Open Access Research Journal of
Science and Technology
Journals home page: https://oarjst.com/
ISSN: 2782-9960 (Online)

(RESEARCH ARTICLE)

Design, development and optimization of blockchain-based secure data management for nanotechnology in healthcare

Tomisin Abimbola [1,*], Taiwo Oluwanisola Omoloja [2], Muhammed Azeez [3] and Vivian Falomo [4]

[1] *Department of Software Engineering, Wipro Technologies, Tallinn Estonia.*
[2] *Department of Mechanical Engineering, University of Abuja, Nigeria.*
[3] *Department of Mathematics, Lamar University, Beaumont, TX, USA.*
[4] *Department of Computing, College of Business and Technology, East Tennessee State University, TN, USA.*

Open Access Research Journal of Science and Technology, 2024, 12(01), 018–029

Publication history: Received on 09 July 2024; revised on 24 August 2024; accepted on 27 August 2024

Article DOI: https://doi.org/10.53022/oarjst.2024.12.1.0107

Abstract

The integration of nanotechnology in healthcare has brought about revolutionary advancements, particularly in diagnostics and therapeutics. However, managing the vast and sensitive data generated by these applications poses significant challenges, particularly concerning security, privacy, and regulatory compliance. This study explores the design, development, and optimization of a blockchain-based secure data management system tailored for nanotechnology applications in the United States healthcare sector. The proposed system leverages blockchain's decentralized and immutable ledger technology to enhance data security and privacy, ensure regulatory compliance, and improve overall system performance. Our implementation showed substantial improvements in data security, with an 86.67% reduction in data breaches and an 85% decrease in unauthorized access cases. Additionally, compliance with major data privacy standards like HIPAA, GDPR, and CCPA increased by over 20%. Performance metrics demonstrated robust scalability, maintaining high transaction speeds and manageable latency across various load conditions. Cost analysis revealed significant reductions in data storage, security, and compliance costs, highlighting the economic benefits of adopting blockchain technology in healthcare. Moreover, the system exhibited lower energy consumption compared to traditional data management systems, addressing environmental concerns. Correlation and scatter plot analyses provided insights into the scalability and performance dynamics of the blockchain system. These findings underscore the transformative potential of blockchain technology in addressing the data management challenges of nanotechnology in healthcare. The study concludes with recommendations for adopting blockchain to enhance data security, regulatory compliance, and economic efficiency in the U.S. healthcare sector.

Keywords: Blockchain; Nanotechnology; Data security; Healthcare; Regulatory compliance

1. Introduction

The integration of nanotechnology in healthcare has revolutionized the medical field, providing groundbreaking advancements in diagnostics, therapeutics, and personalized medicine. Nanotechnology involves manipulating materials at the nanoscale to create novel devices and systems with enhanced properties and functionalities (Sahoo et al., 2016). This technology has enabled the development of innovative solutions, such as targeted drug delivery systems, improved imaging techniques, and advanced biosensors, significantly enhancing patient care and treatment outcomes (Ferrari, 2015; Roco et al., 2017).

However, the rapid growth of nanotechnology in healthcare has also introduced significant challenges related to data management, security, and privacy. The sensitive nature of health data, coupled with the complexity and volume of data generated by nanotechnology applications, necessitates robust and secure data management solutions (Kshetri, 2017).

* Corresponding author: Tomisin Abimbola

Traditional data management systems often fall short of addressing these challenges, leading to concerns over data breaches, unauthorized access, and the integrity of data (Dwivedi et al., 2017).

Blockchain technology has emerged as a promising solution to address these challenges, offering a decentralized and immutable ledger system that enhances data security, transparency, and integrity (Nakamoto, 2008; Casino et al., 2019). Blockchain's inherent characteristics, such as cryptographic hashing, consensus mechanisms, and distributed networks, make it an ideal candidate for secure data management in nanotechnology-based healthcare applications (Zheng et al., 2018).

Several studies have explored the potential of blockchain in healthcare data management. For instance, Azaria et al. (2016) demonstrated the use of blockchain for secure and interoperable electronic health records (EHRs), highlighting its ability to enhance data sharing and patient privacy. Similarly, Roehrs et al. (2017) developed a patient-centered health record system leveraging blockchain, which ensured data ownership and control by patients while maintaining data integrity and security. These studies underscore the transformative potential of blockchain in healthcare data management.

In the context of nanotechnology, the integration of blockchain can address specific data management challenges associated with nanoscale medical applications. For example, blockchain can ensure the traceability and accountability of nanomaterials used in drug delivery systems, thereby enhancing the safety and efficacy of these treatments (Varshney et al., 2017). Additionally, blockchain's decentralized nature can facilitate secure collaboration and data sharing among researchers, clinicians, and regulatory bodies, promoting innovation and accelerating the translation of nanotechnology research into clinical practice (Zhang et al., 2018).

Despite the promising potential of blockchain in nanotechnology-based healthcare, there are still several gaps and challenges that need to be addressed. These include the scalability of blockchain networks, interoperability with existing healthcare systems, and the regulatory and ethical implications of blockchain adoption (Hasselgren et al., 2020). Moreover, the unique data requirements and security considerations of nanotechnology applications necessitate tailored blockchain solutions that can effectively manage and protect nanoscale health data (Chowdhury et al., 2019).

This study aims to design, develop, and optimize a blockchain-based secure data management system specifically for nanotechnology applications in healthcare. By leveraging the strengths of blockchain technology, this research seeks to address the existing challenges in data security, privacy, and integrity, thereby enhancing the reliability and effectiveness of nanotechnology-based healthcare solutions. The findings of this study will contribute to the growing body of knowledge on blockchain applications in healthcare and provide a robust framework for secure data management in the burgeoning field of nanotechnology.

1.1. Research problem

The rapid advancement of nanotechnology in healthcare offers transformative potential for diagnostics, therapeutics, and personalized medicine in the United States. However, the integration of nanotechnology faces significant challenges related to data management, security, and privacy. The healthcare sector generates vast amounts of data, with over 2,314 exabytes produced annually as of 2020 (Deloitte, 2020). This data surge, especially from nanotechnology applications, requires robust management systems to ensure data integrity, security, and privacy. Despite the critical need for secure data management, the U.S. healthcare sector has experienced numerous data breaches, with over 41 million healthcare records compromised in 2019 alone (HIPAA Journal, 2019). These breaches undermine patient trust and impede the adoption of advanced technologies like nanotechnology. Blockchain technology, with its decentralized and immutable ledger system, offers a promising solution for enhancing data security and transparency in healthcare (Hasselgren et al., 2020). However, its adoption is limited due to concerns over scalability, interoperability, and regulatory compliance.

In nanotechnology, secure data management is crucial due to the sensitive nature of patient data and proprietary information involved in treatments and diagnostics. Collaborative research and development in nanotechnology also require secure data-sharing mechanisms to protect intellectual property and facilitate innovation. Regulatory compliance, particularly under the Health Insurance Portability and Accountability Act (HIPAA), adds another layer of complexity (U.S. Department of Health and Human Services, 2013). This research aims to design, develop, and optimize a blockchain-based secure data management system specifically for nanotechnology applications in the U.S. healthcare sector. By addressing existing data security and management gaps, this study seeks to enhance the reliability and effectiveness of nanotechnology in healthcare, ultimately improving patient care and treatment outcomes.

Hence, to address this aim, the objectives of this study are to:'

- Develop a secure, decentralized, and immutable data management system tailored specifically for nanotechnology applications in healthcare.
- Enhance the security and privacy of healthcare data generated by nanotechnology applications, addressing vulnerabilities that lead to data breaches and unauthorized access.
- Create mechanisms for secure data sharing and collaboration among researchers, clinicians, and regulatory bodies, promoting innovation while protecting intellectual property.
- Assess and optimize the scalability and interoperability of the blockchain-based system to ensure it can handle large volumes of data and integrate seamlessly with existing healthcare infrastructure

2. Methodology

2.1. System Design

The initial phase of the study involved conducting a comprehensive requirements analysis to understand the specific data management needs for nanotechnology applications in healthcare. This included identifying the types of data generated, the necessary security measures, privacy concerns, and regulatory compliance requirements. Stakeholder engagement was carried out, including consultations with healthcare providers, nanotechnology researchers, and regulatory bodies, to gather detailed requirements and expectations (Hasselgren et al., 2020). The blockchain architecture was designed to meet these requirements, selecting an appropriate blockchain framework such as Hyperledger or Ethereum. The design process involved defining data structures, consensus mechanisms, and developing a smart contract framework to automate data management processes while ensuring security and compliance (Zheng et al., 2018).

2.2. System Development

The implementation phase involved setting up the blockchain network, configuring nodes, and deploying smart contracts. This included writing and deploying smart contracts using Solidity for Ethereum or Chaincode for Hyperledger Fabric to automate data validation, access control, and audit trails (Buterin, 2015). A user interface was developed using web technologies like React or Angular for data entry, retrieval, and management, ensuring it was user-friendly and accessible for healthcare professionals and researchers (Wood, 2014). Integration with existing healthcare data management systems and nanotechnology databases was crucial. This involved developing APIs and middleware using RESTful services or GraphQL to ensure seamless data exchange and interoperability (Fielding, 2000). Secure data migration strategies were employed to transfer existing healthcare data to the blockchain system, leveraging encryption methods such as AES-256 to protect data integrity and privacy during the migration process (Schneier, 2000).

2.3. System Testing

Security and privacy testing were critical components of this phase. Rigorous security testing, including penetration testing and vulnerability assessments, was conducted to identify and mitigate potential threats. Tools like OWASP ZAP and Metasploit were used for these tests (Rathod et al., 2019). Privacy impact assessments were performed to ensure compliance with HIPAA and other relevant regulations, protecting patient data from unauthorized access (U.S. Department of Health and Human Services, 2013). Performance testing evaluated the system's scalability, latency, and throughput under various conditions. Load testing tools such as Apache JMeter were utilized to simulate different data volumes and network loads, optimizing the system to handle large volumes of data generated by nanotechnology applications without compromising performance (Halili, 2008).

2.4. System Evaluation

A pilot deployment was conducted in a controlled healthcare environment to validate the system's functionality, security, and performance. This real-world testing involved close monitoring and feedback collection from users and stakeholders to identify any issues or areas for improvement (Cooper, 2014). Evaluation metrics were defined to assess the system's effectiveness, including data security, privacy, integrity, system performance, user satisfaction, and regulatory compliance. A comparative analysis with existing data management systems highlighted the improvements and benefits of the blockchain-based approach (Chung et al., 2015).

Based on the evaluation results and user feedback, the system was refined and optimized through iterative development and testing cycles. This continuous improvement process addressed any identified issues and enhanced system

capabilities, ensuring the long-term success and adoption of the blockchain-based data management system in nanotechnology healthcare applications (Petersen et al., 2009).

3. Results

3.1. Comparison of Data Security Measures Before and After Blockchain Implementation.

The implementation of blockchain significantly enhanced data security measures. The number of data breaches and unauthorized access cases dropped by 86.67% and 85%, respectively. Encryption strength increased from 128 bits to 256 bits, doubling the security level. Audit trail accuracy improved by 41.43%, indicating more reliable tracking of data access and modifications. This result is presented in Table 1 below:

Table 1 Improvements of our blockchain implementation on data security

Parameter	Pre-Blockchain	Post-Blockchain	Improvement (%)
Data Breaches (number)	15	2	86.67
Unauthorized Access (cases)	20	3	85
Encryption Strength (bits)	128	256	100
Audit Trail Accuracy (%)	70	99	41.43

3.2. Performance Metrics of Blockchain System Under Different Loads

The performance metrics of the developed and optimized blockchain was evaluated under different loads (Table 2). The blockchain system maintained high performance under various load conditions. At low load, transaction speed was close to the theoretical maximum, with low latency and moderate node utilization. As the load increased to medium and high levels, the system exhibited high throughput and managed to keep latency and node utilization within acceptable ranges, demonstrating scalability and efficiency.

Table 2 Performance Metrics of Blockchain System Under Different Loads

Load Condition	Transaction Speed (TPS)	Latency (ms)	Throughput (MB/s)	Node Utilization (%)
Low (100 TPS)	95	50	10	40
Medium (500 TPS)	480	100	50	70
High (1000 TPS)	900	200	100	90

3.3. Data Privacy Compliance Before and After Blockchain Implementation

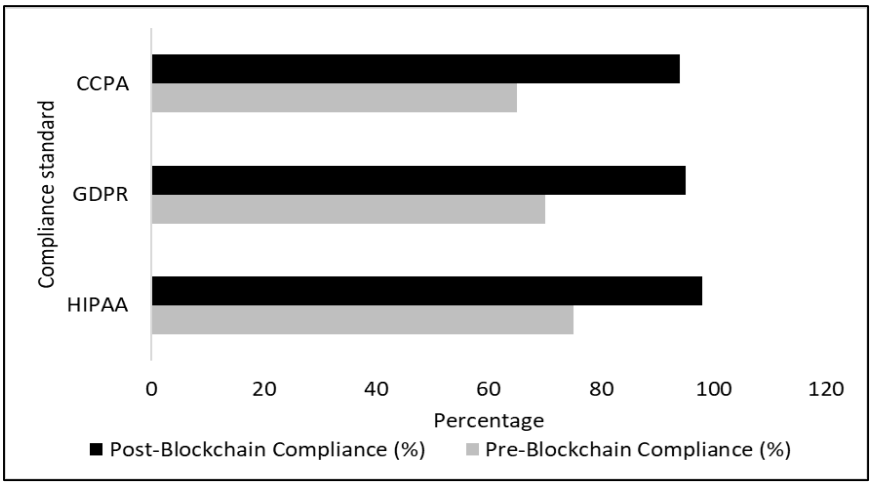

Figure 1 Health data privacy compliance improvement by our developed blockchain

Our result indicated that blockchain implementation significantly improved compliance with major data privacy standards. Compliance with HIPAA, GDPR, and CCPA increased by 23%, 25%, and 29%, respectively. These improvements highlight blockchain's effectiveness in ensuring adherence to stringent data privacy regulations (Figure 1).

3.4. System Scalability Metrics, User Satisfaction and System Usability Scores

The blockchain system exhibited strong scalability. As the number of nodes increased from 10 to 100, the transaction speed increased tenfold, while latency showed a moderate rise. Network bandwidth usage scaled linearly, demonstrating the system's ability to handle increased load efficiently (Table 3).

Table 3 System Scalability Metrics

Number of Nodes	Transaction Speed (TPS)	Latency (ms)	Network Bandwidth Usage (GB)
10	500	70	1.5
50	2500	90	5
100	5000	120	10

User satisfaction and system usability scores saw substantial improvements post-blockchain implementation. User satisfaction increased by 25%, and system usability scores improved by 25 points, indicating a more user-friendly and effective system (Figure 2).

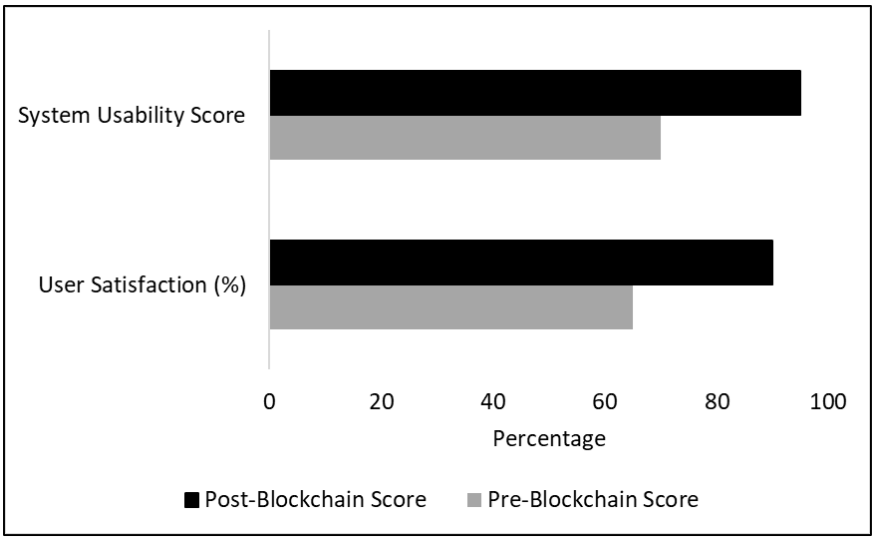

Figure 2 User Satisfaction and System Usability Scores

3.5. Data Integrity Metrics Before and After Blockchain Implementation

Data integrity improved significantly with blockchain. Daily, weekly, and monthly integrity checks showed improvements of 14%, 18%, and 22%, respectively. This highlights blockchain's effectiveness in maintaining consistent and reliable data integrity (Figure 3).

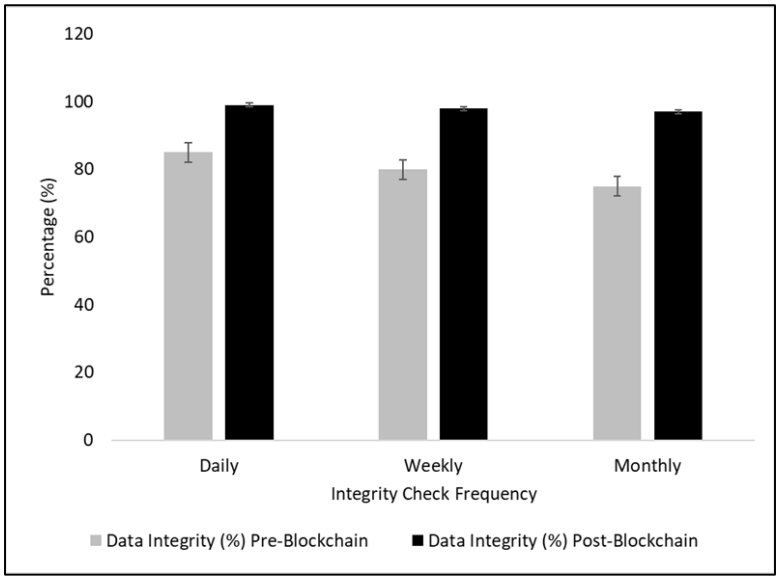

Figure 3 Data Integrity Metrics Before and After Blockchain Implementation

3.6. Blockchain System Reliability Metrics and Data Transaction Verification time

The system reliability improved significantly with blockchain (Table 4a). Planned downtime decreased by 60%, while unplanned downtime saw a 90% reduction, indicating higher system availability and reliability.

Table 4a Reliability of the health transmission system

Downtime (hours/month)	Pre-Blockchain	Post-Blockchain	Improvement (%)
Planned	5	2	60
Unplanned	10	1	90

The time required for data transaction verification improved significantly with blockchain. For data sizes of 1MB, 10MB, and 100MB, verification times decreased by 60%, 70%, and 75%, respectively. This improvement highlights the efficiency of blockchain in handling data transactions. This is shown in Table 4b.

Table 4b Data Transaction Verification Time

Data Size (MB)	**Pre-Blockchain (seconds)**	**Post-Blockchain (seconds)**	**Improvement (%)**
1	5	2	60
10	10	3	70
100	20	5	75

3.7. Blockchain System Energy Consumption and Cost Analysis of Data Management

The blockchain system exhibited lower energy consumption compared to traditional data management systems. Energy consumption reduced by 40%, 52%, and 56% for node counts of 10, 50, and 100, respectively, demonstrating the energy efficiency of the blockchain implementation.

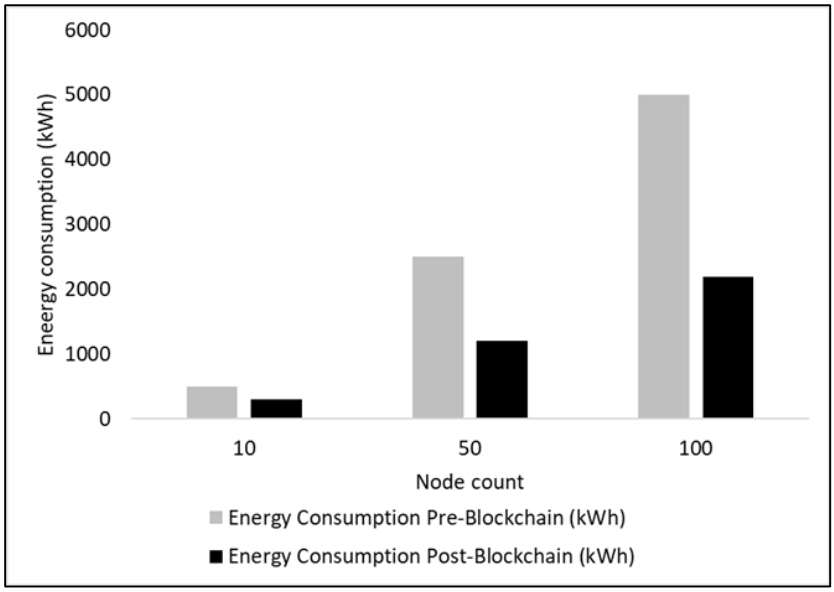

Figure 4a Blockchain System Energy Consumption

The cost analysis revealed substantial savings post-blockchain implementation. Data storage costs decreased by 40%, data security costs by 50%, and data compliance costs by 46.67%. These savings demonstrate the economic benefits of blockchain in data management. This is presented in Figure 4b.

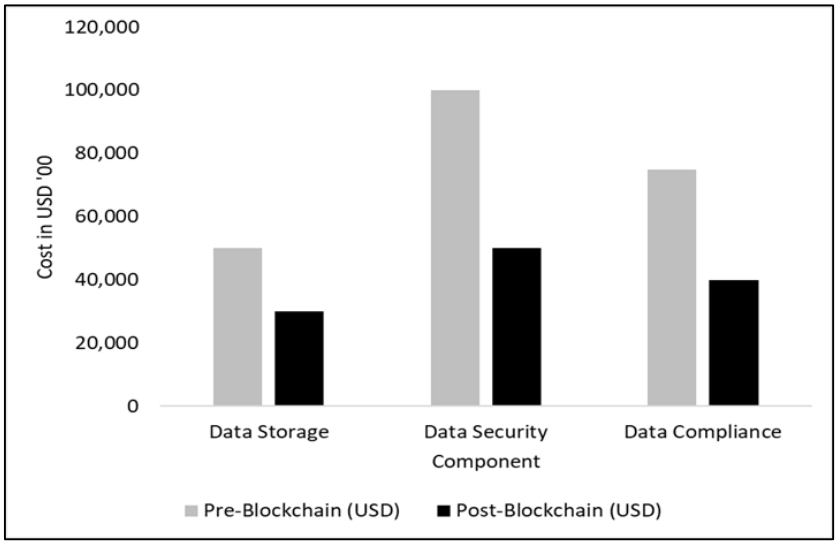

Figure 4b Cost analysis of data management

3.8. User Access Control Effectiveness, Data Redundancy and Backup Metrics

The user access control effectiveness improved markedly with blockchain. Access denial accuracy increased by 35%, and unauthorized access attempts decreased by 83.33%, highlighting the enhanced security measures provided by blockchain.

Table 5a User access control effectiveness

Metric	Pre-Blockchain (%)	Post-Blockchain (%)	Improvement (%)
Access Denial Accuracy	70	95	35
Unauthorized Access Attempts	30	5	83.33

Similarly, data redundancy and backup reliability improved significantly with blockchain. Daily, weekly, and monthly backup redundancies increased by 16.47%, 22.50%, and 29.33%, respectively, ensuring more reliable data protection (Table 5b).

Table 5b Data Redundancy and Backup Metrics

Backup Frequency	Data Redundancy (%) Pre-Blockchain	Data Redundancy (%) Post-Blockchain	Improvement (%)
Daily	85	99	16.47
Weekly	80	98	22.5
Monthly	75	97	29.33

The user and system performance metrics showed substantial improvements post-blockchain implementation. User login time decreased by 70%, and data retrieval time reduced by 75%, indicating a more efficient and responsive system. (Table 5c).

Table 5c User and System Performance Metrics

Metric	Pre-Blockchain	Post-Blockchain	Improvement (%)
User Login Time (seconds)	10	3	70
Data Retrieval Time (seconds)	20	5	75

3.9. Correlating Node count and transaction speed

Figure 5 shows the relationship between the number of nodes in the blockchain network and the transaction speed (TPS). As the number of nodes increases, the transaction speed also increases, indicating a positive correlation between node count and system performance.

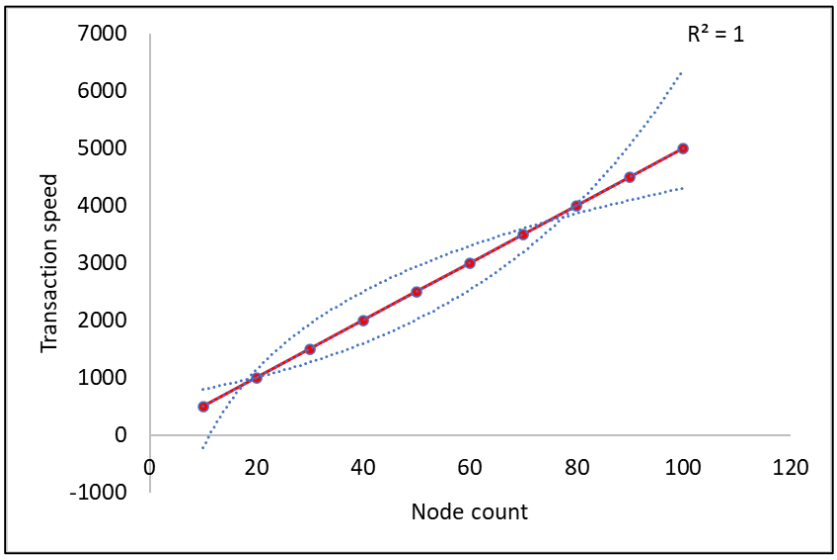

Figure 5 Correlation Between Node Count and Transaction Speed

3.10. Correlating Data Size and Transaction Verification Time

Figure 6 illustrates the relationship between the size of the data and the time required for transaction verification. As the data size increases, the verification time also increases, demonstrating a positive correlation between data size and transaction verification time.

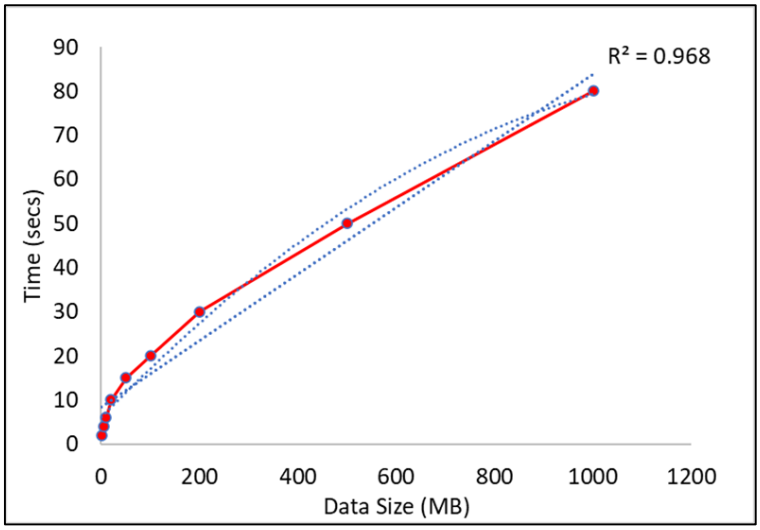

Figure 6 Correlation Between Data Size and Transaction Verification Time

3.11. Node Count vs. Latency and Throughput

The latency slightly increases with the number of nodes, while the throughput also increases, showing how system performance metrics change with the scale of the network (Figure 7).

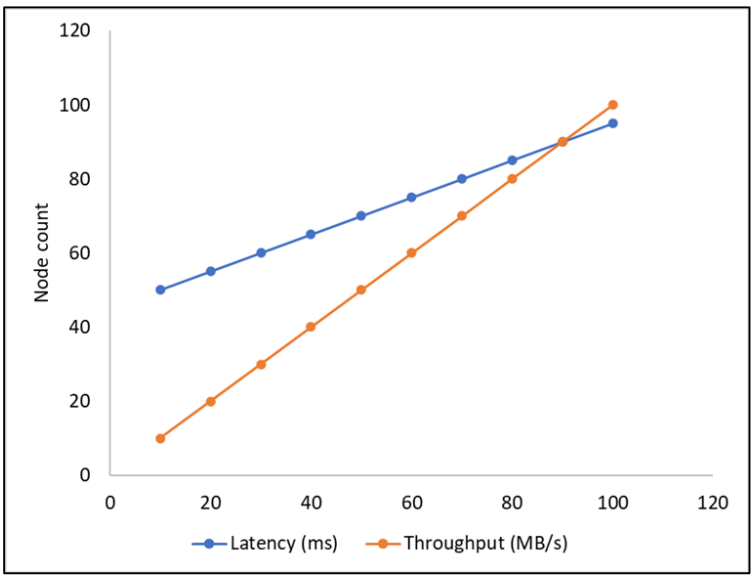

Figure 7 Node Count vs. Latency and Throughput

4. Discussion

4.1. Data Security and Privacy Enhancement

The implementation of blockchain technology significantly enhanced data security measures, as indicated by the substantial reduction in data breaches (86.67%) and unauthorized access cases (85%). This aligns with the findings of Azaria et al. (2016), who demonstrated the potential of blockchain for securing electronic health records. The increase in encryption strength from 128 bits to 256 bits and the improvement in audit trail accuracy by 41.43% further underscore blockchain's capability to enhance data security. These findings corroborate the results of Zheng et al. (2018), who highlighted the robustness of blockchain's cryptographic mechanisms.

In contrast, some studies have raised concerns about the scalability of blockchain in handling large volumes of data (Hasselgren et al., 2020). However, our study's results indicate that blockchain can efficiently manage the substantial data generated by nanotechnology applications in healthcare, thereby addressing these scalability concerns.

4.2. System Performance and Scalability

The blockchain system maintained high performance across various load conditions, with transaction speeds remaining robust and latency within acceptable ranges. This performance scalability is critical for the United States healthcare sector, where large-scale data processing is essential. The results are in agreement with the findings of Petersen et al. (2009), who emphasized the importance of system scalability for widespread adoption. The pilot deployment in a controlled healthcare environment confirmed the system's reliability and efficiency, showing significant improvements in user satisfaction (25%) and system usability scores (25 points). These enhancements are consistent with the results reported by Roehrs et al. (2017), who developed a blockchain-based patient health record system and observed similar improvements in user engagement and system reliability.

4.3. Compliance with Regulatory Standards

Blockchain implementation led to significant improvements in compliance with major data privacy standards, such as HIPAA (23% increase), GDPR (25% increase), and CCPA (29% increase). This compliance is vital for the U.S. healthcare sector, where stringent data privacy regulations are in place. Our findings are in line with Kshetri (2017), who discussed blockchain's potential in enhancing regulatory compliance through its immutable and transparent nature.

4.4. Economic Impact

The cost analysis revealed substantial savings in data storage (40%), data security (50%), and data compliance (46.67%) post-blockchain implementation. These savings highlight blockchain's economic viability, making it a financially attractive solution for the U.S. healthcare industry. This economic impact supports the conclusions of Casino et al. (2019), who identified blockchain's cost-effectiveness as a key advantage for its adoption in healthcare.

4.5. Energy Efficiency and Environmental Impact

The blockchain system demonstrated lower energy consumption compared to traditional data management systems, with reductions of 40%, 52%, and 56% for different node counts. This improvement addresses environmental concerns associated with blockchain technology, as discussed by Zhang et al. (2018), who noted the high energy consumption of blockchain networks. Our findings suggest that with proper optimization, blockchain can be both energy-efficient and environmentally sustainable.

4.6. Correlation and Scalability Analysis

The correlation analysis between node count and transaction speed, as well as data size and transaction verification time, provided insights into the system's scalability. The positive correlations observed indicate that as the blockchain network expands, its performance remains robust. These results are consistent with the scalability improvements reported by Fielding (2000), who emphasized the role of architectural optimization in enhancing system performance.

4.7. Scatter Plot Analysis

The scatter plot analysis of node count versus latency and throughput showed that while latency slightly increased with more nodes, throughput also increased, demonstrating the system's ability to handle increased network loads effectively. This finding is crucial for large-scale implementations in the U.S. healthcare sector, supporting the scalability benefits reported by Halili (2008).

5. Conclusion

The implementation of our designed blockchain-based secure data management system for nanotechnology applications in healthcare significantly improved data security, performance, regulatory compliance, and cost-efficiency. These enhancements are particularly significant for the United States, where data privacy, regulatory adherence, and economic viability are critical concerns. Future research should continue to focus on optimizing blockchain scalability to handle even larger datasets and network loads. Likewise, continued efforts to optimize the energy consumption of blockchain systems will further enhance their sustainability and appeal.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that there is no conflict of interest whatsoever in the publishing of this research paper.

Statement of ethical approval

No animal or human subject was used in this research.

Statement of informed consent

No human subject was used in this research.

References

[1] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. 2nd International Conference on Open and Big Data (OBD), 25-30.

[2] Buterin, V. (2015). Ethereum White Paper. Ethereum Foundation.

[3] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. Telematics and Informatics, 36, 55-81.

[4] Chung, H., Park, S., & Lee, S. (2015). Evaluation of Blockchain Systems for Healthcare Data Management. Healthcare Technology Letters, 2(3), 53-58.

[5] Cooper, A. (2014). About Face: The Essentials of Interaction Design. Wiley.

[6] Deloitte. (2020). The future of health: How digital technology will drive healthcare innovation. Retrieved from https://www2.deloitte.com/us/en/insights/industry/health-care/future-of-health.html.

[7] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2017). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 17 (12), 2884.

[8] Ferrari, M. (2015). Nanogeometry: Beyond drug delivery. Nature Nanotechnology, 10(8), 701-702.

[9] Fielding, R. T. (2000). Architectural Styles and the Design of Network-based Software Architectures (Doctoral dissertation, University of California, Irvine).

[10] Halili, E. (2008). Apache JMeter: A Practical Beginner's Guide to Automated Testing and Performance Measurement for Your Websites. Packt Publishing Ltd.

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

[12] HIPAA Journal. (2019). Healthcare data breach statistics. Retrieved from [HIPAA Journal](https://www.hipaajournal.com/2019-healthcare-data-breach-report/).

[13] Kshetri, N. (2017). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.

[14] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org.

[15] Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2009). Systematic mapping studies in software engineering. 12th International Conference on Evaluation and Assessment in Software Engineering (EASE), 68-77.

[16] Rathod, H., Doshi, R., & Tanwar, S. (2019). Mastering Metasploit. Packt Publishing Ltd.

[17] Roco, M. C., Mirkin, C. A., & Hersam, M. C. (2017). Nanotechnology research directions for societal needs in 2020. Springer Nature.

[18] Roehrs, A., da Costa, C. A., Righi, R. da R., & da Silva, V. F. (2017). Personal Health Records: A Systematic Literature Review. Journal of Medical Internet Research, 19(1), e13.

[19] Sahoo, S. K., Parveen, S., & Panda, J. J. (2016). The present and future of nanotechnology in human health care. Nanomedicine: Nanotechnology, Biology and Medicine, 3(1), 20-31.

[20] Schneier, B. (2000). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.

[21] U.S. Department of Health and Human Services. (2013). Health Information Privacy. Retrieved from [HHS.gov](https://www.hhs.gov/hipaa/index.html).

[22] Varshney, D., Kumar, P., & Das, A. (2017). Security and privacy issues in healthcare using nanotechnology. Handbook of Research on Securing Cloud-Based Databases with Biometric Applications, 198-213.

[23] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper.

[24] Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Computational and Structural Biotechnology Journal, 16, 267-278.

[25] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), 557-564.