JCTA Journal of Computing Theories and Applications ISSN:3024-9104

Research Article

BEHeDaS: A Blockchain Electronic Health Data System for Secure Medical Records Exchange

James Kolapo Oladele[1], Arnold Adimabua Ojugo[1*], Christopher Chukwufunaya Odiakaose[2], Frances Uchechukwu Emordi[3], Reuben Akporube Abere[1], Blessing Nwozor[1], Patrick Ogholuwarami Ejeh[2] and Victor Ochuko Geteloma[1]

[1] Department of Computer Science, Federal University of Petroleum Resources Effurun, Nigeria;
e-mail : kolapooladele@gmail.com, ojugo.arnold@fupre.edu.ng, abere.reuben@fupre.edu.ng, ako.rita@fupre.edu.ng, blessing@fupre.edu.ng, ochukov@gmail.com
[2] Department of Computer Science, Dennis Osadebay University Anwai-Asaba, Delta State, Nigeria;
e-mail : osegalaxy@gmail.com, patrick.ejeh@dou.edu.ng
[3] Department of Cybersecurity, Dennis Osadebay University Anwai-Asaba, Delta State, Nigeria;
e-mail : emordi.frances@dou.edu.ng
* Corresponding Author: Arnold Adimabua Ojugo

Abstract: Blockchain platforms propagate into every facet, including managing medical services with professional and patient-centered applications. With its sensitive nature, record privacy has become imminent with medical services for patient diagnosis and treatments. The nature of medical records has continued to necessitate their availability, reachability, accessibility, security, mobility, and confidentiality. Challenges to these include authorized transfer of patient records on referral, security across platforms, content diversity, platform interoperability, etc. These, are today – demystified with blockchain-based apps, which proffers platform/application services to achieve data features associated with the nature of the records. We use a permissioned-blockchain for healthcare record management. Our choice of permission mode with a hyper-fabric ledger that uses a world-state on a peer-to-peer chain – is that its smart contracts do not require a complex algorithm to yield controlled transparency for users. Its actors include patients, practitioners, and health-related officers as users to create, retrieve, and store patient medical records and aid interoperability. With a population of 500, the system yields a transaction (query and https) response time of 0.56 seconds and 0.42 seconds, respectively. To cater to platform scalability and accessibility, the system yielded 0.78 seconds and 063 seconds, respectively, for 2500 users.

Keywords: Electronic Health Records; Blockchain; Records Exchange; Interoperability; HIPAA.

Received: November, 26th 2023
Revised: January, 4th 2024
Accepted: January, 5th 2024
Published: January, 6th 2024

1. Introduction

Advances in informatics have contributed immensely to healthcare delivery – even with its inherent challenges [1]. Healthcare systems and platforms today are poised to yield patient-centric apps [2]. Patients today are not limited to receiving medicare at specific hospitals. Especially during emergencies or when a patient is unconscious [3] – exchanging patient records is a panacea to improved healthcare. Tracking a patient's medical history becomes critical, mandatory and imperative [4]. Thus, there is a need for electronic medical records (EMR). Patient records and history are often not readily available to expert personnel to medical facilities other than where such records are created [5]. Other include: (a) issues of care coordination, (b) non-provision of telemedicine, as patients have access and control of their medical records [6]–[8], (c) corruption of patient records via tampering, stealing, or mishandling [9], and (d) patient record exchange with unauthorized medical experts with or without a patients' consent [10]–[12]. With EMRs – critical platform interoperability issues for data exchange, confidentiality, privacy, and security must be addressed urgently.

Traditional collection, storage, and processing of electronic health records utilize centralized techniques that pose several risks and lean systems toward a number of data breaches and attacks that compromise data availability [13]–[15]. The blockchain is gradually resolving

DOI : 10.62411/jcta.9509

these challenges with its immutability feat that prevents records alteration. Adapting blockchain in healthcare will improve user-trust and dissemination of private healthcare records [16], [17]. Blockchain is today advanced as a solution with a plethora of features such as transparency, improved authentication, and consensus verification, amongst other unique record sharing capabilities [18]. Blockchains have addressed many challenges to healthcare; While, offering businesses a chance to leverage, harness, and fuse with other emerging technologies [19], [20]. Besides interoperability, the lack of standards for developing blockchain healthcare apps must be addressed as it will ensure a transformative approach for practitioners and researchers [21]–[23].

A blockchain is an incorruptible, distributed database – maintained and validated over a network of interconnected nodes globally [24], [25]. Blockchain quickly resolves the inherent challenges experienced with conventional databases. It records a timestamp to a node to avoid data tampering [26]. There are various blockchain types, namely the private/permissioned, public/permissionless, consortium, and hybrid. Each of these has its ideal uses, numerous benefits, and drawbacks [27]. For the study, we adopt a permissioned blockchain, which: (a) supports controlled access as extra security to patient medical records from unauthorized (non-stakeholder) access, (b) supports customization and identity verification that grant stakeholders access on the networks – as opposed to having users approve each other, (c) supports a network of known participants and high-yield in fault tolerance that supports the platform to keep running always, (d) it yields a higher transaction throughput as participants are preselected, and (e) it requires low energy consumption during mining and with its business transaction logic [28]. In all, the permission mode has less complicated algorithms and a less complex, ease-to-secure model as users (i.e., patients, medical experts, medicare officers, and a host of medical care facilities) are the only stakeholders who can have access to patients' medical records as well as involved in the exchange therein.

The public blockchain is a major type that is both open and decentralized, as it is accessible to anyone. Each validated person helps validate transactions using proof-of-work and proof-of-stake. They are non-restrictive and use distributed ledgers that require no permission, as any user can be authorized to access any part of data they wish to access. The consortium blockchain is semi-decentralized for organizations wishing to manage effectively their own network. Thus, the blockchain can exchange data and mine as well. The hybrid blockchain is a merger of both the public and private blockchain. Better control is required to achieve higher goals as they are centralized with decentralized nodes/systems, which are not open. It yields better security than a public network (though not better than the private blockchain), greater integrity and transparency, and various benefits [29].

With peer-to-peer participation on consensus, there are 2-modes: permissioned and permissionless. For permissionless, any node may participate to reach a consensus over the order of transactions. This is true for Ethereum, But Fabric/Corda is used when users are selected in advance with restricted access to the network [30]. Corda allows better access control to records and enhances privacy; it achieves greater performance only when all transaction participants have reached a consensus [31]. Conversely, the consensus within the fabric ledger starts from proposing to committing a transaction on ledger. Each node (with roles as clients, peers, and orderers) assumes different tasks in reaching a consensus. A client creates and invokes a transaction, communicating this with other peers/orderers. The peer maintains the ledger, while the orderers provide a channel to clients and peers over which message is broadcasted. The channel then ensures that all connected peers deliver the same message in the same logical order [32]. To ensure each record is a complete keyset, with its state initialized as a record in the world state, we use a hyper-fabric ledger. Thus, the record supports several states with attributes that allow the same ledger in its world state to hold various records of the same patient. This will ensure the system evolves and updates its state(s) and structure with the addition of more records [33]–[35].

The study implements an electronic medical information system for improved service delivery with transaction authentication and validation that ensures confidentiality, interoperability, etc., to comply with the regulations and standards of the Health Insurance Portability and Accountability Act (HIPAA) in Nigeria. HIPAA compliance ensures healthcare providers in Nigeria adhere strictly to standards (i.e., policy framework) targeted at the protection of patient health records to ensure privacy and data security

2. Related Literature(s)

2.1. The Blockchain Technology

The blockchain has become one of the greatest innovations. It is designed to foster peer-to-peer financial portfolios [36] and is used as smart contracts in various robust and flexible domains. It is a shared database ledger of digital transactions distributed among interconnected nodes called a blockchain [37]–[39]. Each node on the blockchain refers to a computing (physical and/or virtual) device, as in Figure 1. Its benefits are inherent in its feats and characteristics, including records immutability, data decentralization, consensus validation, data security, etc [40]–[42]. Adopting and adapting the blockchain platform for new applications helps to decentralize data storage and render it immutable so it cannot be owned, edited, controlled, or manipulated by a central authority. A blockchain is a network of nodes (or a chain of blocks) containing information [43]. Stored data in each block depends on blockchain type, and each block consists of (a) data, (b) hash, and (c) a hash of the previous block. Blockchain uses hashing, distributed peer-to-peer networks, and proof of work schemes to ensure data security, non-repudiation, integrity, and immutability in the chain [44]–[46].

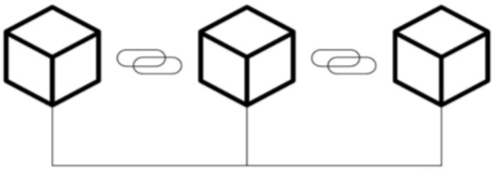


Figure 1. An illustration of cryptographically linked blocks (source: [47])

Each new data or node to be added to the blockchain – is broadcasted first throughout the blockchain for audit and verification via the peer-to-peer network. Using pre-approval rules in the chain, addition approvals are achieved via a consensus mechanism prior to the addition, and each new data or node added to a chain is referred to as a new block. And to ensure its security, records of this new block are distributed across the chain. At the same time, the smart contract supports the chain's performance to ensure that all transactions remain credible with(out) a middle party. Thus, by default – the blockchain was designed from the ground up to help ensure non-repudiation, protection cum transference of valuable data [48]–[51].

2.2. The Electronic Health Information System

An electronic health record (EHR) is an electronic mode to document and store patient records and clinical workflows [52] – allowing patient data to be readily and securely available to users. Widespread adoption of EHR is encouraged [53] with the rise in the cost of healthcare [54] and the continuous request for patient records with a variety of encounters with other healthcare experts. The records include a patient's progress, prescriptions, vital signs, previous medical history, laboratory results, and radiological reports [55], as in Figure 2.

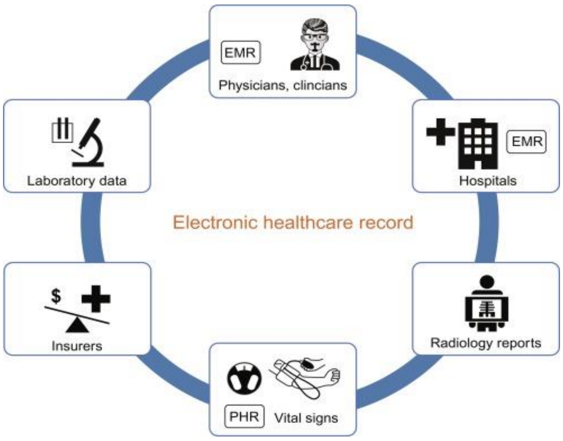


Figure 2. Key components of the EHR (Sources: [62], [63])

An EHR automates a clinical workflow and can yield an exhaustive patient record of clinical encounters – to assist (in)directly in care-related tasks via the interface with decision support, quality management, and outcome reports [56]–[58]. Healthcare practitioners and facilities use EHR to improve the coordination of care, the quality and safety of treatment, the efficiency of care delivery, and patient access to information to encourage patient involvement in health-related choices [59], [60]. Protecting patient data is paramount and critical in adopting EHR, as its maintenance tries to dissect and examine noticeable security procedures for healthcare associations trying to implement a safe EHR platform [61].

Health data exchange seeks to offer medical practitioners and facilities the ability to electronically transfer patients' medical records from one facility to another while maintaining data security and confidentiality during such exchange [64], [65]. Patients records today (even when electronically available) are reposited by various healthcare facilities using a variety of formats, especially when they explore applications from various (disparate) healthcare vendors. Also, these records are accessed by a community of healthcare practitioners; Thus, many of these applications are interoperable [66], [67]. This can make it difficult – a practitioner's complete access to a patient's medical records, especially when referred or hospitalized in a facility not of their choosing. By extension, such patients can be made to repeat tests already initiated in their major healthcare facility of choice due to non-access to prior patients' records [68], [69]. Healthcare providers cannot afford to take an application-centric approach to interoperability by migrating major clinical applications to new systems or performing major upgrades. This is bound to cause new performance issues, scalability, and other features that seek to consume computing resources to emerge [70], [71].

Data exchange protocols are critical as they help ensure a data-driven response, especially if there are interoperability gaps [72]. The interoperability gap yields non-harmonized patient health needs, Leading to poorer outcomes and higher medicare costs [73]–[75]. For effective data exchange amongst medical organizations, providing interoperable systems to help attain better patient care has become imperative. And thus, adopt a uniform standard for data exchange – poised to interface and integrate a variety of data structures to help achieve interoperability [76]. Interoperability is a secure access, integration, and timely adaptation of clinical data explored to help optimize health outcomes in all scenarios [77]–[79]. Its goal is to promote retrieval/access ease of clinical records to yield timely, equitable, and efficient patient-centric care [80], [81]. Some benefits of adopting medical data exchange standards: (a) data integration across all systems and platforms in a variety of healthcare facilities, (b) improved data for faster, effective decision-making, (c) yields quicker and more reliable billing and claims processing, and (d) better compatibility and compliance to reduce data inconsistencies on referrals [82].

3. Material and Method

3.1. The Electronic Health Information Dataset

The study was conducted at the Asaba Specialist Hospital (ASH), Delta State in Nigeria. ASH has a range of healthcare personnel with operational 24-hour, 7-days-a-week healthcare services. As a flagship healthcare center, her administrators ensure patients' records are maintained both digitally and in paper forms in filing cabinets. This also poses a range of complications, such as privacy, missing records, confidentiality, and other inefficiencies. ASH currently has over 287 healthcare professionals (HCPs) to serve an estimated 123,273 residents, and it is growing. Her healthcare officers at various levels retrieve and maintain patient records with various departments. We sampled 34 participants (n=9, 21% physicians; n=11, 36% midwives and nurses; and n=14, 43% health records officers) via purposive sampling as they were directly involved with patient data at ASH Asaba. The study commenced with remote scoping in November 2022, to include readiness assessment via an open-ended interview with our ASH contact person, initial workflow analysis, and risk analysis through email or Zoom consultation with the management team of ASH Asaba. Also, to ensure the network uses the consensus mechanism to authenticate data addition, amendments, and deletion – we added 464 patients, totaling 500 users for the blockchain system.

3.2. The Proposed System

Deciding permission needs on a blockchain is the first critical and pivotal architectural step to deploy the blockchain solution as a distributed ledger technology (DTL). A confluence of societal forces, economic norms, and business logic confronts businesses with renewed urgency regarding when, how, and whether to employ/deploy the blockchain-based application/platform. DTLs in record keeping aid transaction security, interaction, validation, and authentication of records verified across a network [83].

In contrast to the permissionless blockchain for which (a) transactions are fully transparent, (b) are open-source development, (c) have a greater level of anonymity, and (d) explores tokens and other digital assets as incentives – our study will explore the permissioned (private) blockchain for which transactions: (a) yield controlled transparency in lieu with the goals of participating businesses (i.e., healthcare facilities), (b) does not require complex algorithms to implement its smart contracts, (c) requires a level of anonymity (as patients are interested in experts handling their medical records), (d) uses decentralized authority for which medical facilities authorize and decide on exchanged records [84].

We use a 3-tier framework for our medical records exchange blockchain to create secure, transparent storage for medical records. It serves as its hidden database to aid exchanged data authentication and security. As in Figure 3(left), the blockchain, and 3(right) its chain-codes, respectively, our 3-tier n-client framework aids the effective transfer of medical records via the blockchain. The logic layer processes data by interfacing with the hash-codes in each blockchain to ensure the integrity of the medical records. Each hash-code is generated via the hyper-ledger fabric, which maps an input of varying length (i.e., a patient's medical data) to a hashed output of a fixed length. This hashed output value record then morphs as the block of data for the medical record, changes. The blockchain nodes then inspect and validate any new medical record as a store or retrieve transaction requests. Each request is filed via a distributed consensus by various validating nodes (as no single node on a chain validates or has central control of the network). Thus making it tedious for medical records to be altered, distorted, corrupted, compromised and/or stolen [12].

We created a user interface to help effectively manage data memory access, server-side procedures, and storage while keeping each as an autonomous segment on isolated stages using the n-fat client framework. Our 3-tier design allows each layer to be redesigned or supplanted freely without system downtime. The design architecture is thus [85]: (a) the client module, which identifies data with allowable services accessible on the app. This layer enables a user to interact with other layers in the system by sending user query results via a P2P network, (b) the application Server yields the business logic of the blockchain. It controls the application and yields smart contracts using the hyper-fabric ledger, and (c) the blockchain database houses the business logic – acting as a database server for data storage and recovery.

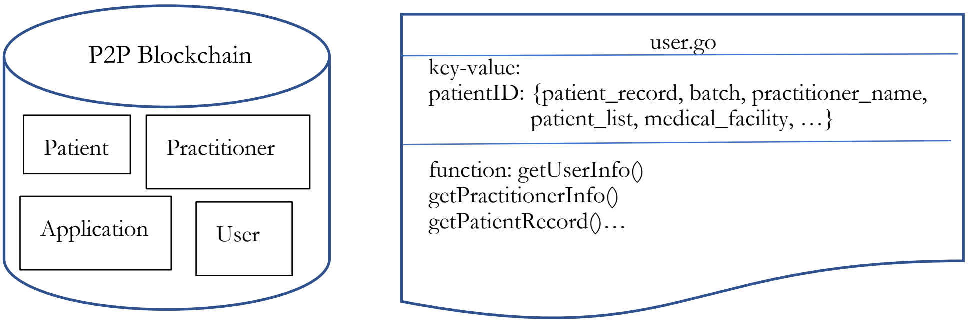


Figure 3. (left) BEHeDaS Blockchain, and (right) BEHeDaS chain-codes

3.3. The BEHeDaS Activity Diagram

An activity diagram represents a series of actions or flow of control in a system similar to a flowchart or a data flow diagram. The activities performed by each entity/class of the system are modeled as in Figure 4 and further explained thus:

1. The health personnel and patients attempt to log in by entering their respective usernames and passwords and awaiting authorization from the blockchain database. If the username and password are invalid, it aborts the operation, but if valid, the users (health personnel and patient) gain access into the system and are assigned individual privileges [85].

2. The health personnel views patients' medical history, diagnose, run tests on the patient, and then uploads the medical results into the system. The blockchain encrypts the medical result and shares it with multiple network participants for consensus.
3. The patient views the medical result uploaded by the health personnel and can request 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 then amended; Otherwise, the operation is aborted. One participant cannot make changes without the consensus of other participants in the network otherwise, the data is said to be compromised.

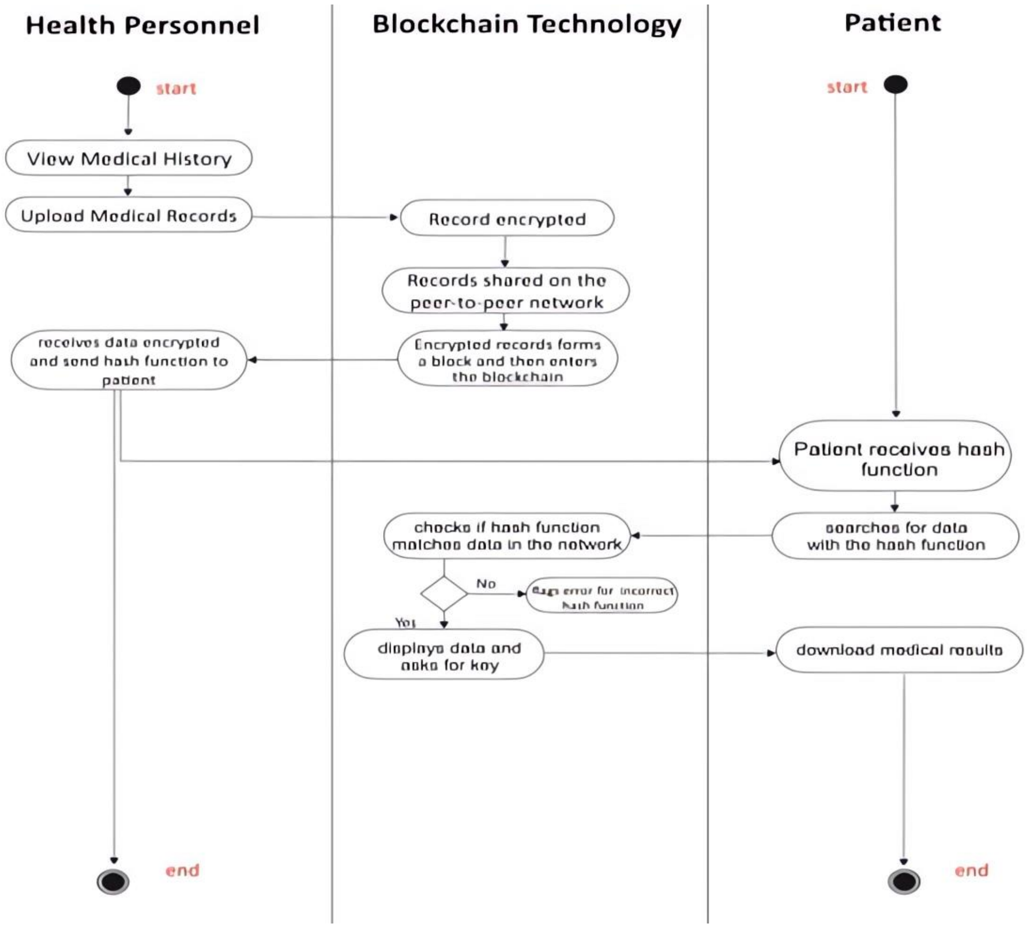

Health Personnel
Blockchain Technology
Patient
start
start
View Medical History
Upload Medical Records
Record encrypted
Records shared on the peer-to-peer network
receives data encrypted and send hash function to patient
Encrypted records forms a block and then enters the blockchain
Patient receives hash function
checks if hash function matches data in the network
searches for data with the hash function
No
flags error for incorrect hash function
Yes
displays data and asks for key
download medical results
end
end

Figure 4. The BEHeDaS Activity Diagram

3.4. The BEHeDaS Structure and Chaincodes

The chain code (s), as in Figure 3 (right), details the transition of records between actors (i.e., patient, practitioner, database) and how medical records are distributed and change their state from one stakeholder to another. These transactions use the smart contracts' logic to execute and regulate these transitions and yield traceability, transparency, and efficiency of these records as they move between these unique states [86]. The BEHeDaS records and states are stored in the hyper-fabric ledger. Details of the chain-code structure is as thus [87], [88].

Stage 1: Ledger State – The medical record represents a set of properties with assigned values that create a unique keyset as well as the state of the patient record. The patient_list is the complete keyset, initializing its state as a record in the world state on the hyper-fabric ledger. This record supports several states with attributes that allow the same ledger in its world state to hold various records of the same patient. This ultimately makes it possible for the system to evolve and update its state(s) and structure.

Stage 2: Proof-of-Trust – With a variety of roles to include (and not limited to) patients, practitioners, application, users (i.e., medical personnel, nurses, etc.), and the varying transaction(s) – the smart contract must have enshrined therein it procedures for (a) transition of the patient records between the actors, (b) how different business interests must approve a transaction, and (c) how each individual state keys work. It implies that BEHeDaS must set a rule in the namespace to define a business logic/transaction that processes a specific patient_record as well as set another to update all retrieved/processed record assets to portray trust relations of the transactions.

Stage 3: Smart Contract – Here, a smart-contracts code sets all valid states for a patient record and the logic that transitions it from one state to another. The smart contract sets up key business processes and information to be shared across various actors interacting on the network. It defines the various states of a business manages the various processes to move an asset/record between these states. In the BEHeDaS network, the same smart contract is shared and used by the different nodes and by the different applications connected therein. Thus, it jointly executes a shared business data and processes. All members of the network must agree a specific version of smart contract to be used

The BEHeDaS framework ensures the system complies with the HIPAA. This is demonstrated via robust implementation of the blockchain traceability processes to manage and secure patient records effectively. It aligns and takes into account Nigeria's healthcare landscape in lieu of its regulatory and business environments. It also covers a range of activities, including patient information processing, storage, transmission and traceability management, and security via the confidential handling of protected health information. Thus, will improves patient trust, healthcare expert collaboration, traceability, and care quality [89]–[91].

4. Results and Discussion

4.1. The BEHeDaS Throughput / Availability

We used the Riverbed 18.0 to test for throughput (and determine the data transfer rate between nodes on the network system over a period. Thus, we measure the number of transactions performed on the network per second for BEHeDaS, as shown in Figure 5. TPS for private chains is often low (i.e., not above 30tps) [92] – as they are specifically for consensus users by adopting a less complex proof of work that enables users to compute the problem during mining. Thus, it requires a lot of computational power and processing time. It takes Ethereum about 420 seconds for public chains to generate a block [93] – making such public chains ineffective in meeting management needs. The observed TPS is about 1105.

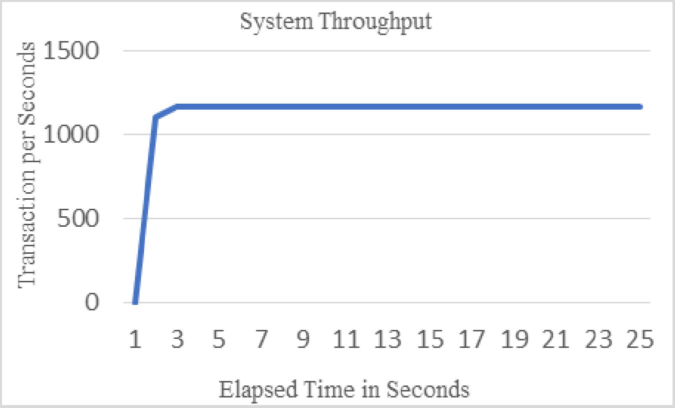


Figure 5: The BEHeDaSE Ensemble Throughput

4.2. Scalability / Application Response Time Performance Evaluation

This performance metric seeks to determine the time interval between a user's request and application response time for feedback to a user. Thus, we measure the response time for each query. To measure the system's scalability, we present 2-cases with (a) 500 users and (b) 2500-users. Querying a record means reading data from the hyper-fabric ledger, stored as a world state (the database that records only key-value pairs). Using the world state, a query retrieves directly current key-value(s) of record sought for without traversing the whole ledger. This improves the effectiveness and efficiency of BEHeDaS [51], as shown in Table 1.

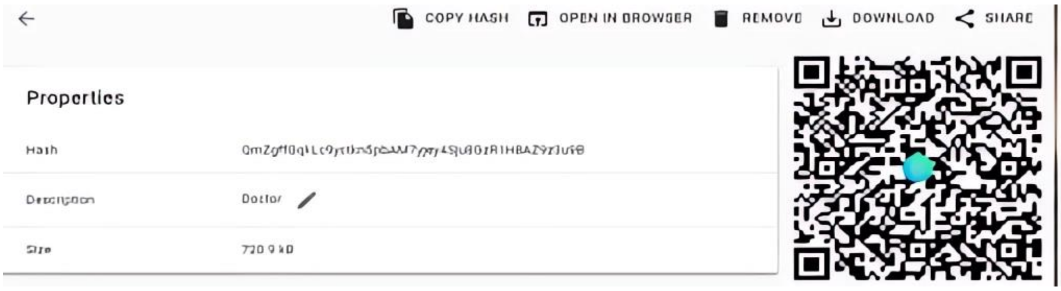
Table 1. Application Response Time / Scalability

Items	Case-1		Case-2	
	Time	Population	Time	Population
Query	0.56secs	500	0.78secs	2500
File	0.48secs	500	0.69secs	2500
Https	0.42secs	500	0.63secs	2500

With a size of 500 users, it yields a response time of 0.56 seconds and 0.42 seconds, respectively, for both queries and page retrieval [16]. With a 500-percent increase in user size, the system yielded a longer response time of 0.78secs and 0.63secs for queries and HTTP page retrieval.

4.3. Result Findings

To validate the efficacy of the proposed system – folders are created and populated with various categories of medical health records either for the health expert professionals' access (i.e., doctors, nurses, etc) or the patient, as in Figure 6. The generated hash value is then used to perform operations such as copying and sharing the folder across the peer-to-peer network. Both the health personnel, such as the doctors and nurses, and the patients can participate in viewing the shared folder. At the same time, the folder can be opened in a browser to view the stored records, including the ability to download it to a local machine, as in Figure 7.



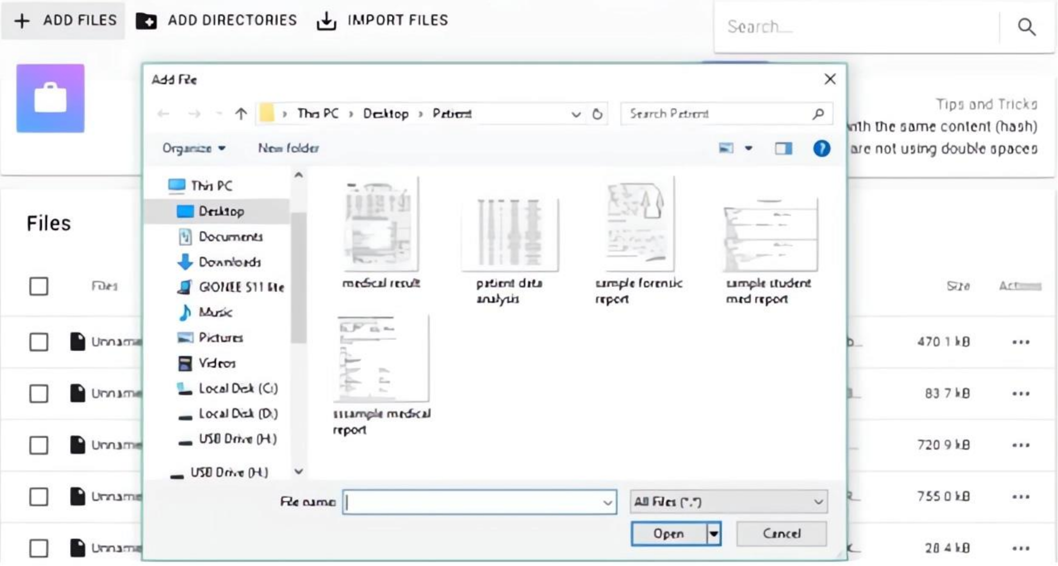
Properties

Hash QmZgf10qLc9ytUn5pbAM7pny4SuB0zR1HBAZ9zJu6B

Description Doctor

Size 720 9 kB

Figure 6. Encrypted Patient's File, Folder and Records



	Files	Size	Actions
□	Unname	470 1 kB	•••
□	Unname	83 7 kB	•••
□	Unname	720 9 kB	•••
□	Unname	755 0 kB	•••
□	Unname	28 4 kB	•••

Figure 7. Adding File to the Encrypted Folder

Next, various created files are added onto the encrypted folders for each entity participating in the blockchain. The added files are encrypted using the generated hash values assigned to them to protect the integrity of their contents. The newly encrypted files are then imported across the network and stored locally using the same generated hash values that were created earlier for each file. Thus, health personnel and patients have transparent access to the health records, and file modifications 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 [93].

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. In this sense, it is possible to maintain a transparent and distributed health records database, which are cryptographically secure and immutable over time [12].

5. Conclusions

We present an electronic health blockchain-based support system based on a permissioned blockchain framework. Our contribution is thus: (a) we used the hyper fabric ledger for permissioned blockchain ledger to record world-state key values of generated blocks on the chain, (b) transformed each records using the key-pair value for the world states to identify patient(s) record, and (c) we used the BEHeDaS support system for patient medical records as Health Information system to aid interoperability [94], [95]. The ensemble tackles the security, interoperability, and privacy of patient records in healthcare facilities in Nigeria – via a high-performance, open-sourced, and user-friendly permissioned chain support [96].

Author Contributions: Conceptualization: A.A. Ojugo, J.K. Oladele and C.C. Odiakaose; Methodology: P.O. Ejeh, F.U. Emordi and B. Nwozor; Software: R.E. Ako, R.A. Abere and V.O. Geteloma; Validation: A.A. Ojugo and J.K Oladele; Formal Analysis: B. Nwozor; Investigation: R.A. Abere and C.C. Odiakaose; Resources: P.O. Ejeh and R.E. Ako; Data Curation: V.O. Geteloma; Writing—original draft preparation: J.K. Oladele, A.A. Ojugo, and F.U. Emordi; Writing—review & editing: J.K. Oladele; Visualization: B. Nwozor; Supervision: A.A. Ojugo and R. Abere; Project administration: A.A. Ojugo; funding acquisition: All.

Funding: This research received no external funding.

Data Availability Statement: We have a non-disclosure agreement (NDA) with the Asaba Specialist Hospital (ASH) Delta State – in lieu of making available and public, the dataset used and retrieved for the period.

Acknowledgments: Our special thanks to the Management Team of The Asaba Specialist Hospital and especially, to the Department of Health Records and Information Management. We also extend our thanks to the Acting Director of the Department of Health and Information Management of the Federal Medical Centre Asaba for his cooperation and assistance.

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

References

[1] R. E. Yoro, F. O. Aghware, M. I. Akazue, A. E. Ibor, and A. A. Ojugo, “Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian,” *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, p. 1943, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1943-1953.

[2] D. Nahavandi, R. Alizadehsani, A. Khosravi, and U. R. Acharya, “Application of artificial intelligence in wearable devices: Opportunities and challenges,” *Comput. Methods Programs Biomed.*, vol. 213. December, 2022, doi: 10.1016/j.cmpb.2021.106541.

[3] C. *Esposito*, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, “Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?,” *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018, doi: 10.1109/MCC.2018.011791712.

[4] P. De *Giovanni*, “Blockchain and smart contracts in supply chain management: A game theoretic model,” *Int. J. Prod. Econ.*, vol. 228, p. 107855, Oct. 2020, doi: 10.1016/j.ijpe.2020.107855.

[5] M. Castro and B. Liskov, “Practical byzantine fault tolerance and proactive recovery,” *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, Nov. 2002, doi: 10.1145/571637.571640.

[6] A. C. Smith *et al.*, “Telehealth for global emergencies: Implications for coronavirus disease 2019 (COVID-19),” *J. Telemed. Telecare*, vol. 26, no. 5, pp. 309–313, Jun. 2020, doi: 10.1177/1357633X20916567.

[7] K. Afifah, I. N. Yulita, and I. Sarathan, “Sentiment Analysis on Telemedicine App Reviews using XGBoost Classifier,” *2021 Int. Conf. Artif. Intell. Big Data Anal.*, pp. 22–27, 2022, doi: 10.1109/icaibda53487.2021.9689735.

[8] A. A. Ojugo and E. O. Ekurume, “Predictive Intelligent Decision Support Model in Forecasting of the Diabetes Pandemic Using a Reinforcement Deep Learning Approach,” *Int. J. Educ. Manag. Eng.*, vol. 11, no. 2, pp. 40–48, Apr. 2021, doi: 10.5815/ijeme.2021.02.05.

[9] J. Liu, X. Sun, and K. Song, “A Food Traceability Framework Based on Permissioned Blockchain,” *J. Cyber Secur.*, vol. 2, no. 2, pp. 107–113, 2020, doi: 10.32604/jcs.2020.011222.

[10] A. A. Ojugo, M. I. Akazue, P. O. Ejeh, C. Odiakaose, and F. U. Emordi, "DeGATraMoNN: Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing," *Kongzhi yu Juece/Control Decis.*, vol. 38, no. 01, pp. 667–678, 2023.

[11] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "Sentiment analysis in detecting sophistication and degradation cues in malicious web contents," *Kongzhi yu Juece/Control Decis.*, vol. 38, no. 01, p. 653, 2023.

[12] A. E. Ibor, E. B. Edim, and A. A. Ojugo, "Secure Health Information System with Blockchain Technology," *J. Niger. Soc. Phys. Sci.*, vol. 5, no. 992, pp. 1–8, 2023, doi: 10.46481/jnsps.2022.992.

[13] J. R. Amalraj and R. Lourdusamy, "A Novel distributed token-based algorithm using secret sharing scheme for secure data access control," *Int. J. Comput. Networks Appl.*, vol. 9, no. 4, p. 374, Aug. 2022, doi: 10.22247/ijcna/2022/214501.

[14] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using GA algorithm for feature selection," *J. Big Data*, vol. 9, no. 1, p. 24, Dec. 2022, doi: 10.1186/s40537-022-00573-8.

[15] G. Sasikala *et al.*, "An Innovative Sensing Machine Learning Technique to Detect Credit Card Frauds in Wireless Communications," *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–12, Jun. 2022, doi: 10.1155/2022/2439205.

[16] A. A. Ojugo, C. O. Obruche, and A. O. Eboka, "Quest For Convergence Solution Using Hybrid Genetic Algorithm Trained Neural Network Model For Metamorphic Malware Detection," *ARRUS J. Eng. Technol.*, vol. 2, no. 1, pp. 12–23, Nov. 2021, doi: 10.35877/jetech613.

[17] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[18] S. J. Damoska and A. Erceg, "Blockchain Technology toward Creating a Smart Local Food Supply Chain," *Computers*, vol. 11, no. 6, p. 95, Jun. 2022, doi: 10.3390/computers11060095.

[19] A. A. Ojugo and D. A. Oyemade, "Boyer moore string-match framework for a hybrid short message service spam filtering technique," *IAES Int. J. Artif. Intell.*, vol. 10, no. 3, pp. 519–527, 2021, doi: 10.11591/ijai.v10.i3.pp519-527.

[20] A. A. Ojugo and O. D. Otakore, "Intelligent cluster connectionist recommender system using implicit graph friendship algorithm for social networks," *IAES Int. J. Artif. Intell.*, vol. 9, no. 3, p. 497~506, 2020, doi: 10.11591/ijai.v9.i3.pp497-506.

[21] K. Fan, Z. Bao, M. Liu, A. V. Vasilakos, and W. Shi, "Dredas: Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT," *Futur. Gener. Comput. Syst.*, vol. 110, pp. 665–674, Sep. 2020, doi: 10.1016/j.future.2019.10.014.

[22] A. A. Ojugo *et al.*, "Evolutionary Model for Virus Propagation on Networks," *Autom. Control Intell. Syst.*, vol. 3, no. 4, p. 56, 2015, doi: 10.11648/j.acis.20150304.12.

[23] M. I. Akazue, I. A. Debekeme, A. E. Edje, C. Asuai, and U. J. Osame, "UNMASKING FRAUDSTERS: Ensemble Features Selection to Enhance Random Forest Fraud Detection," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 201–211, Dec. 2023, doi: 10.33633/jcta.v1i2.9462.

[24] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing," *Futur. Internet*, vol. 14, no. 11, p. 341, Nov. 2022, doi: 10.3390/fi14110341.

[25] A. A. Ojugo, D. A. Oyemade, D. Allenotor, O. B. Longe, and C. N. Anujeonye, "Comparative Stochastic Study for Credit-Card Fraud Detection Models," *African J. Comput. ICT*, vol. 8, no. 1, pp. 15–24, 2015, [Online]. Available: www.ajocict.net

[26] E. Dourado and J. Brito, "Cryptocurrency," in *The New Palgrave Dictionary of Economics*, London: Palgrave Macmillan UK, 2014, pp. 1–9. doi: 10.1057/978-1-349-95121-5_2895-1.

[27] H. Tingfei, C. Guangquan, and H. Kuihua, "Using Variational Auto Encoding in Credit Card Fraud Detection," *IEEE Access*, vol. 8, pp. 149841–149853, 2020, doi: 10.1109/ACCESS.2020.3015600.

[28] R. De', N. Pandey, and A. Pal, "Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice," *Int. J. Inf. Manage.*, vol. 55, no. June, p. 102171, 2020, doi: 10.1016/j.ijinfomgt.2020.102171.

[29] P. K. Paul, "Blockchain Technology and its Types—A Short Review," *Int. J. Appl. Sci. Eng.*, vol. 9, no. 2, 2021, doi: 10.30954/2322-0465.2.2021.7.

[30] S. Linoy, N. Stakhanova, and A. Matyukhina, "Exploring Ethereum's Blockchain Anonymity Using Smart Contract Code Attribution," in *2019 15th Conference on Network and Service Management*, IEEE, Oct. 2019, pp. 1–9. doi: 10.23919/CNSM46954.2019.9012681.

[31] M. Valenta and P. Sandner, "Comparison of Ethereum, Hyperledger Fabric and Corda," *Frankfurt Sch. Blockchain Cent.*, no. June, p. 8, 2017, [Online]. Available: www.fs-blockchain.decontact@fs-blockchain.de

[32] S. Linoy, N. Stakhanova, and S. Ray, "De-anonymizing Ethereum blockchain smart contracts through code attribution," *Int. J. Netw. Manag.*, vol. 31, no. 1, Jan. 2021, doi: 10.1002/nem.2130.

[33] K. Rantos, G. Drosatos, A. Kritsas, C. Ilioudis, A. Papanikolaou, and A. P. Filippidis, "A Blockchain-Based Platform for Consent Management of Personal Data Processing in the IoT Ecosystem," *Secur. Commun. Networks*, vol. 2019, pp. 1–15, Oct. 2019, doi: 10.1155/2019/1431578.

[34] E. Regnath, N. Shivaraman, S. Shreejith, A. Easwaran, and S. Steinhorst, "Blockchain, what time is it? Trustless Datetime Synchronization for IoT," in *2020 International Conference on Omni-layer Intelligent Systems (COINS)*, IEEE, Aug. 2020, pp. 1–6. doi: 10.1109/COINS49042.2020.9191420.

[35] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," *IEEE Trans. Ind. Informatics*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020, doi: 10.1109/TII.2019.2942190.

[36] M. Gasco-Hernandez, W. Feng, and J. R. Gil-Garcia, "Providing Public Value through Data Sharing: Understanding Critical Factors of Food Traceability for Local Farms and Institutional Buyers," 2018. doi: 10.24251/HICSS.2018.285.

[37] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: beyond bitcoin," *Appl. Innov. Rev.*, vol. 27, no. 4–5, pp. 222–228, 2016, doi: 10.15358/0935-0381-2015-4-5-222.

[38] S. Gokarn and A. Choudhary, "Modeling the key factors influencing the reduction of food loss and waste in fresh produce supply chains," *J. Environ. Manage.*, vol. 294, p. 113063, Sep. 2021, doi: 10.1016/j.jenvman.2021.113063.

[39] M. S. Sunarjo, H.-S. Gan, and D. R. I. M. Setiadi, "High-Performance Convolutional Neural Network Model to Identify COVID-19 in Medical Images," *J. Comput. Theor. Appl.*, vol. 1, no. 1, pp. 19–30, 2023, doi: 10.33633/jcta.v1i1.8936.

[40] H. Kabir Bako, M. Abba Dandago, and S. Shamsudeen Nassarawa, "Food Traceability System: Current State and Future Needs of the Nigerian Poultry and Poultry Product Supply Chain," *Chem. Biomol. Eng.*, vol. 4, no. 3, p. 40, 2019, doi: 10.11648/j.cbe.20190403.11.

[41] D. Mao, F. Wang, Z. Hao, and H. Li, "Credit Evaluation System Based on Blockchain for Multiple Stakeholders in the Food Supply Chain," *Int. J. Environ. Res. Public Health*, vol. 15, no. 8, p. 1627, Aug. 2018, doi: 10.3390/ijerph15081627.

[42] A. A. Ojugo and O. Nwankwo, "Spectral-Cluster Solution For Credit-Card Fraud Detection Using A Genetic Algorithm Trained Modular Deep Learning Neural Network," *JINAV J. Inf. Vis.*, vol. 2, no. 1, pp. 15–24, Jan. 2021, doi: 10.35877/454RI.jinav274.

[43] J. Goldenfein and A. Leiter, "Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct," *Law Crit.*, vol. 29, no. 2, pp. 141–149, Jul. 2018, doi: 10.1007/s10978-018-9224-0.

[44] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019, doi: 10.1080/00207543.2018.1533261.

[45] A. A. Ojugo and R. E. Yoro, "Extending the three-tier constructivist learning model for alternative delivery: ahead the COVID-19 pandemic in Nigeria," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, p. 1673, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1673-1682.

[46] K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. Van Nieuwenhuyse, "Research on agricultural supply chain system with double chain architecture based on blockchain technology," *Futur. Gener. Comput. Syst.*, vol. 86, pp. 641–649, Sep. 2018, doi: 10.1016/j.future.2018.04.061.

[47] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *ICT Express*, vol. 7, no. 2, pp. 229–233, Jun. 2021, doi: 10.1016/j.icte.2020.09.002.

[48] K. Behnke and M. . Janssen, "Boundary conditions for traceability in food supply chains using blockchain technology," *Int. J. Inf. Manage.*, vol. 52, p. 101969, Jun. 2020, doi: 10.1016/j.ijinfomgt.2019.05.025.

[49] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation," in *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany)*, IEEE, May 2018, pp. 1–4. doi: 10.1109/IOT-TUSCANY.2018.8373021.

[50] C. N. Verdouw, J. Wolfert, A. J. M. Beulens, and A. Rialland, "Virtualization of food supply chains with the internet of things," *J. Food Eng.*, vol. 176, pp. 128–136, May 2016, doi: 10.1016/j.jfoodeng.2015.11.009.

[51] A. A. Ojugo, P. O. Ejeh, C. C. Odiakaose, A. O. Eboka, and F. U. Emordi, "Improved distribution and food safety for beef processing and management using a blockchain-tracer support framework," *Int. J. Informatics Commun. Technol.*, vol. 12, no. 3, p. 205, Dec. 2023, doi: 10.11591/ijict.v12i3.pp205-213.

[52] A. A. Ojugo and O. D. Otakore, "Improved Early Detection of Gestational Diabetes via Intelligent Classification Models: A Case of the Niger Delta Region in Nigeria," *J. Comput. Sci. Appl.*, vol. 6, no. 2, pp. 82–90, 2018, doi: 10.12691/jcsa-6-2-5.

[53] F. Tian, "An agri-food supply chain traceability system for China based on RFID &amp; blockchain technology," in *13th Conference on Service Systems and Service Management*, IEEE, Jun. 2016, pp. 1–6. doi: 10.1109/ICSSSM.2016.7538424.

[54] K. Kakhi, R. Alizadehsani, H. M. D. Kabir, A. Khosravi, S. Nahavandi, and U. R. Acharya, "The internet of medical things and artificial intelligence: trends, challenges, and opportunities," *Biocybern. Biomed. Eng.*, vol. 42, no. 3, pp. 749–771, 2022, doi: 10.1016/j.bbe.2022.05.008.

[55] S. R. Guntur, R. R. Gorrepati, and V. R. Dirisala, "Internet of Medical Things," in *Medical Big Data and Internet of Medical Things*, no. October 2018, Boca Raton : Taylor & Francis, [2019]: CRC Press, 2018, pp. 271–297. doi: 10.1201/9781351030380-11.

[56] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-alrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," *Int. J. Med. Inform.*, vol. 142, p. 104246, Oct. 2020, doi: 10.1016/j.ijmedinf.2020.104246.

[57] M. I. Akazue, A. A. Ojugo, R. E. Yoro, B. O. Malasowe, and O. Nwankwo, "Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 28, no. 3, pp. 1756–1765, Dec. 2022, doi: 10.11591/ijeecs.v28.i3.pp1756-1765.

[58] A. A. Ojugo and D. O. Otakore, "Redesigning Academic Website for Better Visibility and Footprint: A Case of the Federal University of Petroleum Resources Effurun Website," *Netw. Commun. Technol.*, vol. 3, no. 1, p. 33, Jul. 2018, doi: 10.5539/nct.v3n1p33.

[59] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards Scaling Blockchain Systems via Sharding," in *Proc. of 2019 International Conference on Management of Data*, New York, Jun. 2019, pp. 123–140. doi: 10.1145/3299869.3319889.

[60] R. E. Gier *et al.*, "Evaluation of the therapeutic effect of levamisole in treatment of recurrent aphthous stomatitis.," *J. Oral Pathol.*, vol. 7, no. 6, pp. 405–13, 1978, doi: 10.1111/j.1600-0714.1978.tb01610.x.

[61] A. A. Ojugo and A. O. Eboka, "Assessing Users Satisfaction and Experience on Academic Websites: A Case of Selected Nigerian Universities Websites," *Int. J. Inf. Technol. Comput. Sci.*, vol. 10, no. 10, pp. 53–61, 2018, doi: 10.5815/ijitcs.2018.10.07.

[62] A. A. Ojugo, A. O. Eboka, E. O. Okonta, R. E. Yoro, and F. O. Aghware, "Predicting Behavioural Evolution on a Graph-Based Model," *Adv. Networks*, vol. 3, no. 2, p. 8, 2015, doi: 10.11648/j.net.20150302.11.

[63] E. . Ihama, M. I. Akazue, E. U. Omede, and D. V. Ojie, "A Framework for Smart City Model Enabled by Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 185, no. 6, pp. 6–11, 2023, doi: 10.5120/ijca2023922685.

[64] F. ul Hassan *et al.*, "Blockchain And The Future of the Internet: A Comprehensive Review," Feb. 2019, [Online]. Available: http://arxiv.org/abs/1904.00733

[65] M. J. Hossain Faruk, H. Shahriar, M. Valero, S. Sneha, S. I. Ahamed, and M. Rahman, "Towards Blockchain-Based Secure Data Management for Remote Patient Monitoring," in *2021 IEEE Conf, on Digital Health*, IEEE, Sep. 2021, pp. 299–308. doi: 10.1109/ICDH52753.2021.00054.

[66] A. Khatoon, "A Blockchain-Based Smart Contract System for Healthcare Management," *Electronics*, vol. 9, no. 1, p. 94, Jan. 2020, doi: 10.3390/electronics9010094.

[67] J. W. Kim, S. J. Kim, W. C. Cha, and T. Kim, "A Blockchain-Applied Personal Health Record Application: Development and User Experience," *Appl. Sci.*, vol. 12, no. 4, p. 1847, Feb. 2022, doi: 10.3390/app12041847.

[68] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding," in *2018 IEEE Symposium on Security and Privacy,* May 2018, pp. 583–598. doi: 10.1109/SP.2018.000-5.

[69] H. Li, X. Yang, H. Wang, W. Wei, and W. Xue, "A Controllable Secure Blockchain-Based Electronic Healthcare Records Sharing Scheme," *J. Healthc. Eng.*, vol. 2022, pp. 1–11, Mar. 2022, doi: 10.1155/2022/2058497.

[70] A. Al Mamun, S. Azam, and C. Gritti, "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction," *IEEE Access*, vol. 10, pp. 5768–5789, 2022, doi: 10.1109/ACCESS.2022.3141079.

[71] A. A. Ojugo and O. D. Otakore, "Computational solution of networks versus cluster grouping for social network contact recommender system," *Int. J. Informatics Commun. Technol.*, vol. 9, no. 3, p. 185, 2020, doi: 10.11591/ijict.v9i3.pp185-194.

[72] C. V. N. U. B. Murthy, M. L. Shri, S. Kadry, and S. Lim, "Blockchain Based Cloud Computing: Architecture and Research Challenges," *IEEE Access*, vol. 8, pp. 205190–205205, 2020, doi: 10.1109/ACCESS.2020.3036812.

[73] S. Naz and S. U.-J. Lee, "Why the new consensus mechanism is needed in blockchain technology?," in *2020 Second International Conference on Blockchain Computing and Applications*, IEEE, Nov. 2020, pp. 92–99. doi: 10.1109/BCCA50787.2020.9274461.

[74] F. K. Nishi *et al.*, "Electronic Healthcare Data Record Security Using Blockchain and Smart Contract," *J. Sensors*, vol. 2022, pp. 1–22, May 2022, doi: 10.1155/2022/7299185.

[75] M. M. H. Onik, S. Aich, J. Yang, C.-S. Kim, and H.-C. Kim, "Blockchain in Healthcare: Challenges and Solutions," in *Big Data Analytics for Intelligent Healthcare Management*, Elsevier, 2019, pp. 197–226. doi: 10.1016/B978-0-12-818146-1.00008-8.

[76] A. Panwar, V. Bhatnagar, M. Khari, A. W. Salehi, and G. Gupta, "A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–19, Apr. 2022, doi: 10.1155/2022/3045107.

[77] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *ICT Express*, vol. 7, no. 2, pp. 229–233, Jun. 2021, doi: 10.1016/j.icte.2020.09.002.

[78] A. A. Ojugo and A. O. Eboka, "Empirical Bayesian network to improve service delivery and performance dependability on a campus network," *IAES Int. J. Artif. Intell.*, vol. 10, no. 3, p. 623, Sep. 2021, doi: 10.11591/ijai.v10.i3.pp623-635.

[79] R. E. Yoro, F. O. Aghware, B. O. Malasowe, O. Nwankwo, and A. A. Ojugo, "Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, p. 1922, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1922-1931.

[80] A. A. Ojugo and R. E. Yoro, "Predicting Futures Price And Contract Portfolios Using The ARIMA Model: A Case of Nigeria's Bonny Light and Forcados," *Quant. Econ. Manag. Stud.*, vol. 1, no. 4, pp. 237–248, 2020, doi: 10.35877/454ri.qems139.

[81] A. A. Ojugo and I. P. Okobah, "Prevalence Rate of Hepatitis-B Virus Infection in the Niger Delta Region of Nigeria using a Graph-Diffusion Heuristic Model," *Int. J. Comput. Appl.*, vol. 179, no. 39, pp. 975–8887, 2018.

[82] G. Verma, N. Pathak, and N. Sharma, "A Secure Framework for Health Record Management Using Blockchain in Cloud Environment," *J. Phys. Conf. Ser.*, vol. 1998, no. 1, p. 012019, Aug. 2021, doi: 10.1088/1742-6596/1998/1/012019.

[83] M. Finck, "Blockchains and Data Protection in the European Union," *Eur. Data Prot. Law Rev.*, vol. 4, no. 1, pp. 17–35, 2018, doi: 10.21552/edpl/2018/1/6.

[84] S. Quamara and A. K. Singh, "An In-depth Security and Performance Investigation in Hyperledger Fabric-configured Distributed Computing Systems," *Blockchain Model.*, vol. 1, no. 1, pp. 12–24, 2023.

[85] A. Singh, S. Jadhav, and M. Roopashree, "Factors to overcoming barriers affecting electronic medical record usage by physicians," *Indian J. Community Med.*, vol. 45, no. 2, p. 168, 2020, doi: 10.4103/ijcm.IJCM_478_19.

[86] C. L. Udeze, I. E. Eteng, and A. E. Ibor, "Application of Machine Learning and Resampling Techniques to Credit Card Fraud Detection," *J. Niger. Soc. Phys. Sci.*, p. 769, Aug. 2022, doi: 10.46481/jnsps.2022.769.

[87] A. Wright and P. De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," *SSRN Electron. J.*, 2015, doi: 10.2139/ssrn.2580664.

[88] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intell. Syst. Accounting, Financ. Manag.*, vol. 25, no. 1, pp. 18–27, Jan. 2018, doi: 10.1002/isaf.1424.

[89] T. Adedeji, H. Fraser, and P. Scott, "Implementing Electronic Health Records in Primary Care Using the Theory of Change: Nigerian Case Study," *JMIR Med. Informatics*, vol. 10, no. 8, p. e33491, Aug. 2022, doi: 10.2196/33491.

[90] C. D. Akwaowo *et al.*, "Adoption of electronic medical records in developing countries—A multi-state study of the Nigerian healthcare system," *Front. Digit. Heal.*, vol. 4, Nov. 2022, doi: 10.3389/fdgth.2022.1017231.

[91] F. Mustofa, A. N. Safriandono, A. R. Muslikh, and D. R. I. M. Setiadi, "Dataset and Feature Analysis for Diabetes Mellitus Classification using Random Forest," *J. Comput. Theor. Appl.*, vol. 1, no. 1, pp. 41–48, 2023, doi: 10.33633/jcta.v1i1.9190.

[92] M. Lei, L. Xu, T. Liu, S. Liu, and C. Sun, "Integration of Privacy Protection and Blockchain-Based Food Safety Traceability: Potential and Challenges," *Foods*, vol. 11, no. 15, pp. 1–31, 2022, doi: 10.3390/foods11152262.

[93] M. I. Akazue, R. E. Yoro, B. O. Malasowe, O. Nwankwo, and A. A. Ojugo, "Improved services traceability and management of a food value chain using block-chain network : a case of Nigeria," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 29, no. 3, pp. 1623–1633, 2023, doi: 10.11591/ijeecs.v29.i3.pp1623-1633.

[94] A. R. Rajput, Q. Li, M. Taleby Ahvanooey, and I. Masood, "EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain," *IEEE Access*, vol. 7, pp. 84304–84317, 2019, doi: 10.1109/ACCESS.2019.2917976.

[95] A. Pinna and S. Ibba, "A blockchain-based Decentralized System for proper handling of temporary Employment contracts," Nov. 2017, doi: 1711.09758.

[96] C. Wright and A. Serguieva, "Sustainable blockchain-enabled services: Smart contracts," in *2017 IEEE International Conference on Big Data (Big Data)*, IEEE, Dec. 2017, pp. 4255–4264. doi: 10.1109/BigData.2017.8258452.