Distributed Healthcare Privacy Protection in Emerging Cybersecurity Use of Sensitive Data

UGOCHUKWU O. MATHEW[1]
RENATA LOPEZ ROSA[2]
OYEDEMI OLUYEMISI ADENIKE [3]
DEMOSTENES Z. RODRIGUEZ[4]

Department of Computer Science, Federal University of Lavras, Brazil
[1]ugochukwu.mathew@estudante.ufla.br
[2] renata.rosa@ufla.br
[3] oyedemi.adenike@ufla.br
[3] demostenes.zegarra@ufla.br

Abstract. The necessity for distributed healthcare information systems have grown in the digital health settings, serving as the foundation for Internet of Things cloud data warehouse repositories management and record federation. The amount of sensitive data that are stored including financial information, medical records, and private communications, as well as the expansion of healthcare distributed systems, raises significant concerns about potential security breaches and exploitation. On the account that sensitive patient data is stored in these distributed healthcare systems, there is need to comply with new cybersecurity requirements. Implementing data-driven technology offers a great chance to make significant improvements in the sector toward better patient and public healthcare use of sensitive data. In this study, the author achieved two essential goals by distinguishing the suggested strategy from all other existing methods of patient healthcare data management. In the beginning, we integrated blockchain technology with a federated learning system to develop a cognitive computing paradigm that enhanced accuracy, making healthcare data warehouse information system fake data injection attacks impossible. In the second approach, the author introduced secured message queuing telemetry transport (MQTT) communication as a gatekeeper strategy to prevent indiscriminate node flooding by allowing selective client admittance by the MQTT broker via the MQTT protocol, which ensured that broker node verification and authentication were harmonized using the Practical Byzantine Fault Tolerance (PBFT) blockchain consensus algorithm.

Keywords: Information System, Cybersecurity, Data warehouse Technology, Blockchain technology, Federated Learning, Artificial Intelligence, STEM Paradigm, Cloud Computing , Internet of Things

(Received November 12th, 2024 / Accepted December 28th, 2024)

1 Introduction

The significance of data security in healthcare cannot be undervalued, given the rapid digitization of medical records and the increasing dependence on electronic technologies [52, 15, 50, 14, 11, 42, 49]. Healthcare organizations are trusted with vast amounts of extremely sensitive data [37, 7, 6, 19, 8, 45, 51, 48] , including personally identifiable information, diagnoses, treatment plans, and medical histories. The accuracy of clinical decision-making and patient privacy are at risk in the healthcare industry due to a single data security breach or problem. One of the biggest threats to healthcare data security is the potential for malicious actors to gain unauthorized access or for sensitive data to be inadvertently misused [25]. Healthcare cybersecurity risks are on the rise, and attacks involving phishing are becoming the most common way to compromise data security. Healthcare organizations have a serious difficulty as a result of the growing sophistication of these attacks, which may use artificial intelligence to create phishing operations that are more convincing. Organizations are using AI-powered security solutions for real-time incident response and enhanced threat identification to counter these threats and reduce the risk of healthcare breach [28].

The swift development in information system technology is bringing about revolutionary dynamics in a variety of sectors, influencing how organizations function and interact with their business environments [22]. In the digital health sector for instance, innovative technologies are improving patient care and healthcare informatics, as developments in the artificial intelligence (AI) and machine learning computing are completely changing how services are distributed across all digital ecosystem [4]. Information systems integration is improving the efficiency of healthcare supply chain management, and medical informatics is undergoing a digital revolution that is changing how healthcare service is delivered. Information systems are also essential to the creation of smart cities, which promote sustainability and enhance urban living in general [35].

In order to provide insights into the technological developments influencing these sectors, this paper will examine the new developments in information systems and their particular effects on supply chain management in healthcare informatics. As digital technologies evolves, it is critical to have a thorough incident response strategy on how to identify and stop fake data injection cyberattacks, given the growing web-based and distributed information system-centered nature of the current healthcare systems [33]. Recent technology advances, such as the growth of virtualization, information systems, cloud computing, data warehousing technologies, and mobile applications, have given rise to new cybersecurity scenarios that healthcare service providers must adhere in order to comply with Health Insurance Portability and Accountability Act (HIPAA) 1996 standards on patient data protection [40]. The HIPAA cybersecurity guidelines have proven very helpful as the healthcare industry has moved from paper files to digital healthcare information systems sustainability. In particular, electronic health records (EHRs) have improved the efficiency and security of healthcare protected information, maintained patient privacy, and made hospital administration and management easier. Adoption of information systems can improve general security assessments, and management situations for healthcare organizations in addition to assisting them in meeting the requirements for HIPAA and General Data Protection Regulation (GDPR) on digital data protection [46]. Information system technologies provide effective risk protection in the digital healthcare ecosystem and virtualized environments by connecting mobile applications to the appropriate medical data warehouse repositories for all processes automation.

2 Background of the Study

An organization's formal, sociotechnical system for gathering, processing, storing, and disseminating information is called an information system [16]. Base on the sociotechnical theory, information systems are made up of four distinguishable components as technology, people, structure (or roles), and tasks [10]. Information systems are made up of components for gathering, storing, and processing data into an applicable format for decision making and policy implementation. Healthcare information systems (HIS) serve as the digital pipeline of all hospital operations, and they are crucial to the modern healthcare sector. A number of duties that enhance the federation of medical records across government agencies, departments and private sectors can be carried out through the HIS, since it does away with manual records and keeps all data digital [54]. It is a crucial piece of software that optimizes the hospital's workflow in a number of areas, including financial management, administrative tasks, record keeping, and patient care. In a single secured system, the HIS software arranges and safeguards all important data on patients treatments, staff schedules, and billings. The system has elements such as the clinical information system for order input and medical records, the radiology and laboratory information system for drug and treatment management, and the patient management system for scheduling and registration [58].

Hospital information systems include a variety of specialized designs that handle the numerous facets of patient data and hospital administration, to perform data analysis to determine what aspects of their operations are working well and what needs improvements. The alliance between IBM Watson Health and Cleveland Clinic is a powerful illustration of a company using advanced healthcare informatics to gain a competitive edge [56]. The Cleveland Clinic, a well-known American nonprofit academic medical center with its headquarters in Cleveland, Ohio, partnered with IBM to expand its cancer care capabilities. The healthcare organization included IBM Watson, a cognitive computing platform that can respond to questions in plain language, for Oncology into its medical specialty that focuses on cancer diagnosis and therapy to offer cancer patients individualized therapy suggestions [18]. To help medical professionals make informed treatment decisions and improve human life expectancy and societal well-being, the Cleveland Clinic department is utilizing IBM Watson Health's AI capabilities to analyze clinical trial data, patient records, and medical literature[14]. The advanced healthcare informatics system analyzes vast amounts of clinical trial data, medical literature, and patient information to identify potential therapy alternatives based on individual patient profiles. This expedites the oncologists' decision-making process and ensures that treatment plans are in accordance with the latest medical research and evidence-based practices [26]. Cleveland Clinic earned a competitive edge by providing more accurate and customized cancer treatments through the use of modern healthcare informatics. By keeping up with the most recent developments in oncology and taking into account a wider variety of treatment options, the system helps doctors to improve patient outcomes.

In addition to improving care quality, this creative use of informatics gives Cleveland Clinic a competitive edge in the healthcare sector by establishing the clinic as a pioneer in utilizing technology to deliver state-of-the-art medical solutions [44].Health data privacy is a fundamental concern in the 21st century's digital age, when the need to protect sensitive information and the pursuit of medical insights clashes. The need for a uniform federal framework that complies with HIPAA criteria is argued in this paper in order to effectively address modern cybersecurity threats. In an age of increasing globalization, this paper argues that the HIPAA regulations should take on the task of modernizing data protection laws to take into account current cybersecurity concerns. The author begin by examining the data warehouse federation architecture of the historic healthcare information system, which adopts a proactive and citizen-centric approach to empower patients with greater control over their data. The article also suggests that healthcare providers use the new tools for improved security and consistent risk analysis. The quantity of data in this system grows as healthcare becomes more widely available for a variety of uses. This national data explosion emphasizes how important it is to determine whether privacy regulations governing the ownership of digital health data comply with HIPAA standards. In light of the sharp increase in data breach occurrences inside the healthcare network, it is imperative that healthcare laws be updated in order to implement stricter patient protections. Strict data collection, privacy protection, and cybersecurity enforcement are necessary to prevent breaches since noncompliance has serious repercussions.

This study achieved two significant objectives in differentiating the suggested approach from all other existing methods. In order to develop a cognitive computing paradigm that enhanced accuracy and rendered fake data injection attacks impossible within the distributed healthcare information data warehouse repositories, we initially integrated blockchain technology with a federated learning system that offered an incentive structure for data mining and data warehouse record validation. The second approach used the Practical Byzantine Fault Tolerance (PBFT) blockchain consensus algorithm to enable selective client admittance through the secured Message Queuing Telemetry Transport (MQTT) broker via the MQTT protocol as a gatekeeper strategy to prevent indiscriminate node flooding. The remaining part of this paper is structured thematically into: III. Research Objective, IV. Theoretical Framework, V. Research Methodology, VI. Proposed Framework, VII. Future Research Focus and VIII. Conclusion. .

3 Research Objective

The HIPAA primary focus is healthcare information system management, which aims to safeguard healthcare plans, healthcare data facilities, and healthcare providers who exchange information electronically [53]. These healthcare providers include organization and institutions under HIPAA guidelines that handle patient-protected data. The privacy rule, the security rule, and the breach notification act are some of the fundamental regulations provided by HIPAA's framework that enable the viewing, sharing, and use of patient data in more general contexts, such as research and policy study. In this paper, the following computing objectives were pursued:

i.The author introduced a federated learning framework for distributed healthcare information systems based on blockchain technology that used PBFT consensus algorithm to stop cybersecurity false data injection.

ii. The proposed framework adds another layer of security to the blockchain-based federated learning system, protecting patient data while allowing information sharing for medical treatment and scientific research and complying with the standard HIPAA regulations regarding sensitive data kept electronically in the healthcare information system.

iii. The suggested model considers many medical organizations because the locally trained model of other medical organizations may enhance the ability of the remote healthcare information system to be shared in a global model as a distributed network.

iv. The paper introduced a distributed healthcare information system that enabled information federation to improve patient data security, and it provided a thorough framework that prioritizes the protection of electronic health information in a standardized state-by-state architecture.

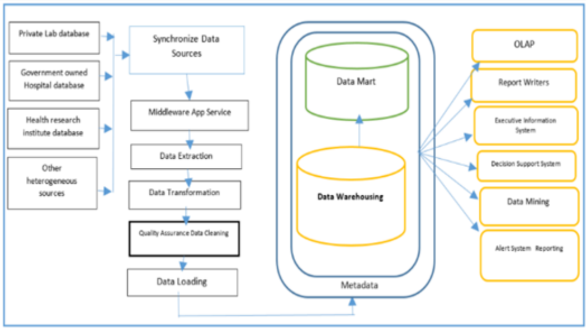

Figure 1: Distributed healthcare information data warehouse system design

4 Theoretical Framework

The distributed information systems used in today's business world are constantly changing in terms of new applications, proportion of users, hardware and software requirements, network components and various research applications that federate data through the multiple heterogeneous sources into the applicable database repositories [16]. A broad framework for describing the thorough administration of health information systems across computerized systems and their secure interactions between patients, providers, the government, regulatory agencies, and other important stakeholders, as well as health insurance companies, are provided by health information technology(HIT) [1]. There is a growing perception that the most promising instrument and vehicle for enhancing the general effectiveness, safety, and quality of the healthcare delivery system depend on HIT [39]. Distributed systems for healthcare are crucial for managing dispersed patient data. The distributed design of these systems includes data warehoused records and a local database on each client machine. In contrast to centralized databases, which keep all of the data in one place, distributed database architectures spread the data over a network of computers that are connected by communication links. Multiple separate computers connected via a network comprise a distributed system. To achieve a common computational goal, these devices exchange information with one other. Rather than being limited to a single computer, this approach divides information processing over several computers. Distributed systems are computer communication network on the Internet that have two distinct types of computer systems: client nodes and server nodes for broad information system federation [43]. Given that many computing jobs are too complicated for a single machine to handle, on the benefit that internet provides the widest computer network, it makes sense that the number of distributed systems is increasing [20]. A communications subsystem and multiple computer systems, some of which may have different designs, are necessary for distributed information systems to address a common issue. Recent technological advancements have given the idea of developing, implementing, and documenting a distributed hospital information system more credibility. The distributed information system approach makes it simple for each department to share data, maintain control over its own application system, and upgrade hardware and software to suit its business operations [57]. Referring to Figure 1, the healthcare distributed information system is a federated data warehouse system that allows authorized users to query data across a network of organizations. The results are compiled and returned to the original questioner after being gathered from each organization in the federation through online analytical processing (OLAP) that allows user to examine corporate data from several perspectives[38]. The organization that owns the data never lets it go, instead, the data is visited and the federation system receives just the calculated answers to the query. The operational components of security, auditing, authentication, and access rights are among the shared technical architectures that form the basis of federated data warehouse systems. A crucial part of establishing the federation that will permit access to the data is reaching an agreement on which aspects of this data warehoused information are shared and which are to be controlled locally based on blockchain consensus algorithm [31]. Several networking layers must be functional in the languages that devices use to guarantee strong security, intelligent routing, and analytics operations. Comprehending these protocols in the network allows traffic to be prioritized, safeguarded, and routed appropriately. As opposed to conventional systems, blockchains decentralized architecture improves security against hacks and data loss while guaranteeing resilience against single points of failure[17].

Consensus algorithms are essential to blockchain networks because they allow different distributed nodes to agree on numbers of variable information system attributes. A consensus method, like proof of stake (PoS) or proof of work (PoW) and PBFT secures the network and stops unauthorized users from verifying a transaction for accuracy [36]. Whether to commit a distributed transaction to a database (information system) is determined by consensus algorithms based on an underlying mechanism. Along with ensuring consistency and transparency in transactions, they are frequently used to synchronize data throughout a decentralized network. Consensus techniques provide consistency between state machine replicas and synchronize them to ensure consistency across distributed data warehouse information system [34]. They are highly helpful for distributed information system recordkeeping and are frequently used to secure and build trust across decentralized computer networks like blockchain. Due to size restrictions and storage costs, blockchain cannot be utilized to store all the data in EHR records; however, it can be used to index the data using hashing methods of federated learning [23]. With the use of a central server and a number of clients acting as nodes to carry out local training using their local data, federated learning is a distributed machine-learning technique for preventing denial-of-service (DoS), distributed denial-of-service (DDoS) and false data injection cybersecurity attack[3], [2]. A standard global model is initially sent to a group of clients by the central server, while the local models are then returned to the server by clients, who used the local data to train the global model [55].

The server initiates an additional training cycle after combining the local models into a new global model. It is possible to repeat this process multiple times until a threshold is met or the global model converges. Fundamentally, speaking, federated learning is a cooperative machine learning method that uses local data samples from several devices or servers to train and device an algorithm without ever transferring the actual data. In situations when access rights, security and data privacy present serious impediments, this idea is revolutionary trend. In a similar development, AI models will allow hospitals to work together to improve patient outcomes without exchanging sensitive patient data, or where digital devices can learn from user behavior to improve features without sacrificing privacy, there are many possibilities and scenarios that federated learning is bringing to electronic healthcare system [5]. No matter how it is stored, sensitive information including genetic health details and demographic data is subject to strict protection requirements under privacy laws like the GDPR in Europe and the HIPAA in the United States of America [41]. To tackle these obstacles, novel approaches that leverage the advantages of the blockchain are required, including data integrity, decentralization for security and resilience, and robust authorization. This shared technology architecture is used to administer application-programming interfaces (APIs), which are a key component of federated data systems. Even though the federated healthcare organizations probably utilize a range of technology systems and data formats, the usage of APIs and the basic architecture allows for a scalable, secure, and dependable way to access their local data stores.

Most significantly, any organization in the federation can define and implement certain governance policies such as respecting local laws through the use of APIs. Using APIs in a federated data system enables any local organization in the federation to have essential governance control, subject to the federation's consensus. In computing world, blockchain federated learning consensus algorithm is a procedure that helps dispersed processes or systems agree on a single data value [24]. In a network with several users or nodes, these methods are made to be dependable. It is crucial to resolve this challenge, sometimes referred to as the consensus problem, in distributed computing and multi-agent systems like blockchain networks for cryptocurrencies. Blockchain-based federated learning consensus algorithms are crucial parts of distributed information data warehouse fault-tolerant systems because they enable a group of distributed computers or servers to work as a cohesive unit and come to an agreement on the system's status even in the face of errors or outages [33]. To do this, the algorithm determines a threshold, or the number of member machines that need to agree. In order to solve a consensus challenges, consensus algorithms assume that only a portion of the nodes will respond and that some systems and processes will be unavailable, however, the reachable nodes need to react. Assume that an algorithm might demand that a minimum of 55% of nodes react in order to reach consensus or agreement on a network status or data value validation. Even if the other resources are flawed or unavailable, this guarantees that consensus is reached with the fewest possible resources. In the fault-tolerant system, the method also preserves the integrity of the judgments made by the nodes that agree. Many practical uses for consensus algorithms can be found in distributed or decentralized computer networks where blockchain manifested it most widely used in the distributed applications [29]. A distributed peer-to-peer network's nodes, or dispersed computers, work together to manage this decentralized database. The ledger is kept in duplicate by every peer or node to avoid a single point of failure. Every change or validation made on the network is instantly reflected in every copy. Without requiring a centralized, reliable third party, this ensures the integrity and security of data records and builds system confidence.

5 Research Methodology

The recognition of the relevance of computational thinking has aided in the quick growth of related cybersecurity studies as well as privacy protection in the computer field [30]. Taking into account the multifaceted nature of computational thinking, which extends beyond programming and computer science, techniques and practices for building cybersecurity computational thinking are not always simple to comprehend in terms of focus and viability in a variety of cybersecurity contexts. In this study, design science research methodology (DSRM) was employed which centered on the creation and validation of information systems prescriptive knowledge related to the distributed healthcare information system and cybersecurity computational paradigm. It encompasses the approaches of various research fields, such as information technology, digital health technology, computer science, cybersecurity and artificial intelligence which provides particular standards for assessment and iteration in research initiatives that contribute to organization information system [21]. Algorithms, human-computer interfaces, and interaction design approaches, such as process models and machine language models, are among the generated model which DSRM is commonly applied [13]. The DSRM is a legitimate research approach that can be used to solve real-world computing problems, especially wicked problems [12].

In this study, three methodology approaches were followed. To identify research gaps, the literature review was covered in the first stage. In the preceding sections, the research issues listed in the research gap were covered. Research on model building using the DSRM approach is being conducted primarily because of the paucity of existing literature on the subject. To identify research gaps, the literature review was covered in the first stage. In the preceding sections, the research issues listed in the research gap were covered. Research on model building using the DSRM approach is being conducted primarily because of the paucity of existing literature on the subject. Subsequently, the stages of model creation are discussed, culminating in the application of the DSRM technique in the design implementation. Figure 2 presents the steps of the research procedure on the consensus algorithm implementation on the healthcare distributed information system that prevented cybersecurity false data injection. While federated learning has applications in many different domains, including healthcare distributed information systems, where machine learning models are trained using large data sets from different system components. Federated learning is a new distributed AI technique that allows machine learning models to be trained collaboratively without exchanging patient data [47].

A real-time distributed networking system based on the MQTT gatekeeping protocol is proposed in this research, which also delves into the examination of several federated learning consensus techniques. Federated learning aims to solve the privacy and data governance issues by allowing algorithms to be trained jointly without sharing the actual data [9]. In order to address these issues and provide a privacy-preserving solution of the patient database system, federated learning employs machine learning models. A blockchain-based federated learning approach was proposed by [27], for the device verification and consensus, the local gradients of each iteration are recorded in blocks, and the end-to-end latency and optimal block production rate are examined. In order to select nodes, integrate the learned model into the blockchain, and carry out two-stage validation, [32] introduced a hybrid blockchain architecture-based federated learning model that consists of a permissioned blockchain and a local directed acyclic graph. In addition to maintaining the security and reliability of the blockchain, [32] combined blockchain with federated learning to give the system the optimal decision-making power of artificial intelligence, enabling blockchain's efficiency and communication to improve its functionality. Modified versions of the underlying consensus protocols, such as Proof-of-Word(PoW) and Practical Byzantine Fault Tolerance (PBFT) algorithm stops as soon as the global model satisfies the stopping criterion for fresh block creation. Blockchains employ a range of consensus techniques to decide what will be included in the following block. Some blockchains use a consensus algorithm called PBFT, which is a variant of the Byzantine Fault Tolerant (BFT) algorithm.

Blockchains that use a variation of BFT, like PBFT, usually combine it with another algorithm to minimize the number of voting nodes. The delegates in a permissioned blockchain could be chosen by a centralized authority or by a decentralized consensus method such as Delegate Proof of Stake (DPoS). To ensure consensus and its ability to function even in the presence of malicious nodes, it is crucial to ensure that the consensus algorithm is appropriately implemented and well-designed, regardless of the mechanism used. The in-

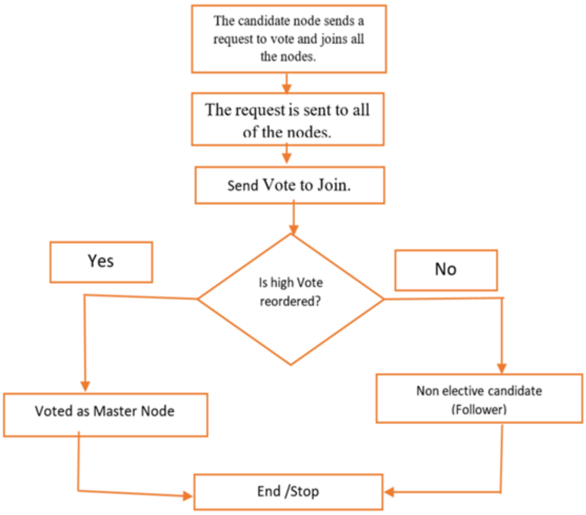
The candidate node sends a request to vote and joins all the nodes.
The request is sent to all of the nodes.
Send Vote to Join.
Yes
Is high Vote reordered?
No
Voted as Master Node
Non elective candidate (Follower)
End /Stop

Figure 2: Master Node Election for block committal

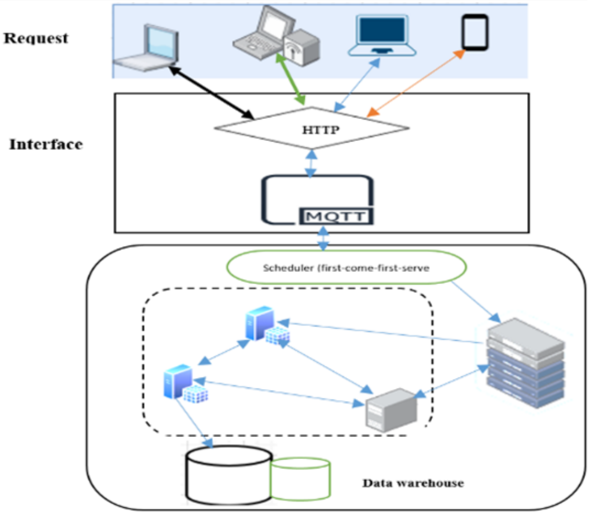

Figure 3: Distributed information system based on MQTT blockchain federated learning method using the consensus algorithm, Author illustration

tegrity and reliability of decentralized networks depend on these consensus methods that were implement. Figure 2 illustrates the recommended adaptive PBFT algorithmic flowchart method, which is utilized to improve learning efficiency and node admittance.

6 Proposed Framework

The overall system design for the blockchain federated learning framework was mainly made up of several information system components that were structured in a coordinated way to enable healthcare information data federation, as shown in Figure 3. When necessary, the IoT node is first equipped with the information system cluster application that controls the distant device response. The second step involves a MQTT broker collecting data from an IoT distant node and forwarding it to the computing platform for scenario analysis. Every subscriber to a particular topic is run by a MQTT broker, which uses the publish/subscribe mechanism to forward data as it is received. Third, this study employed a distributed information system platform that connected the MQTT and the intrusion detection system that notifies the authentication protocols. The complete system is comprised of an IoT-enabled information system with MQTT clients and nodes stationed, as shown in Figure 3. Each client accesses the IoT information system platform to send and receive data when data validation consensus are reached. When creating a blockchain application, it is crucial to select the appropriate type of network of distributed information systems and operational data warehouse systems for healthcare. Data warehouse servers for blockchain information systems and MQTT components make up the majority of IoT remote nodes communication interchange. The MQTT component allows for instant data transfer and also functions as a broker and subscriber to the protocol, allowing various actions to be performed after the data is obtained. This study uses a component for dependable data transfer and storage to obtain specified data, which is then sent to the verifiable recipient under blockchain supervision in service compliance with the HIPAA regulation.

Blockchain's consensus method generates a decentralized, immutable record that ensures data authenticity, authorization, and integrity. Once captured, data cannot be altered since it is tamper-proof. This feature is very helpful for maintaining data integrity in a variety of Internet of Things applications, such as supply chain management and healthcare data storage. The decentralized architecture of blockchain also increases system resilience against attacks and malfunctions, and its encryption algorithms safeguard data privacy. By integrating cryptography, decentralization, and immutability disposition, blockchain can enhance IoT security. Clients use optimal TLS/SSL encryption to create a TCP/IP connection with the broker in order to provide secure communication. Clients enter their login credentials and choose between a clean or persistent session. Clients have the option to publish messages or subscribe to particular topics in order to receive communications. While publishing clients communicate the broker, subscribers express interest in receiving communications on particular topics. The broker distributes the published messages to all clients who have subscribed to the relevant topics. Depending on the session type, it controls message storage for disconnected clients and guarantees constant message delivery based on the selected QoS level. MQTT's broad support for platforms and technologies makes integration simple and encourages seamless communication and interoperability between IoT ecosystems. The MQTT Broker manages requests to route messages, subscribe and unsubscribe, and connect and disconnect clients. Publish-subscribe patterns, as opposed to client-server patterns, separate the client sending messages (publisher) from the client receiving them (subscriber). The MQTT Broker routes and distributes all messages, so publishers and subscribers do not need to connect directly. Lastly, a robust and intelligent MQTT broker is required to manage millions of connections and message throughput comparable to the suggested approach, allowing IoT service providers to focus on creating more reliable MQTT applications and managing cybersecurity issues emerging within the distributed data warehouse information system.

7 Future Research Focus

To solve different query problems with healthcare information systems, a distributed healthcare information system based on computer database technology such as a data warehouse computing infrastructure will be developed in addition to the blockchain federated machine learning algorithmic framework. By fostering trust among users, blockchain-based federated learning systems can facilitate auditability and use smart contracts to implement automated incentive schemes. A number of duties that enhance the federation of medical records across government agencies, departments and private sectors must be carried out through the HIS, since it does away with manual records and keeps all data digital

7.1 Conclusion

In order to monitor public health, provide patient care, and assist in the formulation of health policy, the healthcare information system is essential. It improves public health surveillance, gives healthcare practitioners access to patient data, and aids in the evidence-based decision-making of policymakers. In order to enhance public health and healthcare delivery, the department of health and its connected agencies gather, evaluate, and disseminate health information, making them the most trustworthy source. Improving the general health and well-being of the populace as well as managing the healthcare system effectively depend on the HIS. Implementing distributed information systems has changed the healthcare industry's paradigm and created new chances for improved data management, operational efficiency, and patient care. With the use of healthcare distributed information systems, healthcare organizations may be able to offer more collaborative, patient-centered services. To increase cybersecurity and reduce the likelihood of unauthorized material being inserted into healthcare information system databases, the authors of the study developed the PBFT blockchain consensus technique. Each candidate node has an equal chance of getting certified, which reduces communication costs and boosts consensus efficiency among the candidates who participated in the voting process. This is the foundation of the proposed system's PBFT consensus mechanism.

8 Conflict of Interest

There is no conflict of interest regarding this paper.

References

[1] Abdul, A. et al. A review of the challenges and opportunities in implementing health informatics in rural healthcare settings. *International Medical Science Research Journal*, 4, 2024.

[2] Agrawal, a. o., Sarkar. Federated learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications*, 195, 2022.

[3] Ali, L. et al. Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial iot networks: A survey. *Ad Hoc Networks*, 2024.

[4] Aminizadeh, H. and others. Opportunities and challenges of artificial intelligence and distributed systems to improve the quality of healthcare service. *Artificial Intelligence in Medicine*, 149:102779, 2024.

[5] Antunes, A. et al. Federated learning for healthcare: Systematic review and architecture proposal. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 13, 2022.

[6] Araujo, A., Okey, O., Saadi, M., Adasme, P., Rosa, R., and Rodriguez, D. Quantum-assisted federated intelligent diagnosis algorithm with variational training supported by 5g networks. *Scientific Reports*, 14(1):26333, 2024.

[7] Awotunde, B., Sur, J., Imoize, S., Rodriguez, A., and Akanji, D. An enhanced keylogger detection systems using recurrent neural networks enabled with feature selection model. *Advances in Communication, Devices and Networking*, 1, 2024.

[8] Ayub, M., Adasme, P., Rodriguez, D., Saadi, M., and Shongwe, T. Expanding horizon: The role of reconfigurable intelligent surfaces in enabling massive connectivity. In *2024 Horizons of Information Technology and Engineering (HITE)*, pages 1–6, 2024.

[9] Bharati, M. et al. Federated learning: Applications, challenges and future directions. *International Journal of Hybrid Intelligent Systems*, 18, 2022.

[10] Brockhaus, B. and others. Digitalization in corporate communications: understanding the emergence and consequences of commtech and digital infrastructure. *Corporate Communications: An International Journal*, 28:274–292, 2023.

[11] Carvalho Barbosa, R., Shoaib Ayub, M., Lopes Rosa, R., Zegarra Rodrïgues, D., and Wuttisittikulkij, L. Lightweight pvidnet: A priority vehicles detection network model based on deep learning for intelligent traffic lights. *Sensors*, 20, 2020.

[12] Chatterjee, B. et al. A typology of knowledge creation in design science research projects. In *International Conference on Design Science Research in Information Systems and Technology*, 2024.

[13] Cheng and Lin. Building a low-cost wireless biofeedback solution: Applying design science research methodology. *Sensors*, 23, 2023.

[14] de Sousa, A. L., Okey, O. D., Rosa, R. L., Saadi, M., and Rodriguez, D. Z. A novel resource allocation in software-defined networks for iot application. In *2033 International conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2023.

[15] dos Santos, M. R., Batista, A. P., Rosa, R. L., Saadi, M., Melgararejo, D. C., and Rodrí'guez, D. Z. Aqm: Audio streaming quality metric based on network impairments and user preferences. *IEEE Transactions on Consumer Electronics*, 2023.

[16] Ebong, M. and others. Multimedia cloud data warehouse design for knowledge sharing in the university environment: A proposed digital solution. In *Implementing Interactive Learning Strategies in Higher Education, ed: IGI Global*, pages 273–300, 2024.

[17] Falayi, W. et al. Survey of distributed and decentralized iot securities: approaches using deep learning and blockchain technology. *Future Internet*, 15, 2023.

[18] Gao, a. o., He. Artificial intelligence applications in smart healthcare: A survey. *Future Internet*, 16:308, 2024.

[19] GonÃ§alves, J., Ayub, M., Zhumadillayeva, A., Dyussekeyev, K., Ayimbay, S., and RodrÃguez, D. Decentralized machine learning framework for the internet of things: Enhancing security, privacy, and efficiency in cloud-integrated environments. *Electronics*, 13(21):4185, 2024.

[20] Gupta and Tripathi. A comprehensive survey on cloud computing scheduling techniques. *Multimedia Tools and Applications*, 83, 2024.

[21] Haryanti, R. et al. The design science research methodology (dsrm) for self-assessing digital transformation maturity index in indonesia. In *IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA)*, 2022.

[22] Hovenga and Hullin. Global collaborative leadership challenges and economic drivers. In *in Roadmap to Successful Digital Health Ecosystems, ed: Elsevier*, pages 35–63, 2022.

[23] Hu, Q. et al. Privacy-preserving healthcare and medical data collaboration service system based on blockchain and federated learning. *Computers, Materials Continua*, 80, 2024.

[24] Issa, M. et al. Blockchain-based federated learning for securing internet of things: A comprehensive survey. *ACM Computing Surveys*, 55, 2023.

[25] Javaid, H. et al. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, 1:100016, 2023.

[26] Khan, a. o., Shiwlani. Revolutionizing healthcare with ai: Innovative strategies in cancer medicine. *International Journal of Multidisciplinary Sciences and Arts*, 3:316–324, 2024.

[27] Kim, P. et al. Blockchained on-device federated learning. *IEEE Communications Letters*, 24, 2019.

[28] Kumari, S. Optimizing mobile platform security with ai-powered real-time threat intelligence: A study on leveraging machine learning for enhancing mobile cybersecurity. *Journal of Artificial Intelligence Research*, 4:332–355, 2024.

[29] Lao, L. et al. A survey of iot applications in blockchain systems: Architecture, consensus, and traffic modeling. *ACM Computing Surveys (CSUR)*, 53, 2020.

[30] Li, S. et al. *On computational thinking and STEM education*, volume 3. Springer, 2020.

[31] Liu, C. et al. Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning. *Knowledge and Information Systems*, 2024.

[32] Lu, H. et al. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Transactions on Vehicular Technology*, 69, 2020.

[33] Mathew, D. Z. R. et al. Advancing healthcare 5.0 through federated learning: Opportunity for security enforcement using blockchain. In *in 2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–6, 2024.

[34] Merlec and In. Blockchain-based decentralized storage systems for sustainable data self-sovereignty: A comparative study. *Sustainability*, 16, 2024.

[35] Mohammed, A. et al. Bahrain's urban transformation: A comprehensive review of smart city development, benefits, and future prospects. In *in 2024 Arab ICT Conference (AICTC)*, pages 237–243, 2024.

[36] Nasir, H. et al. *Securing Permissioned Blockchain-based Systems: An Analysis on the Significance of Consensus Mechanisms*. IEEE Access, 2024.

[37] Omole, O., Rosa, R., Saadi, M., and Rodriguez, D. Agrinas: Neural architecture search with adaptive convolution and spatialâtime augmentation method for soybean diseases. *AI*, 5(4):2945–2966, 2024.

[38] Onyebuchi, M. et al. Cloud-based iot data warehousing technology for e-healthcare: A comprehensive guide to e-health grids. In *Pioneering Smart Healthcare 5.0 with IoT, Federated Learning, and Cloud Security, ed: IGI Global*, 2024.

[39] Paul and Singh. Healthcare employee engagement using the internet of things: a systematic overview. *The Adoption and Effect of Artificial Intelligence on Human Resources Management, Part A*, 2023.

[40] Perle, F. and others. Data security in the digital age: A consolidated guide for psychologists to understand health insurance portability and accountability act-compliant telehealth. *Translational Issues in Psychological Science*, 10:111, 2024.

[41] Rahnasto, J. enetic data are not always personalâdisaggregating the identifiability and sensitivity of genetic data. *Journal of Law and the Biosciences*, 10, 2023.

[42] Rosa, R. L., Rodriguez, D. Z., and Bressan, G. Sentimeter-br: A social web analysis tool to discover consumers' sentiment. In *2013 IEEE 14th international conference on mobile data management*, volume 2, 2013.

[43] RosÃ¡rio and Raimundo. Internet of things and distributed computing systems in business models. *Future Internet*, 16, 2024.

[44] Roth, a. o., Petersilge. Himss-siim enterprise imaging community white papers: Reflections and future directions. *Journal of Imaging Informatics in Medicine*, 37:429–443, 2024.

[45] Salgado, J., Rodriguez, D., Dias, V., and Rosa, R. Automated validation of spatial data. In *2024 International Conference on Software, Telecommunications and Computer*, 2024.

[46] Sargiotis, D. Data security and privacy: Protecting sensitive information. In *Data Governance: A Guide, ed: Springer*, pages 217–245, 2024.

[47] Sheller, E. et al. *Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data*, volume 10. Scientific reports, 2020.

[48] Silva, S. D., Rodriguez, D., Rosa, R., Adasme, P., and Saadi, M. Ai/ml-enhanced security monitoring for 5g-enabled big data sensor networks. In *2024 International Conference on Software, Telecommunications and Computer*, 2024.

[49] Sivakumar, M. et al. Addressing privacy concerns with wearable health monitoring technology. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 14:e1535, 2024.

[50] Teodoro, A. A., Silva, D. H., Rosa, R. L., Saadi, M., Wuttisittikulkij, L., Mumtaz, R. A., and Rodriguez, D. Z. A skin cancer classification approach using gan and roi-based attention mechanism. *Journal of Signal Processing Systems*, 95(2-3), 2023.

[51] Ugochukwu, O., Ayub, M., Adasme, P., Rosa, R., Rodriguez, D., and Saadi, M. Adaptive resource management in software-defined networks for iot ecosystems. In *2024 International Conference on Software, Telecommunications and Computer*, 2024.

[52] Vieira, S. T., Rosa, R. L., and Rodrí’guez, D. Z. A speech quality classifier based on tree-cnn algorithm that considers network degradations. *Journal of Communications Software and Systems*, 16(2), 2020.

[53] Wager, L. et al. *Health care information systems: a practical approach for health care management*. John Wiley Sons, 2021.

[54] Wang, S. and others. Integrating digital technologies and public health to fight covid-19 pandemic: key technologies, applications, challenges and outlook of digital healthcare. *International Journal of Environmental Research and Public Health*, 18:6053, 2021.

[55] Ye, W. et al. Openfedllm: Training large language models on decentralized private data via federated learning. In *Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 2024.

[56] Yingngam, K. et al. Motivations and barriers to using digital healthcare. In *Multi-Sector Analysis of the Digital Healthcare Industry, ed: IGI Global*, pages 33–79, 2024.

[57] Zeydan, A. et al. *Managing Distributed Machine Learning Lifecycle for Healthcare Data in the Cloud*. IEEE Access, 2024.

[58] Ètefan, a. o., Rusu. Empowering healthcare: A comprehensive guide to implementing a robust medical information systemâcomponents, benefits, objectives, evaluation criteria, and seamless deployment strategies. *Applied System Innovation*, 7:51, 2024.