Records Framework

We propose electronic medical records framework which consists of three groups of modules: the patients, the health institutions and the decentralized block chain solution.

The patient group handles patients with the characteristics of mobility. That is the patients can seek medical advices from hospitals and clinics across a city, country and globe. The electronic medical records of the patients include basic patients' biodata and the mobility characteristics data.

The health institutions group is made of clinics that exist at different locations but registered in the same decentralized network. Each hospital in the module can access and maintain the EHRs of patients' data and the business logic. Figure 3 shows the data flow of the proposed framework. In Figure 3, Hospital 1, Hospital 2 and Hospital 3 represent the health institution module with their respective and accessible EHRs.
The decentralized blockchain group implements the blockchain operations. It consists of three logic layers: the electronic health record decentralized application programming interface, blockchain solidarity and the analytics. These are connected to MetaMask which controls the smart contracts and spring boost using Jason.

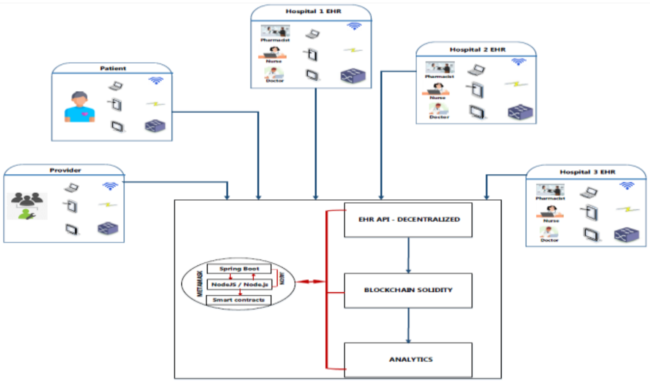


Figure 3. Data Flow of the Proposed Framework

In Figure 3, Patients are the primary users of the system. Patients can access and view their electronic health records through the system. Providers represent the healthcare providers, such as doctors, nurses, and other medical professionals. Providers can access and update patient records within the system. The Hospital EHR Systems represent the existing electronic health record systems used by different hospitals or healthcare organizations. These systems can interface with a cloud based EHR system through a standardized API layer. Cloud Database is the central repository where patients' EHRs are stored and accessed. It is designed as a distributed database architecture to avoid single points of failure. The API Layer module acts as an intermediary layer, providing a standardized Application Programming Interface for data exchange between the hospital EHR systems and the cloud database. It facilitates interoperability by allowing heterogeneous data sources to share and access patient records stored in the cloud. The Analytics module performs data analysis and generates insights from the aggregated health data stored in the cloud database. It provides valuable information for healthcare research, population health management, and decision-making.

When hospital 1 treats a patient, the data is time-stamped. When 2 treats the same patients after a period of time, hospital 2 will have a read access to the information of Hospital 1 but it cannot overwrite or edit it since it has a unique time stamp and linked to previous data in the block chain. Electronic records in the block include information about patients, vital signs, presenting complaints' history, medical consultants, laboratory, diagnosis, pharmacy and drugs' administration.

3.3 Materials

The robust implementation incorporates a suite of carefully chosen algorithms to fortify the system's security, performance, and scalability. BCrypt is employed for secure password storage, enhancing protection against unauthorized access. AES 256bit encryption is applied to safeguard sensitive data, ensuring confidentiality and integrity during transmission and storage. OAuth 2.0 algorithms govern token-based authentication, enhancing the system's security posture. Data transfer optimization was done with compression techniques, minimizing latency and bandwidth usage. Key management algorithms are employed to control and secure encryption keys, an essential component of the system's security infrastructure. Indexing and partitioning were implemented to ensure swift and efficient querying, particularly crucial for managing large datasets at scale. This amalgamation of proven technologies and algorithms culminates in a production-ready system designed for enterprise level use.

3.4 Blockchain Implementation for the Framework

Blockchain technology is integrated into the Electronic Health Record (EHR) system using smart contracts and the Ethereum blockchain. The implementation utilizes several technologies and frameworks, including Truffle, Ganache, IPFS, and MetaMask. Compilation of solidity with Truffle, a development environment and testing framework implemented Smart contracts. Ganache, an Ethereum blockchain, was used for testing purposes after employing it for development. Storing and sharing of data in a decentralized manner was done with the InterPlanetary File System. MetaMask, a browser extension, allows users to interact with decentralized applications built on the Ethereum blockchain. The front-end application was built using JavaScript and running on a local lite server.

4. Results and Discussion

This section discusses the performance metrics used for the analysis of the systems.

4.1 Response Time Performance Metrics' Application

The response time performance metric evaluates the time interval between a user's request and the actual feedback response time. This is achieved by tracking file downloads from FTP and Email Server. This gives the response time from a Database Query and a HTTP Page. The response time is shown in Figure 4 and Figure 5 using two scenarios and cases.

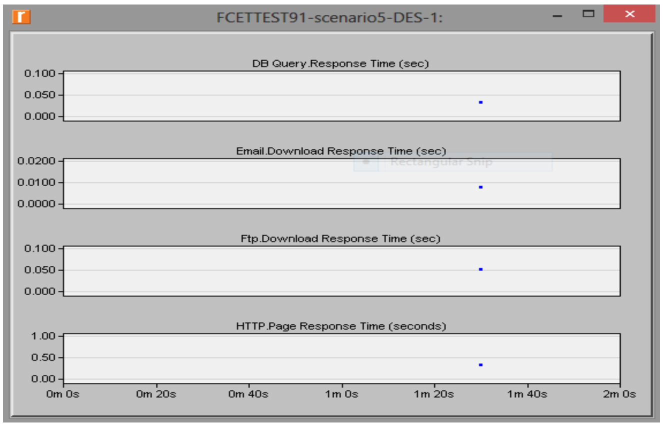


Figure 4: Response time with 2500-users

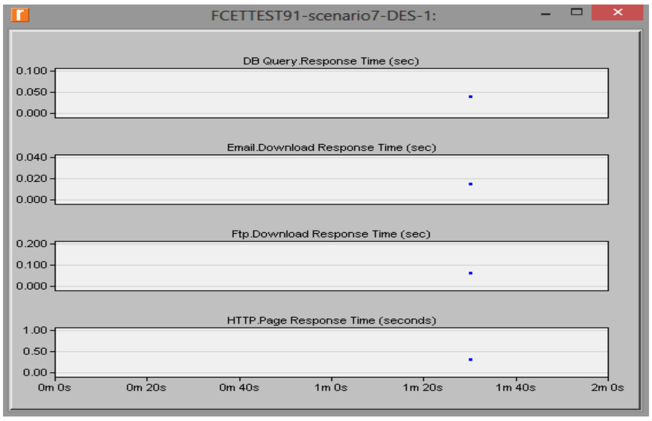


Figure 5: Response time with 7500-users

For the first scenario, the response time for our database queries was about 0.38 secs, for email download 0.008 secs, 0.052 secs for file download and 0.32 secs for page retrieval. For the second scenario, there was a longer response time as it took about 0.40 secs for database queries, 0.015 secs for email, 0.060 secs for file download and 0.35 secs for http retrieval. There was no significant difference in the response time for the various applications in both scenarios. With these results, we can conclude that the response time even with a doubled population is still very fast and it demonstrates that the system is highly scalable. The results of the simulation for the first and the second scenarios are shown in Table 1

Table 1: The results of the simulation for Scenarios 1 and 2

Items	Scenario 1 Time Secs	Scenario 2 Population	Scenario 1 Time Secs	Scenario 2 Population
DB Query	0.38	0.40	3512	7230
Email	0.008	0.015	3512	7230
FTP	0.052	0.060	3512	7230
HTTP	0.32	0.35	3512	7230

4.2 Application Throughput Performance Metrics

Throughput is the actual transfer rate of data in a medium over a given period of time. Being another performance metric test, throughput test is essential because the capacity of a network can be affected by interference and errors, thus making the stated capacity quite different from the actual capacity. For throughput, the data transfer rate of four LAN segments were analysed as in Figure 6 and 7 respectively.

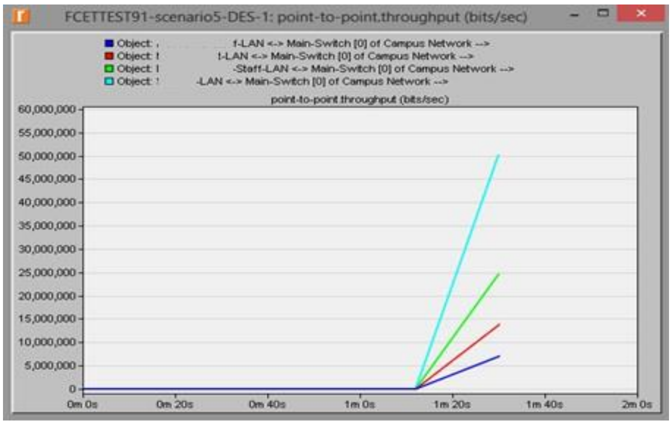


Figure 6: Throughput test for scenario 1

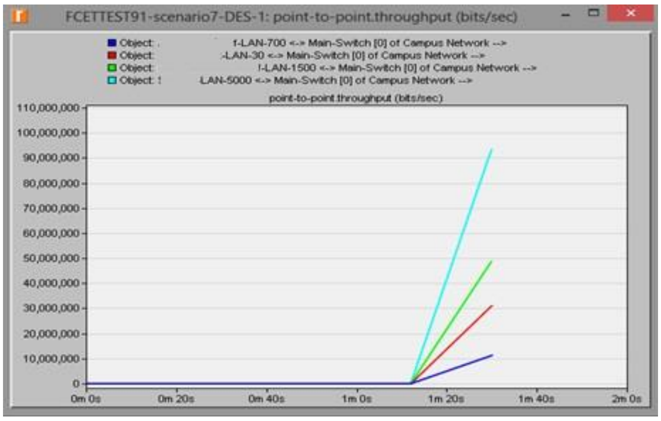
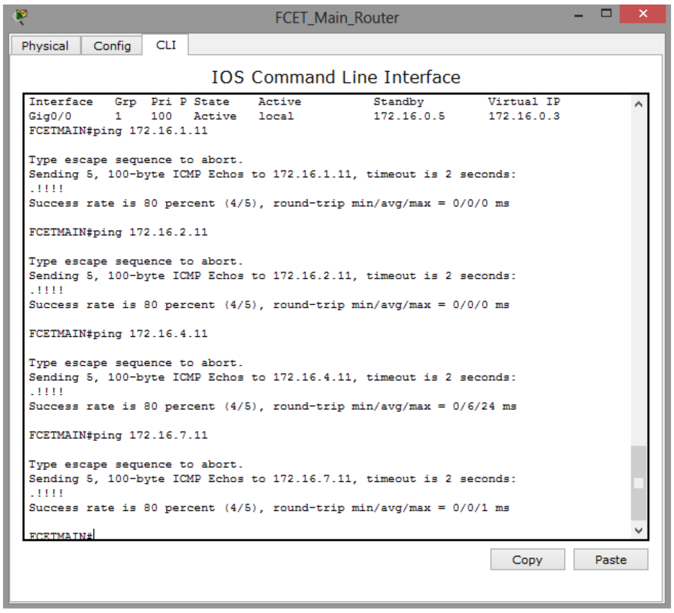


Figure 7. Throughput test for scenario 2

In scenario 1, the highest data transfer rate or throughput was about 50,000,000 bps (i.e. 47.68mbps); while the, lowest was about 7,000,000 bps (i.e. 6.68 mbps). For scenario 2, the highest throughput was about 94,000,000 bps (i.e. 89.65 mbps), and lowest was about 12,000,000 bps (i.e. 11.44 mbps). Reaching the different nodes on the network was accomplished with the ping command. The Internet Control Message Protocol is sent to different devices of the network via the ping command. Figure 8 shows its execution.



```
Interface    Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0       1    100   Active   local           172.16.0.5      172.16.0.3
FCETMAIN#ping 172.16.1.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

FCETMAIN#ping 172.16.2.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

FCETMAIN#ping 172.16.4.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.4.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/6/24 ms

FCETMAIN#ping 172.16.7.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.7.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

FCETMAIN#
```

Figure 8. Reachability Test for the Network

Figure 8 shows the different nodes sent and the response rate of 80%. This shows that the different nodes were reachable. Table 2 shows comparison of Existing versus Proposed System in terms of security measures, interoperability, database architecture and access control and auditing.

Table 2: Comparison of Existing versus Proposed System

Feature	Existing System	Proposed System
Security Measures	Limited security features with potential vulnerabilities	Robust encryption, Single Sign-On (SSO),
Interoperability	Relies on proprietary interfaces, limiting data exchange capabilities	Adopts standardized Application Programming Interfaces (APIs) for seamless data exchange
Database Architecture	Utilizes a centralized database structure	Shifts to a distributed database architecture.
Access Control and Auditing	Basic access control mechanisms and limited auditing capabilities	Implementation of granular access control and auditing mechanisms, safeguarding patient privacy.

The four comparison indicators in Table 2 show that the proposed system significantly improves on the existing system. The proposed system architecture represents a significant advancement over the existing design, addressing several key limitations and ushering in a new era of efficiency, security, and adaptability in the realm of Electronic Health Record (EHR) systems. The emphasis on enhanced security is evident through the implementation of robust encryption, Single Sign-On (SSO), and comprehensive access controls. This fortified security infrastructure and provides a resilient defence against unauthorized access and potential breaches. Secondly, the proposed architecture prioritizes interoperability by adopting standardized Application Programming Interfaces instead of proprietary interfaces. This shift ensures seamless data exchange between disparate healthcare systems, fostering a more interconnected and collaborative healthcare ecosystem. The transition from a centralized to a distributed database architecture represents a notable improvement, mitigating the risks of outages and enhancing system reliability. Additionally, the implementation of granular access control and auditing mechanisms not only bolsters security but also ensures compliance with regulatory requirements, thereby safeguarding patient privacy.

5. Conclusion and Future Scope

The security and immutability characteristics of the blockchain have made it a technology that is quickly gaining attention for its profitable applications in practical aspects of security challenges. Electronic health records need not only the protection of patients' data but also the mobility and interoperability of medical information within collaborative networks and health care organizations for easy and secured access to patients' information over wide geographical locations. The application of the blockchain technology is well suited for this because blockchain is inherently designed for use in a distributed and decentralized environment. This paper is the study of the application of blockchain and it proposes a secured framework for electronic medical record protection and exchange. The framework was implemented with Ganache, an Ethereum blockchain. Our ensemble produced a query response time of 0.56 secs and https response time of 0.42 secs for 2500-users, and 0.78 secs and 0.63 secs respectively for 7500-users. The proposed framework demonstrates a good scalability quality. Future work shall focus on the development of algorithms for block mining.

Data Availability
The data will be made available on demand.

Conflict of Interest
The authors declare that there are no conflicts of interest.

Funding Source
This research is funded by the authors. There is no external funding.

Authors' Contributions
David Ademola Oyemade reviewed the article, the framework and wrote the related works. James Kolapo Oladele wrote the first draft of the manuscript as a dissertation.

Acknowledgements
We acknowledge the efforts of professors who read the manuscript in its dissertation form.

References

[1] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, A. Abd-alrazaq, " The benefits and threats of blockchain technology in healthcare: A scoping review," International Journal of Medical Informatics, Elsevier, Vol. **142**, 104246, pp.**1-9**, **2020**.

[2] H. Dang, T. T. A. Dinh, D. Loghin, E. Chang, Q. Lin, B. C. Ooi, "Towards Scaling Blockchain Systems via Sharding," *In the Proceedings of the 2019 International Conference on Management of Data, ACM*, **2019**.

[3] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, M. Ishfaq, “Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet,” MDPI 14 (11): 1-22, **14 (11)**, pp.**1–22, 2022**.

[4] M. J. H. Faruk, H. Shahriar, M. Valero, S. Sneha, S. I. Ahamed and M. Rahman, "Towards Blockchain-Based Secure Data Management for Remote Patient Monitoring," *In the Proceedings of the IEEE International Conference on Digital Health (ICDH)*, Chicago, IL, USA, pp.**299-308**, **2021**.

[5] A. Khatoon, “A Blockchain-Based Smart Contract System For Healthcare Management. Electronics,” MDPI, **9** (**94**), **2020**.

[6] J. W. Kim, S.J. Kim, W. C. Cha, T. A. Kim, “Blockchain-Applied Personal Health Record Application: Development and User Experience,” Appl. Sci., MDPI, **12**, **1847**, **2022**

[7] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta and B. Ford, "OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding," *In IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, **2018**.

[8] H. Li , X. Yang , H. Wang, W. Wei, W. Xue, “A Controllable Secure Blockchain-Based Electronic Healthcare Records Sharing Scheme,”. Journal of Healthcare Engineering,v Hindawi, pp.**1-11**, **2022**.

[9] J. Liu, X. Sun, K. Song, “A Food Traceability Framework Based on Permissioned Blockchain. Journal of Cyber Security, **2**(**2**), pp.**107–113**, **2020**.

[10] S. Sayyad-Modi, R. K. Shingate, R. G. Jagtap, M. D. K., R. H. Sabale, “Smart Transfer Certificate Generator and Employer Verification Using Blockchain,” International Journal of Computer Sciences and Engineering, Vol.**11**, Issue.**6**, pp.**26-29**, **2023**.

[11] K. Saraf, “Fusing Blockchain and AI with the Metaverse: Unveiling the Future of Digital Transformation,” International Journal of Computer Sciences and Engineering, Vol.**11**, Issue.**9**, pp.**1-10**, **2023**.

[12] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,”, SSRN Product and Services, pp.**1-9**, **2008**.

[13] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, “Hyperledger Fabric: A Distributed Operating System For Permissioned Blockchains,” *In the Proceedings of 13th EuroSys Conference*, Article **30**, pp.**1-15**, **2018**.

[14] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, E. Zenner (2015). “Ripple: Overview and outlook," *In Proceedings of 8th International Conference on Trust Trustworthy Computing*, Heraklion, Greece: Springer, pp.**163180**, **2015**.

[15] S. B. Far, M. R. Asaar, “A blockchain-based anonymous reporting system with no central authority: Architecture and protocol,” Cyber Security and Applications, Volume **2**, **100032**, Elsevier, pp.**1-17**, **2024**.

[16] A. Wahrstatter, S. Khan, D. Svetinovic, “OpenFL: A Scalable and Secure Decentralized Federated Learning System on the Ethereum Blockchain,” Internet of Things, Vol. **00**, Elsevier, pp.**1**–**18**, **2024**.

[17] A. S. Balobaid, Y. H. Alagrash, A. H. Fadel, J. N. Hasoon, “Modeling of blockchain with encryption based secure education record management system,” Egyptian Informatics Journal, Vol.**24**, **100411**, Elsevier, pp.**1-11**, **2023**.

[18] A. Panwar, V. Bhatnagar, Manju. Khari, A. W. Salehi and G. Gupta (2022) A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake. Computational Intelligence and Neuroscience, Hindawi, Vol.2022, pp.**1-19**, **2022**.

[19] G. Verma, N. Pathak, N. Sharma, “A Secure Framework for Health Record Management Using Blockchain in Cloud Environment,” Journal of Physics: Conference Series, **1998 012019**, **2021**.

[20] S. Sabu, H. M. Ramalingam M. Vishaka, M. H. R. Swapna, S. Hegde, “Implementation Of A Secure And Privacy-Aware E-Health Record And Iot Data Sharing Using Blockchain,” Global Transitions Proceedings, Elsevier, Vol.**2**, Issue.**2**, pp.**429**–**433**, **2021**.

[21] Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding; Aruna Seneviratne, “Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges,” IEEE Communications Surveys & Tutorials, IEEE, Vol.**22**, Issue: **4**, **2020**.

[22] R. Sangeetha, B. Harshini, A.Shanmugapriya, T.K.P. Rajagopal, “Electronic Health Record System using Blockchain.” International Research Journal of Multidisciplinary Technovation, **1**(**2**), pp.**57-61**, **2019**.

[23] M. Usmana,. U. Qamar, “Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology,” Procedia Computer Science, Elsevier, Vol.**174**, pp. **321**–**327**, **2020**.

[24] H. L Gururaj, A. M. Athreya, A. A. Kumar, A. M. Holla, S M Nagarajath, V. R. Kumar, “A New Era of Technology,” Wiley, pp.**1-24**, **2020**.

[25] A. Ekblaw, j. D.. Azaria, M. D. Halamka, A. Lippman, “A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data,” MIT Media Lab, **2016**.

[26] D. Allenotor, D. A. Oyemade. “An optimized parallel hybrid architecture for cryptocurrency mining.” Computing, Information Systems, Development Informatics & Allied Research Journal; Vol.**12**, Issue **1**, pp.**94-104**, **2022**.

[27] A. Abayomi-Alli, A. J. Ikuomola,, I. S. Robert, O. O. AbayomiAlli, “An enterprise cloud-based electronic health records system.” Journal of Computer Science and Information Technology, **2**(**2**), pp.**21-36, 2014.**

AUTHORS PROFILE

David Ademola OYEMADE is an Associate Professor of Computer Science at the Federal University of Petroleum Resources, Effurun, Delta State, Nigeria. He holds a PhD degree in Computer Science obtained from the University of Benin, Benin City, Nigeria in 2014. He also holds M.Sc. degree in Computer Science obtained from the University of Benin, Benin City, Nigeria in 2007 and a postgraduate diploma in Computer Science obtained from the University of Benin, Benin City, in 2004. He is a life member of Nigeria Computer Society (NCS) and a professional member of Association for Computing Machinery (ACM). He has served as a lecturer in the Department of Computer Science, Federal University of Petroleum Resources, Effurun and rose through various ranks. He has supervised several students of at undergraduate and postgraduate levels at the department of Computer Science, Federal University of Petroleum Resources, Effurun. He has many articles in international and local journals. His research area is Software Engineering, Software Architecture, Intelligent Systems and financial market algorithms and modelling.

James Kolapo Oladele earned his B.Sc. form University of Benin, Benin City, Nigeria. He completed M.Sc. in Computer Science from Federal University of Petroleum Resources, Effurun, Delta State, Nigeria in 2024 with his result awaiting Senate approval.