A Blockchain-Enabled Security System for Enhancing Data Integrity and Access Control in Hospital Communication Networks

Ruihan Dong

Computer Science, The University of Texas at Arlington, Arlington, USA

Abstract: ***The relentless iteration of medical information technology has positioned the hospital computer communication system as the central nervous system of modern healthcare infrastructure. This system is entrusted with the storage and transmission of highly sensitive data, including patient diagnostic information, comprehensive electronic medical records (EMRs), and critical clinical decision support plans. However, the inherent complexity of hospital network environments, coupled with the continuous evolution of cyber-attack methodologies, has led to increasingly prominent security vulnerabilities within medical communication networks. Incidents of data leakage or tampering pose a direct threat to patient privacy and safety, while the manipulation of diagnostic and treatment information can severely disrupt the continuity of care, potentially leading to life-threatening risks in extreme scenarios. Blockchain technology, characterized by its decentralization, immutability, and cryptographic security, presents an innovative pathway to address these inherent security flaws. Its distributed ledger structure ensures data integrity and provides a transparent, auditable trail for all transactions. This paper, building upon this premise, conducts a systematic study on the construction of a robust security protection system for hospital computer communication networks, supported by blockchain technology. We propose a framework that leverages blockchain to create a secure, tamper-proof repository for access logs and data transaction records, ensuring the traceability and non-repudiation of all data access events. The study details the architectural integration of blockchain within existing hospital information systems, focusing on modules for identity and access management, secure data sharing between departments, and automated audit compliance. By providing a reference model that enhances data confidentiality, integrity, and availability, this research aims to contribute to the development of more resilient and trustworthy medical communication infrastructures, ultimately safeguarding patient welfare and the operational continuity of healthcare services.***

Keywords: Medical Information System, Computer Communication Network, Blockchain, Data Security, Immutability, Distributed Ledger, Patient Privacy, Healthcare Infrastructure.

1. INTRODUCTION

In the field of digital healthcare, the security protection of hospital computer communication networks has become a key issue. Cyberattack incidents emerge in an endless stream—data breaches and ransomware invasions continue to threaten the operational order of medical institutions, and patient privacy information faces serious risks. Relying on a decentralized architecture and encryption mechanisms, blockchain technology opens a new path for data security. The technology ensures data is tamper-proof—achieving transparent traceability and effectively preventing external attacks and internal malicious operations. Establishing a hospital communication network security system based on blockchain technology has core value for medical data preservation. This protective architecture not only promotes the application of medical information sharing but also optimizes service quality, creating a solid foundation for improving diagnosis and treatment efficiency. 1 Introduction to blockchain technology

Blockchain technology was initially recognized as the underlying architecture of Bitcoin; its essence is a decentralized distributed ledger system. The data storage mechanism breaks through the traditional model—information is not concentrated on a single server; network nodes jointly undertake storage functions. Each node maintains a complete copy of the ledger, and data changes require consensus verification by the majority of nodes, enabling the immutability of information. The blockchain system uses cryptographic methods to process transaction information, ensuring data confidentiality. Each transaction carries a timestamp identifier, and chronological ordering forms a chain structure, thereby establishing a complete traceability system. Technical characteristics endow blockchain with multidimensional application potential, covering scenarios such as data protection, identity verification, and smart contract execution. The medical field has ushered in an innovative solution for information security protection; blockchain technology supports full lifecycle management of diagnosis and treatment data—secure storage, efficient transmission, and compliant processing are all technically guaranteed.

Recent advances in artificial intelligence and machine learning demonstrate their transformative potential across biomedical, commercial, and industrial domains. In biomedical engineering, Ding and Wu (2024) provided a systematic review of self-supervised learning applications for ECG and PPG signal processing[1], while Qin et al. (2025) developed optimized deep learning models to combat amyotrophic lateral sclerosis disease progression[4]. Chen et al. (2023) further contributed to this field through generative text-guided 3D vision-language pretraining for unified medical image segmentation[14].

The development and deployment of large language models have seen significant innovation. Zhang (2025) introduced InfraMLForge, a developer tooling framework for rapid LLM development and scalable deployment[2], while Sun et al. (2025) constructed an Automated Machine Learning framework based on large language models[15]. Question answering systems were enhanced by Jiang et al. (2025) through a knowledge-enhanced multi-task learning model for domain-specific applications[9], and Zhuo et al. (2025) developed an intelligent-aware transformer with domain adaptation and contextual reasoning[10].

Advertising technology has evolved through several key contributions. Hu (2025) created GenPlayAds for procedural playable 3D ad creation via generative models[3], while Li, Lin, and Zhang (2025) proposed a privacy-preserving framework incorporating federated learning and differential privacy for advertising personalization[5]. Li, Wang, and Lin (2025) enhanced cross-platform ad campaigns using graph neural network-enhanced sequential recommendation methods[6].

Multimodal and generative AI applications have expanded across various domains. Zheng et al. (2025) developed FinGPT-Agent, an advanced framework for multimodal research report generation with task-adaptive optimization and hierarchical attention[7]. Chen et al. (2025) enhanced large-scale multimodal models via adaptive data synthesis and cleaning with SyntheClean[8]. Video generation capabilities were advanced by Zhang et al. (2025) through dynamic attention-guided text-to-video generation with multi-scale synthesis and LoRA optimization[11].

Dialogue systems and user modeling saw improvements through Shih et al. (2025) DST-GFN, a dual-stage transformer network with gated fusion for pairwise user preference prediction in dialogue systems[12]. Foundational data analysis techniques were explored by Chen (2023), who examined the application of data mining in data analysis[13]. Collectively, these studies highlight the extensive cross-disciplinary impact of AI technologies, spanning healthcare, finance, advertising, and human-computer interaction.

2. VALUE OF CONSTRUCTING A HOSPITAL COMPUTER COMMUNICATION NETWORK SECURITY PROTECTION SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

2.1 Ensuring the integrity of medical data

The integrity and reliability of medical data form the bedrock of the healthcare system; traditional centralized storage models carry inherent security risks—hacker attacks, human tampering, and equipment failures can lead to data corruption or loss. Blockchain technology, with its distributed storage architecture and chain-based encryption, erects an anti-tampering barrier—medical information authenticity is safeguarded, and full-lifecycle traceability is preserved. These technical features reshape the clinical pathway: physicians' diagnostic decisions draw on more accurate historical records, research institutions obtain more complete case samples, and patients' privacy rights receive tighter digital protection. In medico-legal disputes, blockchain-based treatment trajectories become irrefutable evidence, providing the judiciary with trustworthy digital proof. Continuity of medical information directly affects the tier of care quality; in cross-institution referrals, blockchain medical records eliminate information silos. The receiving physician can instantly access core data such as allergy history, imaging, and medication records, sharply reducing the time cost of formulating personalized treatment plans. Distributed ledger technology is reconstructing the medical collaboration network: mutual recognition of lab reports across hospitals becomes more efficient, data synchronization delays in tele-consultations are shortened, and regional medical resource utilization grows exponentially—signaling a new medical-informatization ecosystem that moves from data rights confirmation to value circulation.

2.2 Protecting Patient Privacy and Promoting Data Security

Medical privacy is a pivotal issue in healthcare; during the electronic storage and transmission of patient information, the risk of privacy breaches rises markedly—blockchain technology, through its encryption mechanisms and distributed storage characteristics, opens a new path to solving this problem. Medical data are encrypted and stored on the blockchain network; only users holding the corresponding private key can decrypt and access the content. Even if the transmission link is illegally intercepted, attackers cannot decipher sensitive information. Under traditional centralized storage, breaching a single server can lead to global data leakage; blockchain's distributed node architecture reduces the risk of data centralization. Medical information is dispersed across different nodes, so an attack on a local node does not endanger overall network security; this architecture simultaneously enhances data availability and attack resistance, providing multidimensional support for the privacy-protection system.

2.3 Resisting Malicious Network Attacks

Cyberattacks can lead to data breaches or tampering, and may even disrupt the normal operation of medical devices, endangering patients' lives in severe cases. The decentralized architecture and consensus mechanism of blockchain technology provide an effective means of resisting cyberattacks, because in a blockchain network any addition or modification of data must be agreed upon by a majority of nodes. This mechanism makes it difficult for attackers to tamper with data or launch attacks by controlling a single node or a small number of nodes; even if attackers successfully compromise some nodes, they cannot alter the data state of the entire network. Blockchain technology can also be combined with mechanisms such as smart contracts to enable automatic monitoring and management of network behavior. A smart contract is essentially a self-executing contract clause that automatically performs corresponding actions when specific conditions are met. In a hospital's computer communication network, smart contracts can be used to monitor network traffic, detect anomalous behavior, and promptly take measures to prevent attacks. This automated management approach enhances network security and reduces the cost and risk of human intervention.

2.4 Facilitating Real-Time Sharing of Medical Information

Sharing and collaboration of medical information is a key direction for the development of modern healthcare systems, but it has long faced numerous challenges due to data security and privacy protection concerns. The emergence of blockchain technology has opened up new possibilities for medical information sharing. On the blockchain, medical data is stored in encrypted form and can only be accessed by authorized users, ensuring data confidentiality and security and allowing medical institutions to share information with greater confidence. During medical collaboration, all participating parties can share patient medical records, test results, and other information via the blockchain network; this information is verified and tamper-proof, helping to improve the efficiency and accuracy of medical collaboration and reduce medical risks caused by inconsistent or erroneous information. Blockchain technology can also be combined with artificial intelligence to enable intelligent analysis and mining of medical information, providing more precise and personalized support for medical decision-making.

2.5 Enhancing the Security and Trustworthiness of Medical Devices

Medical devices are a critical component of a hospital's computer communication network; their security and trustworthiness directly affect patient safety and the normal operation of medical services. Traditional medical-device management approaches often harbor many security risks, such as device identity forgery and data tampering. The decentralized and tamper-proof nature of blockchain technology offers a new solution for the secure management of medical devices. For example, by storing device identity information and operational data on a blockchain, device authentication and data traceability can be achieved. When a medical device connects to the hospital's computer communication network, the system verifies the device's identity and the authenticity of its data via the blockchain, preventing security threats like identity forgery and data tampering. The transparency and openness of blockchain also make device operating status and maintenance records more traceable and controllable, thereby increasing the trustworthiness of medical devices.

3. COUNTERMEASURES FOR CONSTRUCTING A HOSPITAL COMPUTER COMMUNICATION NETWORK SECURITY PROTECTION SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

3.1 Strengthening Blockchain-Based Medical Device Security Management

The enhanced blockchain medical-device security management system focuses on optimizing security performance and trust mechanisms, covering three core areas: device identity authentication, data traceability verification, and remote monitoring and maintenance. By leveraging blockchain technology, each medical device is assigned a unique address and a digital identity certificate to ensure its identity is authentic and reliable. Operational data and maintenance records are stored intact on the blockchain, creating a verifiable data chain for subsequent fault diagnosis and maintenance support. A blockchain-based medical-device management platform is built to monitor operating status and maintenance conditions in real time; when a device failure or security risk occurs, an instant response mechanism is triggered, and the platform automatically pushes alerts to the maintenance terminal. This distributed supervision model overcomes the response-delay limitations of traditional centralized systems. Implementing this comprehensive solution systematically improves medical-device security, simultaneously reducing failure rates and security risks. Maintenance personnel can quickly verify device authorization information through the on-chain certificate verification module, while the data-tracking function records the complete parameter fluctuation curves, firmware update logs, and other key information throughout the device’s entire lifecycle.

3.2 Designing a Decentralized Network Architecture to Enhance System Attack Resistance

To build a hospital computer-communication network security protection system based on blockchain technology, the hospital must first design a decentralized network architecture. This architecture abandons the traditional centralized server model and instead distributes data and services across multiple nodes in the network. Each node undertakes the functions of data storage, processing, and transmission, jointly maintaining the security and operation of the entire network. This decentralized design means the network no longer relies on a single server or data center; even if some nodes are attacked or fail, the overall network continues to function normally. On top of this decentralized architecture, the blockchain consensus mechanism can be introduced to further enhance the system’s attack resistance. The consensus mechanism is one of the core components of a blockchain network; it ensures that all nodes share a consistent view of the data state. When new data needs to be added to the blockchain, nodes use a consensus algorithm to verify the data’s legitimacy and correctness. Only data that has been validated by a majority of nodes can be appended to the blockchain, thereby guaranteeing data immutability and reliability. This mechanism makes it difficult for attackers to tamper with data or launch attacks by controlling a small number of nodes, effectively improving network security.

3.3 Using Encryption Technology to Ensure the Security of Data Transmission and Storage

Hospitals must ensure the security of their communication systems; cryptography is a highly valuable tool for this purpose. During transmission, both symmetric and asymmetric methods can be used to encrypt data, preventing interception or tampering. Symmetric encryption uses the same key for both encryption and decryption, offering high speed and efficiency. Asymmetric cryptography employs a public–private key pair for encryption and decryption, providing greater security. For data storage, the essence of blockchain is encrypted storage: each block contains the hash of the previous block along with its own transaction data, all of which is encrypted. This approach safeguards data privacy and integrity, making unauthorized access, cracking, or modification by hackers extremely difficult. Combined with access-control technologies, it imposes stricter restrictions on data access, ensuring that only legitimate users can retrieve and utilize the data.

3.4 Establishing a Smart-Contract Mechanism to Achieve Automated Security Management

Smart contracts are another key concept in blockchain technology; they are self-executing contractual clauses that automatically perform the corresponding actions once specific conditions are met. Building on this, the hospital proposes a design for a medical information system based on smart contracts and provides a detailed analysis. For example, we can embed certain constraints or policies in the smart contract so that, under defined circumstances, it can take preventive and early-warning actions. On this basis, the hospital also introduces a new smart-contract-based medical device system that, on the one hand, performs online monitoring and alerting for users, enabling timely detection and response to potential safety hazards, and on the other hand automatically handles access control, data backup, and other security management tasks, reducing the cost and risk of human intervention. Thanks to its transparency and traceability, the system operates more fairly and is fully auditable.

3.5 Strengthen Identity Authentication to Ensure Reasonable User Permissions

In the communication system of medical devices, user authentication and permission management are critical. To address this, the hospital proposes an enhanced identity-verification mechanism to ensure that user authorizations are appropriate. It incorporates multifactor authentication, biometrics, and other methods to guarantee that only legitimate users can access and utilize online resources. For access control, the hospital employs models such as RBAC (Role-Based Access Control) or ABAC (Attribute-Based Access Control) to manage user permissions. RBAC partitions users by function and grants corresponding authorizations, while ABAC makes dynamic decisions based on user attributes such as position and department. These models can be dynamically configured and adjusted to meet the hospital’s specific needs, ensuring that user permissions remain reasonable and accurate.

3.6 Promote Blockchain-Based Medical Data Sharing Operations

The hospital must establish unified data standards and interface specifications to ensure smooth interoperability among different medical institutions. Adopting internationally recognized medical data standards such as HL7 effectively safeguards the exchangeability and readability of medical data, laying a solid foundation for cross-institutional data flow. The hospital should also fully leverage blockchain technology to protect privacy during data sharing—for example, by employing advanced techniques like zero-knowledge proofs to enable encrypted data transmission while meeting verification requirements, thereby comprehensively securing the data-sharing process and eliminating the risk of data breaches. The hospital must clearly stipulate that only authorized medical personnel may access shared medical data. For subsequent auditing and tracking, detailed logs of every data access must be recorded, preventing unauthorized access and providing strong assurance for the secure use of data.

4. CONCLUSION

Overall, blockchain technology, introduced alongside Bitcoin, has garnered widespread attention. Its core architecture is a decentralized distributed ledger that leverages cryptographic principles to ensure data immutability and traceability. In the field of hospital computer communication network security, blockchain’s unique attributes open new avenues for addressing complex issues such as data privacy protection and defense against network attacks. This study focuses on designing a hospital communication network security architecture empowered by blockchain technology, introducing blockchain to create a secure and reliable protection mechanism that safeguards the integrity of medical data and protects patient privacy. In the digital healthcare environment, distributed storage mechanisms and smart contract technologies complement each other; the blockchain structure effectively prevents unauthorized data tampering and establishes end-to-end traceability. These technical features constitute the underlying logic of medical information security protection.

REFERENCES

[1] Ding, C.; Wu, C. Self-Supervised Learning for Biomedical Signal Processing: A Systematic Review on ECG and PPG Signals. medRxiv 2024.

[2] Zhang, Yuhan. "InfraMLForge: Developer Tooling for Rapid LLM Development and Scalable Deployment." (2025).

[3] Hu, Xiao. "GenPlayAds: Procedural Playable 3D Ad Creation via Generative Model." (2025).

[4] Qin, Haoshen, et al. "Optimizing deep learning models to combat amyotrophic lateral sclerosis (ALS) disease progression." Digital health 11 (2025): 20552076251349719.

[5] Li, X., Lin, Y., & Zhang, Y. (2025). A Privacy-Preserving Framework for Advertising Personalization Incorporating Federated Learning and Differential Privacy. arXiv preprint arXiv:2507.12098.

[6] Li, X., Wang, X., & Lin, Y. (2025). Graph Neural Network Enhanced Sequential Recommendation Method for Cross-Platform Ad Campaign. arXiv preprint arXiv:2507.08959.

[7] Zheng, Haoran, et al. "FinGPT-Agent: An Advanced Framework for Multimodal Research Report Generation with Task-Adaptive Optimization and Hierarchical Attention." (2025).

[8] Chen, Yang, et al. "SyntheClean: Enhancing Large-Scale Multimodal Models via Adaptive Data Synthesis and Cleaning." 2025 5th International Conference on Artificial Intelligence and Industrial Technology Applications (AIITA). IEEE, 2025.

[9] Jiang, Gaozhe, et al. "A Knowledge-Enhanced Multi-Task Learning Model for Domain-Specific Question Answering." 2025 7th International Conference on Information Science, Electrical and Automation Engineering (ISEAE). IEEE, 2025.

[10] Zhuo, Jiayang, et al. "An Intelligent-Aware Transformer with Domain Adaptation and Contextual Reasoning for Question Answering." 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT). IEEE, 2025.

[11] Zhang, Hanlu, et al. "Dynamic Attention-Guided Video Generation from Text with Multi-Scale Synthesis and LoRA Optimization." 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT). IEEE, 2025.

[12] Shih, Kowei, et al. "DST-GFN: A Dual-Stage Transformer Network with Gated Fusion for Pairwise User Preference Prediction in Dialogue Systems." 2025 8th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE). IEEE, 2025.

[13] Chen, Rensi. "The application of data mining in data analysis." International Conference on Mathematics, Modeling, and Computer Science (MMCS2022). Vol. 12625. SPIE, 2023.

[14] Chen, Yinda, et al. "Generative text-guided 3d vision-language pretraining for unified medical image segmentation." arXiv preprint arXiv:2306.04811 (2023).

[15] Sun, N., Yu, Z., Jiang, N., & Wang, Y. (2025). Construction of Automated Machine Learning (AutoML) Framework Based on Large LanguageModels.