Library Progress International *Print version ISSN 0970 1052*
Vol.44 No.2,July-December 2024: P.180-190 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Blockchain-Based Cloud Security Management System for Hospital

Sang Young Lee

How to cite this article: Sang Young Lee (2024). Blockchain-Based Cloud Security Management System for Hospital. *Library Progress International,* 44(2), 180-190

ABSTRACT

Cloud-edge healthcare systems aim to provide low-latency services to both doctors and patients by leveraging storage and computing capabilities located on hospital servers. However, these servers often need to be more trusted and possess limited computing resources, raising concerns regarding data integrity verification. In this paper, we introduce a blockchain-based solution to tackle this challenge. Our approach involves the development of a distributed data integrity verification method that eliminates the need for a third-party auditor. Data is segmented into smaller chunks and hashed to create a hash table, from which verification tags are generated using column-based techniques and a secret string derived from a pseudo-random function. Furthermore, we present a comprehensive blockchain-based data integrity auditing system, which includes mechanisms for verifying the frequency of verification and defining the structure of blocks. Additionally, we conduct a thorough security analysis to assess the resilience of our system against common attacks. Finally, we evaluate the effectiveness of our proposed system against two leading schemes in a simulated cloud-edge healthcare environment. Our results confirm that our system can ensure data integrity without compromising efficiency.

KEYWORDS

Blockchain, Cloud, Edge, Architecture

1. INTRODUCTION

Edge Computing refers to a computing model where data processing and computing tasks are performed at data generation points or nearby network edges rather than in centralized locations such as central data centers or clouds. The reason for constructing this model is to provide faster response and processing speeds to devices or users generating data. Additionally, it helps conserve network bandwidth and contributes to enhancing the privacy and security of data. Particularly, Edge Computing offers advantages in quickly processing and analyzing large-scale data generated from devices such as Internet of Things (IoT) devices, sensors, and smartphones (Alladi & Chamola, 2020; Amato et al., 2019; Moses, Nithya, & Parameswari, 2022).

Applying edge computing in hospitals enables immediate processing of data generated from medical devices such as medical equipment, sensors, and patient monitoring devices on-site. It supports rapid analysis of hospital-related data and real-time decision-making, enhancing the efficiency and quality of medical services. Additionally, it strengthens the security and privacy of medical data, conserves network bandwidth, and reduces response times, allowing for quicker responses to patient treatments (Gupta et al., 2022; Al-Muhtadi et al., 2019; Gotwald, Musiaka, & Szymura, 2012).

When examining the specific application model of edge computing in hospital systems, patient data is processed using the same LAN-based computing resources. For example, some hospitals may have edge computers within networking equipment, while ambulances may possess all-in-one cellular edge routers with data processing capabilities in compact compartments. Embedded edge computing processors within medical devices facilitate nearly simultaneous data collection and processing, significantly reducing transmission speeds. Figure 1 shows the typical structure of edge computing (Mohammed et al., 2021; Shrimali & Patel, 2021).

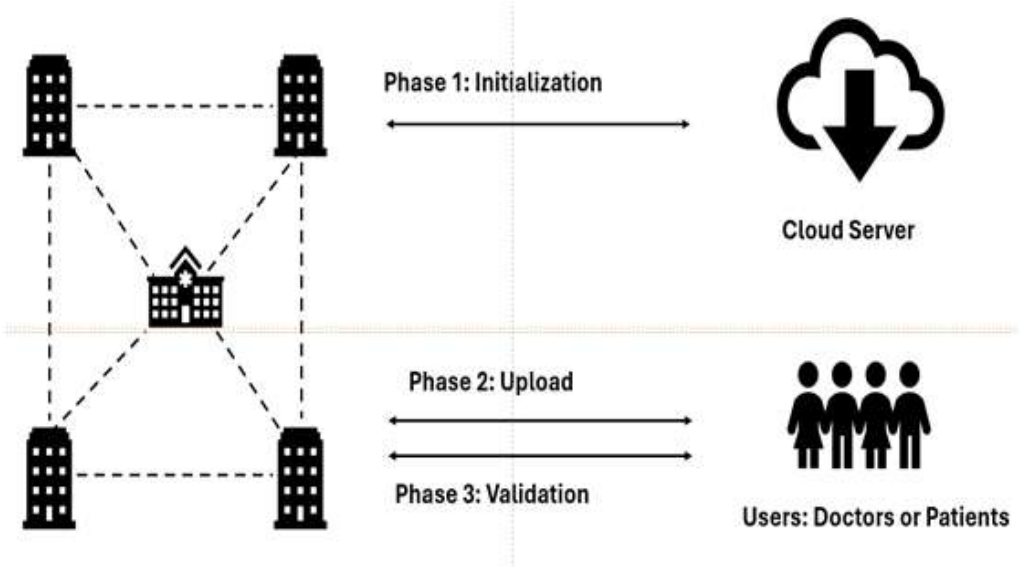

Fig. 1 Structure of edge computing

"Cleveland Clinic" is one of the cases where edge computing is applied in hospitals. The Cleveland Clinic processes large-scale data generated from medical devices on-site and analyzes it in real-time for patient monitoring and diagnosis. This allows doctors to quickly assess patient conditions and take necessary actions, improving patient treatment processes. Additionally, edge computing helps securely protect patient medical records and data, enhancing privacy protection. In summary, it contributes to improving the quality of healthcare services and ensuring patient safety (Askar, 2019; Humayun, 2021; Kumar & Sharma, 2021; Fathi et al., 2021; Mohammed & Fiaidhi, 2022; Sohal & Sharma, 2017; Kim & AlZubi, 2024).

When applying edge computing to hospitals, several potential issues may arise:

Security Concerns: Medical data is highly sensitive, and strict requirements for personal information protection apply. Additional security measures are necessary to ensure data security and privacy in edge computing environments.

Data Integration and Compatibility: Various medical systems and devices within hospitals may use different formats and protocols. This can lead to issues with data integration and compatibility, necessitating standardized approaches to resolve them.

Network and Connectivity Issues: Edge computing involves processing data on-site, making reliable network connections essential. Network problems or connectivity instability can impact data processing and the delivery of medical services.

Resource Limitations: Hospital environments may have limitations on computing and storage space, power, and bandwidth. When implementing edge computing systems, these resource constraints must be taken into account and addressed accordingly.

These challenges need to be carefully considered and addressed to ensure the successful implementation of edge computing in hospitals. To address these issues, the application of appropriate cutting-edge technology is necessary. Additionally, establishing proper security and data management policies is essential to build a secure and efficient edge computing environment.

In general, there is a significant demand for healthcare systems in society. When data needs to be shared among various medical institutions, edge computing becomes a crucial architecture for resolution. Blockchain technology can be utilized as a means to support anti-counterfeiting and tamper-proofing (Kim & AlZubi, 2024).

Different hospitals collaborate and share medical data for better healthcare and diagnostic services. Cloud computing architecture can act as a convenient solution. Users from various hospitals, such as doctors

and patients, can directly upload data to central cloud servers to share medical data. However, the centralized cloud computing model has issues such as single points of failure and delays between some users and cloud servers. For these reasons, cloud-based architectures are preferred. While hospital servers operate as edge servers, users store data directly on the nearest hospital server (Thomasian & Adashi, 2021; Muheidat & Tawalbeh, 2023).

The blockchain technology applied here helps overcome problems that may arise in hospital systems.

Enhanced Security: Blockchain operates with a distributed database structure, linking changes to previous blocks when data is altered. This helps prevent data forgery or alteration and ensures data integrity.

Data Sharing and Transparency: Blockchain provides a distributed ledger that allows transparent sharing and tracking of data. This facilitates easy data sharing with other hospitals or medical institutions and enables transparent management of patient medical records.

Regulatory Compliance Using Smart Contracts: Blockchain can provide automated regulatory compliance using programmable conditions called smart contracts. This allows management of access rights to medical records and ensures secure data sharing.

Distributed Data Storage: Blockchain distributes data across multiple nodes, removing single points of failure and enhancing the availability and durability of data.

Furthermore, blockchain technology addresses the crucial issue of ensuring data integrity in environments with unreliable and limited computing resources, such as medical hospital servers.

Firstly, it involves distributed data integrity verification. Blockchain technology employs distributed methods for data integrity, eliminating the need for third-party auditors. It partitions data into smaller segments and hashes them to construct hash tables, facilitating efficient verification. Secondly, it involves integrity verification tag construction. Verification tags are composed based on secret strings generated by the columns of hash tables and pseudo-random functions. This ensures the safe verification of data integrity. Thirdly, it involves establishing an audit framework based on blockchain. By utilizing blockchain technology, data integrity audits are further strengthened. It integrates features such as proof of audit frequency and defining appropriate block structures to provide a robust audit framework. Fourthly, it enables thorough security analysis. Rigorous security analysis against external attacks is feasible, ensuring the protection of medical data integrity against potential threats.

This proposed structure addresses urgent issues of data integrity in cloud-edge healthcare systems by leveraging distributed verification methods and blockchain technology. These security features and efficiency become a promising solution for ensuring the integrity of sensitive medical data.

Related Works

So far, research related to the use of cloud-edge computing and blockchain in the medical field includes the following topics (Zaraket et al., 2021; Shitharth et al., 2021):

- Security and Privacy of Cloud-Edge Healthcare Systems: Security and privacy of medical data are critical issues. Research is being conducted on technical solutions and policies to enhance data security and privacy in cloud-edge healthcare systems.
- Secure Sharing and Access Mechanisms for Medical Data Using Blockchain: Blockchain technology can provide a distributed ledger for secure sharing and access of data. Research is underway on methods for securely sharing and accessing patients' medical records in the healthcare domain.

However, there currently needs to be direct research on cloud-edge computing medical system data auditing. Therefore, this study focuses on related research on cloud computing data auditing and cloud-edge computing data auditing. The limitations of edge computing and blockchain technology to date are evident in several aspects. Firstly, there is the issue of scalability. Edge computing and blockchain technologies still have scalability issues for large-scale data and transaction processing. Especially in the medical field, where numerous data and transactions can occur, solutions are needed to handle them

efficiently. Secondly, there are performance issues. Edge computing and blockchain require additional computational and network resources. This can lead to performance degradation and impact real-time processing and response times. Thirdly, there are security and privacy concerns. While blockchain provides data integrity and security, it may lack considerations for privacy. Medical data is particularly sensitive, and measures are needed to protect it appropriately. Fourthly, there are legal and regulatory aspects. The medical field has very strict legal regulations and compliance requirements. When applying edge computing and blockchain, it is crucial to comply with these regulations and requirements. However, currently, there is a lack of standardized guidelines in this area (Peterson et al., 2016; Bao et al., 2021; Besher et al., 2020; Bi et al., 2021).

Cloud-Edge Medical Systems

Cloud-edge medical systems present new challenges for data security. Generally, users trust hospital servers more than they trust cloud servers. Different hospital servers belong to various institutions and do not trust each other. Provable Data Possession (PDP) and Proof of Retrievability (POR) are existing data integrity verification methods in cloud computing. However, existing data integrity verification methods are not suitable for cloud-edge medical systems for two reasons (Kyun & Jang, 2021; Wu & Kim 2022a).

Third-Party Auditors (TPAs) for auditing are not suitable for the distributed nature of cloud-edge medical systems. Secondly, hospital servers have limited computing resources. Therefore, data integrity must be verified within the cloud-edge medical system. Blockchain can offer a potential direction for data integrity auditing in cloud-edge medical systems. Each hospital server can become a blockchain node to participate in consensus and maintain a distributed ledger for data integrity auditing.

Cloud-edge computing is a crucial architecture for data-sharing medical systems, and blockchain is a technology that supports anti-counterfeiting and anti-collusion. However, there are still unresolved issues, such as pending solutions for building a distributed architecture among hospital servers, ensuring the efficiency of distributed data integrity verification, and defending against threats from malicious hospital servers. Therefore, an efficient data integrity auditing scheme based on blockchain is proposed (Wu & Kim 2022b; Fathi et al., 2021).

Looking at cloud computing data auditing, we start with Proofs of Retrievability (POR), the first data auditing mechanism proposed in 2007. This scheme ensures secure data storage by allowing users to verify the integrity of outsourced data. However, it lacks the ability for public auditing. Provable Data Possession (PDP) reduces user costs by employing a third-party auditor to verify data integrity on behalf of the user. In practical applications, the demand for dynamic operations is more common. Scalable PDP schemes support only some dynamic operations.

To improve upon these POR models, homomorphic authentication techniques have been developed to reduce communication overhead for dynamic operations. Examples include the rank-based authentication skip table method and the first data integrity auditing scheme supporting full dynamic updates. Additionally, there are novel data dynamic update integrity verification schemes based on the Merkel Hash Tree (MHT). These methods support public auditing and reduce some overhead but are not resistant to replacement attacks. To address replacement attacks, the position-aware Merkle Tree (PMT) method was developed. This method improves upon MHT by including location information in each node.

In cloud-edge computing data auditing, establishing collaborative models is crucial. One study proposes an integrity scheme for app providers' cached data within the edge computing environment. This scheme categorizes threats into unexpected failures and malicious attacks. It introduces a lightweight sampling-based probabilistic approach with a novel data structure called Variable Merkle Hash Tree, focusing on accuracy, efficiency, and security. Additionally, it suggests a collaborative system that utilizes distributed consensus to form an edge caching system, where all edge servers share the responsibility of ensuring data integrity, emphasizing privacy and efficiency. The study aims to achieve meaningful results by addressing the edge data integrity concerns of application providers (Sohal & Sharma, 2017).

However, the scenarios mentioned above primarily focus on the data integrity verification needs of single application providers. In reality, each edge server is responsible for storing data from multiple

application providers. Additionally, application provider servers possess greater computing power and storage space compared to individual user servers and edge servers. Consequently, these methods are not suitable for diverse edge servers providing individual services. To address this challenge, a blockchain-based framework without a Third-Party Auditor (TPA) has been proposed. This framework incorporates Merkle tree-based verification methods and sampling strategies. Although a prototype has been implemented by deploying smart contracts on Ethereum, it may be suitable for something other than resource-constrained edge servers.

Furthermore, a consensus-based blockchain data integrity framework has been suggested, dividing the framework into private and edge sections. The private section maintains a private chain for IoT devices, while the edge section consists of a public chain formed by edge servers. The verification methods for these sections are based on the Merkle tree structure. Blockchain-based data integrity verification frameworks often adopt similar approaches based on Merkle trees and sampling. While they may not guarantee a 100% success rate for verification, new schemes are proposed to improve success rates. Consequently, this paper focuses on designing a blockchain-based distributed data auditing scheme specifically for medical systems.

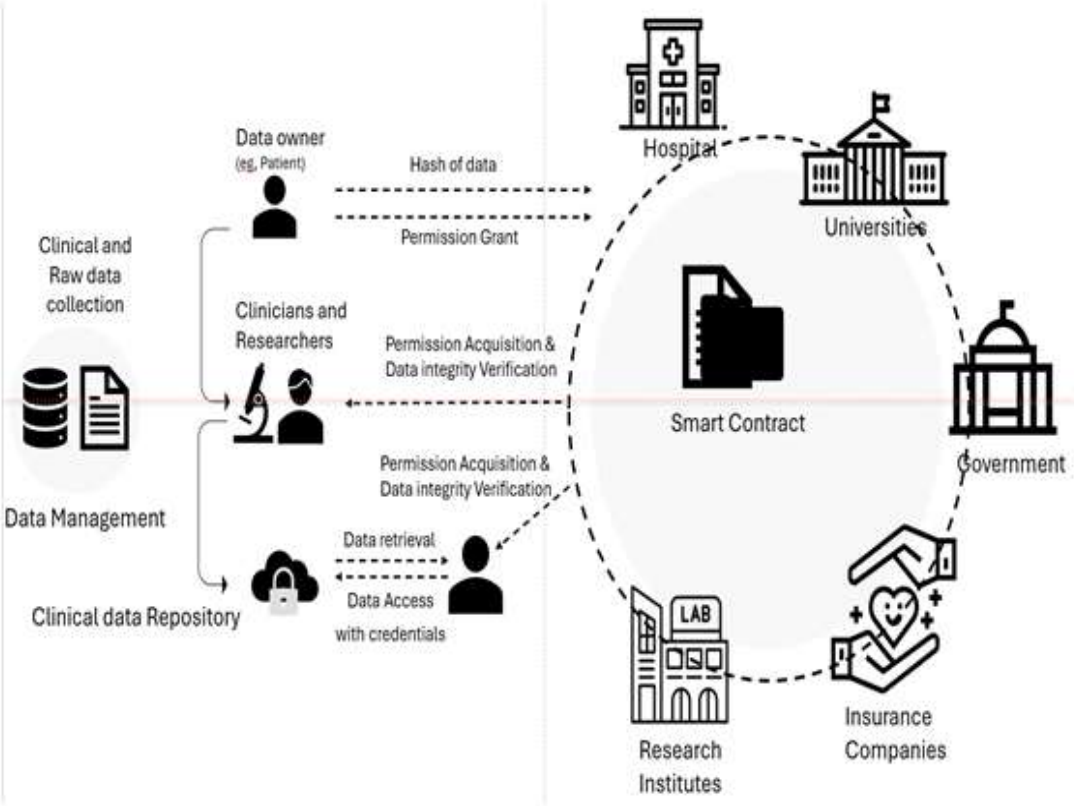

Fig. 2 Blockchain-based model for permission-based access control operation

4. BLOCKCHAIN-BASED DISTRIBUTED DATA AUDITING SCHEME

The proposed system framework involves three distinct roles: users, hospital servers, and the cloud server. Users, such as doctors and patients, typically upload their data to the nearest hospital server and request data integrity verification services. Hospital servers, considered untrusted, are responsible for storing user data, performing data integrity verification processes, and participating in the blockchain consensus mechanism. These servers may act maliciously and attempt to hide any data loss. The cloud server plays a more limited role, responsible only for setting initial system parameters and generating blocks.

This architecture not only eliminates the need for a trusted third party but also leverages the tamper-proof and collusion-resistant properties of blockchain technology. The notations used in this paper are summarized in Table 1. The proposed scheme comprises the following three phases:

Table 1. Notations

Symbols	Meaning
$F = \{f_1, f_2, \ldots, f_i, \ldots, f_N\}$	The data file with m data blocks
N	The order of cyclic group
g	Generator of cyclic group
$H_1()$ and $H_2()$	Two hash functions
$PRF(k)$	The pseudo random function with key k
β_1 and β_2	The length of the digest of the two hash functions
VT	The matrix of verification message
S	The secret string

Phase 1: System Initialization

Key Generation and Distribution: Both hospital servers and the cloud server generate their respective public and private key pairs. They then hash their public keys to obtain their addresses and broadcast both the public keys and addresses to all other servers in the network. Genesis Block Creation: Upon receiving the public keys of all hospital servers, the cloud server assigns an order to each hospital server and creates the first block of the blockchain, known as the genesis block. The genesis block includes a timestamp, the order of edge servers, their addresses, and their public keys. Genesis Block Distribution: The cloud server then transmits the genesis block to all hospital servers, marking the initiation of the blockchain.

Phase 2: Data Upload and Verification Information Submission

User Key Generation and Hashing: Users, such as doctors or patients, begin by generating their own public and private key pairs. Similar to servers, they hash their public key to derive their address. Verification Information Generation: Users then process and generate verification information for the data they intend to upload. Data Upload and Verification Information Submission: Users upload their data to the nearest hospital server and simultaneously submit the corresponding verification information to the blockchain network. Consensus and Storage: Following a consensus process among the hospital servers, the verification information is stored on the blockchain, and accessible to all edge servers.

Phase 3: Data Integrity Verification

User Request: Users initiate a request for data integrity verification services. Distributed Verification: Hospital servers collaboratively verify the integrity of the user's data using the verification information stored on the blockchain. Consensus and Result Delivery: After reaching a consensus on the verification outcome, the hospital servers send the data integrity verification result back to the user.

The distributed data integrity verification method encompasses the following key steps: tag generation, verification, and tag updating.

-Tag Construction

Considering the resource constraints of edge servers and the blockchain, we construct verification tags for data using hash functions and pseudo-random functions. Data Segmentation: The data is initially divided into N data blocks, denoted as F = {f1, f2, ..., fi, ..., fm}. Verification Tag Matrix Construction: A V_T matrix of size (β1 × β2) is then constructed. The algorithm for this process is as follows:

Table 2. Algorithm 1

1: Input: $F = \{f_1, f_2, \cdots, f_i, \cdots, f_m\}$, g, N, β_1, β_2 , $H_1()$, $H_2()$, $PRF()$, k
2: Output: VT
3: $S = PRF(k)$
4: Initial $hashT\ able$ as a binary matrix with a size of $m \times \beta_1$
5: **for** $i = 1$ to m **do**
6: Set the ith row of $hashTable$ as $H_1(g^{s_i + f_i} mod\ N)$
7: Initial VT as a binary matrix with a size of $\beta_1 \times \beta_2$, elements 0
8: **for** $i = 1\ to\ \beta_1$ **do**
9: Set the $temp$ as the ith column of$hashTable$
10: Set the ith row of VT as $H_2(temp)$
11: **Return** $\boldsymbol{VT}$

-Verification

Once the tags have been generated, the verification process can be carried out in a distributed manner by other hospital servers. The detailed steps of this process are outlined in Algorithm 2.

n lines 3 to 4 of Algorithm 2, the hospital server computes a secret string and reconstructs the hash table (hash Table') using the currently stored data file. From lines 5 to 12, the verifier checks the data based on hash Table' and V_T.

The process involves:

- Determining Sampling Times: The number of times sampling will occur is determined.

- Requesting and Comparing Hash Values: A random column (rand) from hashTable' is requested, and its hash value is compared with the corresponding rand row of V_T.

- Verification Result: If all t samplings pass the verification, the algorithm returns "true," indicating data integrity. Otherwise, it returns "false," suggesting potential data corruption or manipulation.

Algorithm 2 can be executed in a distributed and parallel manner across different hospital servers, enhancing efficiency and scalability.

Table 2. Algorithm 2

1: Input: VT, N, m, H_2, β_1, β_2 , $PRF()$, k
2: Output: True of False
3: The hospital server calculates the $S = PRF(k)$
4: The hospital server reconstruct the $hashT\ able'$
5: The validator (other hospital server) decries the times for sampling t
6: **for** $i = 1$ to t **do**
7: The validator generates a random number $(rand)$ from $[1, \beta_1]$
8: The validator requests the ith column of $hashT\ able'$
9: The validator calculates $H_2(hashT\ able'_{r\ and})$and compares with the VT
10: **if** $H_2(hashT\ able'_{r\ and}) \neq VT_{r\ and}$ **do**
11: **Return** False
12: **Return** *True*

-Tag Updating

After the verification process, the hospital servers become aware of the secret string held by the user. Consequently, the previous V_T becomes invalid, and the user needs to update the verification tag. Due to communication overhead concerns, sending the entire file back to the user is impractical.

Building upon the proposed distributed verification method, the detailed blockchain design for cloud-edge computing encompasses the following four phases: setup, consensus, upload, and verification.

5. EVALUATION

The proposed data integrity auditing system for cloud-edge healthcare systems is highly significant. It addresses the critical need to ensure data integrity in environments like medical hospital servers, which are untrusted and have limited computing resources, using blockchain technology. In cases where data needs to be shared across multiple medical institutions, cloud-edge computing architectures will become increasingly important. Based on this premise, blockchain can be utilized as a technology supporting forgery prevention and tamper resistance. Various hospitals have a tendency to collaborate and share medical data for better healthcare and diagnostic services. Cloud computing architecture can serve as a straightforward solution. Users from various hospitals, such as doctors and patients, can directly upload data to central cloud servers to share medical data. However, the centralized cloud computing model faces issues such as single points of failure and high latency between some users and cloud servers. For these reasons, cloud-edge healthcare systems are preferred. While hospital servers operate as edge servers, users directly store data on the nearest hospital server, as depicted in Figure 3.

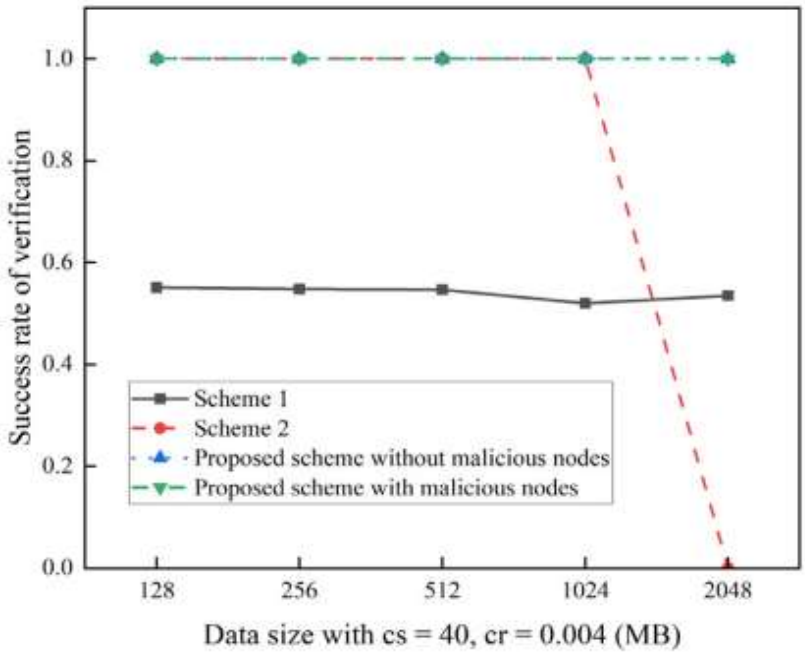

Fig. 3 Verification Success Rate Results

As depicted in the figure, the success verification rates of the three methods do not vary as the data size increases. This is because the detection rates remain the same due to similar tampering sizes and rates. The verification success rate of Method 1 is slightly higher due to 200 samplings. Additionally, both Method 2 and the proposed method achieve a 100% success rate. The presence of malicious nodes does not have a negative impact. For data sizes not exceeding 1024 MB, hash operations on the entire data file ensure a 100% success rate for Method 2. However, for hash operations on a 2 GB file, memory errors occur due to the limited memory of the experimental virtual machine and some memory occupied by the Ubuntu system.

Overall, the tampering size does not significantly affect the success rate for all methods. This is due to the one-wayness and collision-resistant properties of hash functions. In the case of Method 1, as the tampering rate increases, the verification success rate also increases. Higher tampering rates make it easier to sample tampered data blocks. For Method 2, the success rate is 100% due to direct comparison of hash values of data files. For the proposed method, the success rate is nearly 100% when the

tampering rate is 0.001. However, due to malicious nodes attempting to conceal data loss or modification, the success rate of the proposed method could be higher in the presence of malicious nodes. Nevertheless, the rate remains above 90%..

This paper presents a mechanism for facilitating user-to-user access using blockchain technology. The proposed design aims to enable secure data sharing through an extensible and lightweight blockchain while ensuring privacy protection. The approach involves comparing shared data pools and blockchain networks to achieve these goals. Specifically, the paper applies the Semantic Data Transformation and Classification (SDTC) technique to analyze the meaning of significant data generated by a company's legacy system.

5. CONCLUSIONS

Cloud-edge healthcare systems provide low latency to doctors and patients by offering storage and computing capabilities on hospital servers. However, hospital servers are untrusted and have limited computing resources. Data integrity verification in cloud-edge healthcare systems is an urgent issue.

In this paper, we propose a blockchain-based data integrity auditing system to address this issue. Firstly, we design a distributed data integrity verification method without the need for a third-party auditor. Data is divided into smaller chunks and hashed to form a hash table. Verification tags are generated based on the columns of the hash table and a secret string generated by a pseudo-random function. Then, we propose a detailed blockchain-based data integrity auditing system including proofs of verification frequency and block structure. Additionally, we provide security analysis against common attacks. Finally, we evaluate the proposed system against two state-of-the-art schemes in a simulated cloud-edge healthcare system. The results demonstrate that the proposed system can verify data integrity without sacrificing efficiency.

Furthermore, we propose a blockchain-based schema for data integrity auditing in cloud-edge healthcare systems without a third-party auditor. Firstly, we design a distributed data integrity verification method. Verification tags, composed of hash tables of data files and secret strings, ensure a verification rate close to 100%. This paper proposes a mechanism for mediating user-to-user access based on blockchain. We propose a design that allows data sharing in a secure way with extensible (redesigned to allow fast transactions) and lightweight blockchain and protects privacy by comparing it to shared data pools and blockchain networks. In this paper, the SDTC technique that may be processed on a semantic basis was applied to analyze the meaning of important data of a company produced through a legacy system.

6. ACKNOWLEDGEMENTS

Funding for this paper was provided by Namseoul University

Funding Details

This research received no external funding.

Authors' contributions

All authors contributed toward data analysis, drafting and revising the paper and agreed to be responsible for all the aspects of this work.

Declaration of Conflicts of Interests

Authors declare that they have no conflict of interest.

Availability of data and materials

Not Applicable

Use of Artificial Intelligence

Not applicable

Declarations

Authors declare that all works are original and this manuscript has not been published in any other journal.

References

Alladi, T., & Chamola, V. (2020). HARCI: A two-way authentication protocol for three entity healthcare IoT networks*. IEEE Journal on Selected Areas in Communications*, 39(2), 361–369.

Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W., & Orgun, M. A. (2019). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. *Health Informatics Journal*, 25(2), 315–329.

Amato, F., Casola, V., Cozzolino, G., De Benedictis, A., & Moscato, F. (2019). Exploiting workflow languages and semantics for validation of security policies in IoT composite services. *IEEE Internet of Things Journal,* 7(5), 4655–4665.

Askar, A. J. (2019). Healthcare management system and cybersecurity. *International Journal of Recent Technology and Engineering*, 237–248.

Bao, Y., Qiu, W., & Cheng, X. (2021). Secure and lightweight fine-grained searchable data sharing for IoT-oriented and cloud-assisted smart healthcare system. *IEEE Internet of Things Journal*, 9(4), 2513–2526.

Besher, K. M., Subah, Z., & Ali, M. Z. (2020). IoT sensor-initiated healthcare data security. *IEEE Sensors Journal*, 21(10), 11977–11982.

Bi, H., Liu, J., & Kato, N. (2021). Deep learning-based privacy preservation and data analytics for IoT-enabled healthcare. *IEEE Transactions on Industrial Informatics*, 18(7), 4798–4807.

Fathi Islam S., Ahmed Mohamed Ali, Makhlouf, M. A., & Osman, E. A. (2021). Compression techniques of biomedical signals in remote healthcare monitoring systems: A comparative study. *International Journal of Hybrid Information Technologies*, 1(1), 33-50. https://doi.org/10.21742/IJHIT.2021.1.1.03

Gotwald, B., Musiaka, L. & Szymura. K. (2012). Tourism in strategic documents of local self- government bodies of the Łódź voivodeship and Norwegian good practices in tourism management. *Acta Innovations*, 5, 25–50. https://www.actainnovations.com/index.php/pub/article/view/5_4

Gupta, L., et al. (2022). Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach. Applied Soft Computing, 118, 108439.

Humayun, M. (2021). Industry 4.0 and cyber security issues and challenges. *Turkish Journal of Computer and Mathematics Education* (TURCOMAT, 12, 2957–2971.

Kim, S.Y. & AlZubi, A.A. (2024). Blockchain and Artificial Intelligence for Ensuring the Authenticity of Organic Legume Products in Supply Chains. *Legume Research*, 47(7), 1144- 1150. https://doi.org/10.18805/LRF-786

Kumar, R., & Sharma, R. (2021). Leveraging blockchain for ensuring trust in IoT: A survey. *Journal of King Saud University - Computer and Information Sciences*, 34(9), 8599–8622.

Mohammed, M. A., Ibrahim, D. A., & Abdulkareem, K. H. (2021). Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoMT environment*. Journal of King Saud University - Computer and Information Sciences*, 35(1), 1–12.

Mohammed, S., & Fiaidhi, J. (2022). Extending the power of problem-oriented medical record with disease association discovery: The case study of empowering QL4POMR with OpenTargets. *International Journal of Hybrid Information Technology*, 2(1), 1-12. https://doi.org/10.21742/IJHIT.2022.2.1.01

Moses, M. B., Nithya, S. E., Parameswari, M. (2022). Internet of Things and Geographical Information System based Monitoring and Mapping of Real Time Water Quality System. *International Journal of Environmental Sciences*, 8(1), 27-36,

Muheidat, F., & Tawalbeh, L. A. (2023). AIoMT artificial intelligence (AI) and Internet of Medical Things (IoMT): applications, challenges, and future trends. In *Computational Intelligence for Medical Internet of Things (MIoT) Applications* (pp. 33-54). Academic Press.

Peterson, K., Deeduvanu, R., Kanjamala, P., & Boles, K. (2016). A blockchain-based approach to health information exchange networks. In Proceedings of the 2016 *IEEE International Conference on Big Data (Big Data*) (pp. 1–10).

Shitharth, S., Satheesh, N., Kumar, B. P., & Sangeetha, K. (2021). IDS detection based on optimization based on WI-CS and GNN algorithm in SCADA network. In Architectural Wireless Networks Solutions and Security Issues (pp. 247–265).

Shrimali, B., & Patel, H. B. (2021). Blockchain state-of-the-art: Architecture, use cases, consensus, challenges, and opportunities. *Journal of King Saud University - Computer and Information Sciences*, 34(9), 6793–6807.

Sohal, M., & Sharma, S. (2017). Enhancement of cloud security using DNA-inspired multifold cryptographic technique. *International Journal of Security and Its Applications*, 11(12), 15-26.

Suna Kyun, Jaekyung Yi, & Jiyoung Jang. (2021). A decentralized approach to education powered by blockchain technology. *Asia-Pacific Journal of Convergent Research Interchange*, 7(7), 131-141. https://doi.org/10.47116/apjcri.2021.07.13

Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the internet of medical things. *Health Policy and Technology*, 10, 100549.

Wu, Y. F., & Kim, H. H. (2022a). Research on the application of blockchain technology in the comprehensive health industry. *Asia-Pacific Journal of Convergent Research Interchange*, 8(3), 15-26. https://doi.org/10.47116/apjcri.2022.03.02

Wu, Y. F., & Kim, H. H. (2022b). Vocational education system architecture based on blockchain technology. *Asia-Pacific Journal of Convergent Research Interchange*, 8(6), 1-12. https://doi.org/10.47116/apjcri.2022.06.01

Zaraket, C., Hariss, K., Chamoun, M., & Nicolas, T. (2021). Cloud-based private data analytic using secure computation over encrypted data. *Journal of King Saud University - Computer and Information Sciences*, 34(9), 4931–4942.