INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 10, (2024) E-ISSN: 2222-6990

Development of Blockchain Framework to Enhance Data Integrity in Healthcare Information Systems in Jiangxi, China

Hu Ming
City Graduate School, City University Malaysia
Email: 7752379@qq.com

Dr. Shamsul Arrieya Bin Ariffin
Faculty of Computing and Meta Technology, Sultan Idris Education University, Perak, Malaysia
Email: shamsul@meta.upsi.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i10/23253 DOI:10.6007/IJARBSS/v14-i10/22727

Published Date: 15 October 2024

Abstract

The integration of electronic information systems (EIS) in healthcare has revolutionized data management, enhancing efficiency and accessibility. The centralized nature of current electronic information systems in Jiangxi's healthcare sector poses significant vulnerabilities, including risks of data tampering, unauthorized access, and single points of failure. These vulnerabilities threaten the security and integrity of sensitive patient data, potentially leading to severe consequences such as breaches of patient confidentiality, financial losses, and diminished public trust in the healthcare system. This study adopts a comprehensive approach to develop and evaluate a blockchain framework for enhancing data integrity in Jiangxi's healthcare information systems. The research is structured into three primary objectives: identifying the key characteristics of blockchain technology that contribute to data integrity, developing a blockchain framework tailored for Jiangxi's EIS, and evaluating the effectiveness of the implemented blockchain system. Data will be collected through literature reviews, expert interviews, and pilot implementations, followed by rigorous analysis to assess the framework's impact on data security and integrity. The study anticipates that the blockchain framework will significantly enhance the integrity and security of healthcare data in Jiangxi. The expected outcomes include reduced incidents of data tampering and unauthorized access, improved traceability and accountability of data transactions, and strengthened public trust in the healthcare system.

Keywords: Blockchain Technology, Healthcare, Data Security, Data Integrity.

Introduction

In 2009, an unidentified person or group going by the name of Satoshi Nakamoto launched Bitcoin, which introduced the world to blockchain technology. As a distributed ledger, its original purpose was to keep track of cryptocurrency transactions and introduce a novel method of handling both financial and personal data securely. Blockchain's defining characteristics are its decentralized and tamper-resistant nature and the fact that information is stored in blocks that are cryptographically linked to one another to form an immutable chain (Tseng et al., 2020). Beyond the realm of cryptocurrencies, this technology has received attention for its revolutionary possibilities in data management and security. Blockchain's decentralized design, transparency, and cryptography techniques have opened the door to a wide range of use cases beyond financial transactions. Improving healthcare data integrity has never been easier than with its decentralized, tamper-resistant, and cryptographically secure design. Critical for private medical information, the unchangeable data block chain provides visibility and auditability (Khezr et al., 2019).

The security of digital information has always been a top priority for IT professionals. For trustworthy record-keeping and decision-making, it is crucial to safeguard data against tampering and loss throughout storage, transfer, and processing. In the past, data verification and access controls were the primary means of ensuring data accuracy. Data breaches, cyberattacks, and illegal access are all new threats made possible by the proliferation of digital information systems and the internet (Ali et al., 2022). This has led to an increased emphasis on data integrity as businesses and government agencies look for foolproof methods of protecting the accuracy of their electronic documents.

The healthcare industry has considerable difficulties in preserving data integrity due to the large and delicate data repositories it houses. With the proliferation of cyber dangers, the old ways of data verification and access control aren't cutting it anymore, thus there's a renewed emphasis on strong data security measures (Saeed et al., 2022). More and more, people are starting to see blockchain as a way to solve these problems by making sure that electronic health data are accurate and secure (Attaran, 2022).

The ability to store, distribute, and manage data across several sectors is made possible by electronic information systems, which represent the backbone of the modern society. They developed from early computer systems used for data processing in the middle of the 20th century. These systems have grown increasingly complex as technology has advanced, and now incorporate databases, software, networks, and hardware. Electronic information systems are already widespread in all kinds of industries, from medicine and banking to government and more (Faccia & Mosteanu, 2019). Electronic information systems have numerous advantages over traditional ones, but their open nature also makes them vulnerable to threats to data security and trustworthiness, calling for constant innovation and research to address these concerns.

Modern healthcare EIS incorporate sophisticated software, networks, and databases to manage patient information. Blockchain and other new solutions are needed to ensure the integrity of data because of their open nature, which makes them susceptible to security risks (Vyas et al., 2022). Data security and integrity are major concerns in Jiangxi's healthcare

industry due to the prevalence of electronic information systems used for data management. Patient data security can be compromised due to these systems' centralized design, which introduces vulnerabilities including single points of failure (Rahman et al., 2020). These systems are integral to the digital infrastructure, supporting everything from government services to private sector operations (Berdik et al., 2021). However, the reliance on such systems brings forth significant challenges in data integrity and security. The risk of data tampering, unauthorized access, and manipulation looms large, threatening the very fabric of digital trustworthiness that modern civilization depends upon. The centralized nature of current electronic information systems in Jiangxi presents a single point of failure, which is a glaring vulnerability in the quest for robust data integrity (Rahman et al., 2020).

Serious repercussions could befall Jiangxi's healthcare industry in the absence of resolution to these data integrity concerns. Public trust might be eroded and individuals could suffer serious harm as a result of data breaches exposing sensitive patient information. Financial losses owing to fraud and lower efficiency in healthcare operations are two potential economic impacts (Awan et al., 2020). The potential for data breaches and fraudulent activities could escalate, undermining public trust and jeopardizing the security of sensitive information. Economic ramifications could include financial losses from fraud, decreased efficiency due to lack of trust in digital transactions, and a stifling of innovation due to the fear of intellectual property theft. Socially, the erosion of data reliability could lead to misinformation, affecting decision-making processes at both the individual and governmental levels. The cumulative effect of these issues could significantly hinder Jiangxi's progress towards technological advancement and economic growth (Awan et al., 2020).

We suggest integrating blockchain technology into Jiangxi's healthcare systems to improve data integrity. According to Hussien et al. (2019), blockchain technology has the potential to completely transform healthcare data management by making it more secure and transparent. This would greatly decrease the chances of data manipulation and illegal access. To mitigate these risks and enhance the data integrity of electronic information systems in Jiangxi, this study proposes the integration of blockchain technology. Blockchain offers a decentralized framework, which inherently counters the single point of failure issue prevalent in centralized systems. By leveraging the immutable and transparent nature of blockchain, Jiangxi can pioneer a shift towards a more secure, distributed ledger for data management. This technology not only promises to reduce the incidence of data tampering and unauthorized access but also enhances the traceability and accountability of data transactions. Implementing blockchain could revolutionize the way data is handled, fostering a new era of digital trust and security that could set a benchmark for electronic information systems globally.

In order to address the urgent problem of maintaining the integrity of data in Jiangxi's healthcare information systems, the implementation of blockchain technology stands out as a solution that may completely revolutionize the situation. The implementation of blockchain technology allows Jiangxi to strengthen its data management infrastructure by providing it with a decentralized framework. This helps to mitigate the dangers that are connected with centralized systems. As a result of the irreversible and transparent nature of blockchain technology, incidents of data tampering and unauthorized access can be drastically decreased, hence building a higher degree of confidence and security within the healthcare

ecosystem. Furthermore, the intrinsic characteristics of blockchain technology improve the traceability and accountability of data transactions, so paving the way for a paradigm shift in the way that healthcare data is managed. The adoption of blockchain technology not only tackles existing weaknesses, but it also establishes Jiangxi as a pioneer in the implementation of innovative data management techniques, thereby establishing a new standard for electronic information systems all across the world.

Literature Review

The blockchain technology has emerged as a revolutionary framework that is capable of improving data integrity across a variety of sectors, including healthcare, banking, supply chain management, and other areas. Blockchain is a decentralized and immutable digital ledger that records transactions across several computers in a manner that assures data is consistent, safe, and tamper-proof. At its heart, blockchain is a distributed ledger that cannot be altered. Blockchain technology possesses fundamental qualities that have the potential to improve data integrity (Wei et al., 2020). These properties include decentralization, cryptographic security, transparency, and immutability. In traditional centralized systems, where data is susceptible to corruption, unauthorized access, and manipulation, these features jointly solve many of the issues involved with maintaining data integrity. These challenges also include the fact that data is subject to manipulation.

When it comes to improving data integrity, the decentralization that is inherent in blockchain technology is absolutely necessary. A single point of failure can put the entire data set at risk in traditional centralized systems by compromising the integrity of the data. It's possible that this is the result of hostile attacks, human error, or issues with the system. The blockchain, on the other hand, is dependent on a peer-to-peer network in which every member, also known as a node, is responsible for keeping a copy of the complete blockchain (Komalavalli et al., 2020). The validation of transactions is accomplished by the utilization of a consensus mechanism, which may include proof-of-work or proof-of-stake. This process guarantees that all nodes are in agreement regarding the legitimacy of the transactions before they are added to the blockchain. The elimination of the single point of failure and the creation of an environment in which it is extremely difficult for a single entity to change the data without the agreement of the majority of the network participants are both outcomes of this decentralized approach. This results in the data that is stored on a blockchain being more resistant to attacks and tampering, which ultimately results in an increase in the data's integrity.

Another key feature of blockchain technology that contributes to the enhancement of data integrity is cryptographic security. Every block that makes up a blockchain includes a cryptographic hash of the block that came before it, a timestamp, and information on financial transactions. Input data is converted by the hash function into a string of characters of a predetermined length, which serves as a digital fingerprint that is unique to each individual. When the input data is altered in any way, regardless of how slight the change may be, the resulting hash value is radically different. Because of this quality, it is possible to easily identify even the most minute changes that have been made to the data contained within a block. In addition, the combination of cryptographic hashes and the chaining of blocks results in the creation of a record of all transactions that is both secure and transparent. Not only does the utilization of cryptography ensure the safety of the data, but it also guarantees its validity and

non-repudiation (Wang et al., 2021). This means that once a transaction is recorded, it cannot be rejected or altered in any way. When it comes to ensuring data integrity in contexts where data security and authenticity are of the utmost importance, this cryptographic underpinning is absolutely necessary.

Transparency is yet another essential characteristic of blockchain technology that plays a role in maintaining the integrity of data. A public ledger that is open to all members in a blockchain network is where all transactions are recorded. This ledger is visible to everyone in the network. The fact that this transparency makes it possible to conduct audits and verifications of data in real time contributes to an increase in user trust. In industries such as supply chain management, for example, blockchain technology may provide an immutable record of the route that a product takes from its point of origin to the consumer. This ensures that all parties involved have access to the same information and can independently verify that it is accurate. Because of this amount of transparency, the likelihood of fraud and discrepancies is decreased, which ultimately results in an improvement in the data's overall integrity. Furthermore, transparency in blockchain can also improve accountability and traceability. This is because every transaction is time-stamped and connected to a specific participant (Yi et al., 2021). This makes it much simpler to identify the origin of any errors or inconsistencies that may occur.

The immutability of blockchain technology is likely the most important characteristic of this technology in terms of improving the integrity of data. Following the addition of a block to the blockchain and its subsequent validation by the network, it is extremely difficult, if not impossible, to modify the data contained within that block without also modifying all blocks that follow after it. This occurs due to the fact that every block contains the hash of the block that came before it, so producing a chain of blocks that is resistant to being altered. The amount of computational effort that is required to modify a block and then revalidate all subsequent blocks renders such attempts economically and practically impossible, particularly in blockchain networks that are large and have been in operation for a considerable amount of time (Zhou et al., 2020). For the purpose of establishing a trustworthy and long-lasting record that can be relied upon over time, immutability guarantees that historical data will continue to be unaltered and unaltered. For the sake of regulatory compliance and legal matters, where it is vital to keep a history of transactions that has not been altered, this attribute is very beneficial.

The capacity of blockchain technology to improve data integrity is increasingly being investigated and deployed across a wide range of businesses, with a great deal of success. When it comes to the healthcare industry, for instance, blockchain technology can offer a safe and tamper-proof method of storing and exchanging patient records. The use of blockchain technology can help minimize the number of medical errors, improve patient outcomes, and promote more effective care coordination. This is accomplished by assuring that medical records are correct and cannot be altered. Patients are able to have a higher level of confidence in the safety and precision of their health information, while healthcare providers are able to rely on the integrity of the data in order to make educated clinical decisions. Furthermore, blockchain technology has the potential to facilitate regulatory compliance in the healthcare industry by delivering an auditable record of all data transfers (Shah & Konda,

2022). This can assist firms in being in compliance with high data protection and privacy expectations.

The ways in which transactions are carried out and documented are being completely transformed by blockchain technology in the banking sector (Chowdhury et al., 2021). The traditional banking system is dependent on centralized databases, which are susceptible to instances of fraud, hacking, and errors. The irreversible and decentralized ledger that blockchain technology provides offers an option that is more secure. According to blockchain, every transaction is recorded openly and cannot be changed after it has been confirmed. The integrity of the financial data is improved as a result of this, as is the level of confidence among the participants, the removal of the requirement for intermediaries, and the reduction of the expenses associated with transactions. System architectures that are built on blockchain technology have the potential to improve procedures like as international payments, securities trading, and compliance reporting, hence making these activities more expedient, efficient, and trustworthy.

Blockchain technology is also having a huge impact in managing supply chains, which is another area of application (Dutta et al., 2020). There are several parties involved in traditional supply chains, and each of them is responsible for maintaining their own records. This results in inefficiencies, delays, and discrepancies. Blockchain has the potential to offer a unified, shared ledger in which all transactions are recorded in a way that is both transparent and unchangeable. By doing so, it is possible to track things in real time, which enhances traceability and decreases the likelihood of fraudulent activity and counterfeiting. By providing a verifiable record of the origin, processing, and distribution of food goods, blockchain technology can, for instance, enable the food sector to maintain the integrity of its supply chain. This, in turn, can improve both the safety of food and the faith that consumers have in the company.

Additionally, blockchain technology has the potential to improve data integrity in a wide variety of other applications, in addition to these industries (Wei et al., 2020). When it comes to the government, blockchain technology has the potential to enhance the reliability of public documents, including voting systems, property registries, and identity management. Blockchain technology has the potential to eliminate instances of corruption, promote transparency, and improve citizen faith in government procedures by giving a record that cannot be altered and is completely transparent. On the subject of intellectual property, blockchain technology has the potential to safeguard the authenticity of digital content by delivering an unchangeable record of ownership and provenance. This can be of great assistance to creators and rights holders in their efforts to prevent infringement and piracy of their works.

Although there are a great number of benefits associated with the deployment of blockchain technology to improve data integrity, there are also some problems involved. The issue of scalability continues to be a big concern, as blockchain networks have the potential to become tedious and resource-intensive as the number of transactions increases. Shading, off-chain transactions, and layer-2 protocols are some of the solutions that are currently being researched in order to solve these issues regarding scalability. Interoperability across the various blockchain networks and with the systems that are already in place is also essential for making blockchain technology more widely adopted. The full potential of blockchain

technology can only be realized through the implementation of standards and protocols that facilitate the exchange and integration of data in a trouble-free manner. Because the transparency of blockchain technology may come into conflict with the requirement to safeguard sensitive information, privacy is another key factor to take into account (Nissenbaum, 2020). In order to overcome these privacy problems while still preserving the benefits of blockchain's immutability and transparency, advanced cryptographic approaches are now being investigated. Some examples of these techniques include zero-knowledge proofs and secure multi-party computing.

Blockchain technology provides a solid foundation for improving data integrity by virtue of its decentralized, cryptographically secure, transparent, and immutable qualities through which it operates. Many of the problems that are associated with traditional centralized systems are addressed by blockchain technology. These problems include the elimination of single points of failure, the guarantee of data authenticity and non-repudiation, the provision of real-time auditing and verification, and the creation of a record that is both permanent and tamper-proof. The widespread implementation of blockchain technology across a variety of sectors, including healthcare and banking, as well as supply chain management and government, highlights the technology's potential to transform the way data is stored and security is maintained. In spite of the fact that there are still obstacles to overcome, constant research and innovation are paving the way for blockchain solutions that are more scalable, interoperable, and protect confidentiality. As these improvements continue, blockchain technology is positioned to play a crucial role in preserving the integrity of data in our increasingly digital and linked world (Duggineni, 2023). This is because blockchain helps to verify the authenticity of data.

Methodology

The proposed framework for this study is centered on integrating blockchain technology into Jiangxi's healthcare information systems to enhance data integrity and security. The framework consists of several key components: a decentralized ledger system, consensus algorithms, smart contracts, and integration points with existing systems. The decentralized ledger system ensures that all transactions are securely recorded and immutable, thereby preventing unauthorized modifications. Consensus algorithms are used to validate transactions across the network, ensuring consistency and reliability of the data. Smart contracts automate and enforce the rules for data access and sharing, reducing the risk of human error and fraud. Integration points enable seamless interaction between the blockchain network and the existing healthcare information systems, facilitating secure and efficient data exchange.

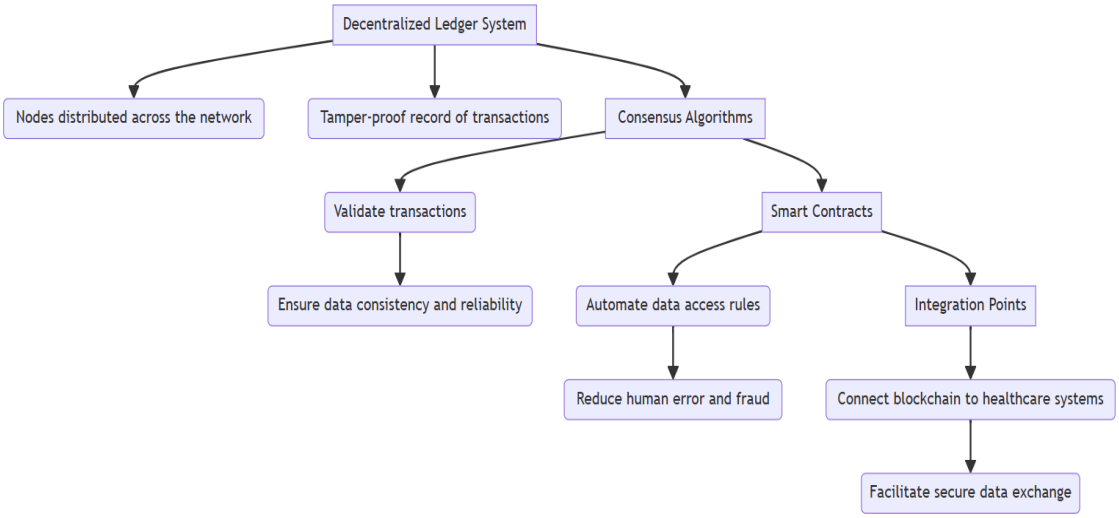

Figure 1: Proposed Framework

The diagram of the proposed framework visually represents these components and their interactions. The decentralized ledger forms the backbone of the framework, with nodes distributed across the network to maintain a tamper-proof record of all transactions. The consensus algorithms ensure that only validated transactions are added to the ledger, while the smart contracts define the rules for data handling. The integration points connect the blockchain network to the healthcare systems, allowing for real-time data synchronization and enhanced security measures. This framework is designed to address the specific needs and constraints of healthcare information systems in Jiangxi, ensuring scalability, interoperability, and compliance with regulatory requirements.

Once the prototype has been produced, it is then installed and configured into the information systems that are designed for healthcare. In order to ensure the safety of the network, this requires the installation of the required infrastructure, the deployment of nodes, and the configuration of security measures. The functionality, performance, and security of the blockchain framework are all subjected to extensive testing in order to guarantee their integrity. In order to discover and address any problems or vulnerabilities, this comprises testing at the unit level, testing at the integration level, and testing at the system level.

Evaluation of the efficiency of the blockchain architecture in improving data integrity and security constitutes the final element of the research design process. For the purpose of evaluating the performance of the framework, different metrics and performance indicators that have been predefined are utilized. These metrics and indicators include transaction throughput, latency, consensus efficiency, and data consistency. In order to examine the data that has been acquired, statistical methods and visualization tools are utilized. This analysis provides insights into the system's strengths and limitations. In addition, qualitative input from users and stakeholders is acquired through the use of surveys, interviews, and usability testing. This feedback provides useful perspectives on the user experience and the perceived impact of the blockchain framework.

References

Ali, A., Septyanto, A. W., Chaudhary, I., Al Hamadi, H., Alzoubi, H. M., & Khan, Z. F. (2022). Applied Artificial Intelligence as Event Horizon Of Cyber Security. 2022 International Conference on Business Analytics for Technology and Security (ICBATS),

Awan, K. A., Din, I. U., Almogren, A., Guizani, M., & Khan, S. (2020). StabTrust—A stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks. *IEEE Access*, *8*, 21159-21177.

Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. *Information Processing & Management*, *58*(1), 102397.

Chowdhury, M. U., Suchana, K., Alam, S. M. E., & Khan, M. M. (2021). Blockchain application in banking system. *Journal of Software Engineering and Applications*, *14*(7), 298-311.

Duggineni, S. (2023). Impact of controls on data integrity and information systems. *Science and Technology*, *13*(2), 29-35.

Dutta, P., Choi, T.-M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation Research Part E: Logistics and Transportation Review*, *142*, 102067.

Faccia, A., & Mosteanu, N. R. (2019). Tax evasion, information systems and blockchain. *Journal of Information Systems & Operations Management*, *13*(1), 65-74.

Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In *Handbook of research on blockchain technology* (pp. 349-371). Elsevier.

Nissenbaum, H. (2020). Protecting privacy in an information age: The problem of privacy in public. In *The ethics of information technologies* (pp. 141-178). Routledge.

Rahman, S. A., Tout, H., Talhi, C., & Mourad, A. (2020). Internet of things intrusion detection: Centralized, on-device, or federated learning? *IEEE network*, *34*(6), 310-317.

Shah, V., & Konda, S. R. (2022). Cloud Computing in Healthcare: Opportunities, Risks, and Compliance. *Revista Espanola de Documentacion Cientifica*, *16*(3), 50-71.

Tseng, L., Wong, L., Otoum, S., Aloqaily, M., & Othman, J. B. (2020). Blockchain for managing heterogeneous internet of things: A perspective architecture. *IEEE network*, *34*(1), 16-23.

Wang, L., Liu, J., & Liu, W. (2021). Staged data delivery protocol: A blockchain-based two-stage protocol for non-repudiation data delivery. *Concurrency and Computation: Practice and Experience*, *33*(13), e6240.

Wei, P., Wang, D., Zhao, Y., Tyagi, S. K. S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems*, *102*, 902-911.

Yi, W., Huang, X., Yin, H., & Dai, S. (2021). Blockchain-based approach to achieve credible traceability of agricultural product transactions. Journal of Physics: Conference Series,

Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. *IEEE access*, *8*, 16440-16455.