Global Journal of Medical Terminology Research and Informatics, Vol. 3, No, 1, 2025
ISSN-3107-5282

Securing Multi-Modal Medical Data Management System using Blockchain and the Internet of Medical Things

Dr. Alessandra Moretti[1], and Hiroshi Tanaka[2]

[1] *Institute of Medical Informatics, Kyoto University, Japan.*

[2] *Professor, Institute of Medical Informatics, Kyoto University, Japan*.

Received: 23/October/2024; Revised: 20/November/2024; Accepted: 25/December/2024; Published: 30/January/2025

Abstract

The Internet of Medical Things (IoMT) refers to a network of interconnected smart medical devices, apps, medical systems, and institutions. The smart medical gadgets and apps are interconnected over the Internet with healthcare frameworks. Confidentiality and safety of patient information, scalability, and information availability are the most intricate difficulties of IoT, especially within the Internet of Medical Things (IoMT), and must be addressed. Blockchain (BC) can potentially transform existing methods of information admission, interchange, gathering, regulator, and involvement. This study presents a Secured Multi-Modal Medical Data Management System (SMMDM) using BC and the IoMT. The proposed SMMDM ensures safe data management among individual servers and sensor-based therapeutic devices, as well as among cloud and individual servers. The IoMT-based safety architecture employs BC to provide secure data transfer and management across interconnected nodes. The BC key has been employed in a healthcare application network, enabling the safe generation of alerts from patient health data for verified healthcare practitioners.

Keywords: Internet of Medical Things, Blockchain, Data Management, Multi-Modal Medical Data, Cloud servers, Security.

1 INTRODUCTION AND RELATED WORKS ON IOMT, DATA MANAGEMENT, AND BC

The primary objective of medical care is to improve the living standards via health promotion and assistance (Girardi et al., 2020). Treatment for patients includes illness prevention, rehabilitation, administration, and medical personnel safeguarding mental and physical well-being. Medical Data Management (MDM) at a healthcare facility entails establishing a functional data framework as the foundation for cohesive management and data accessibility across the organization. An extensive MDM approach is becoming vital as firms depend on intangible assets to create value (Arul et al., 2021). It necessitates collecting, inputting, encoding, analysis, results, recovery, and data storage from many healthcare domains.

The IoMT category comprises intelligent devices, including sensors and medical/vital monitoring systems, specifically designed for application in the healthcare sector, whether at home, in community settings, or inside hospitals and medical centers, and facilitates real-time applications in telemedicine and additional services (Ding et al., 2023). Wi-Fi-enabled medical equipment offers connection among

machines within the IoMT. The IoT enables sensors to collect essential data and transmit it to clinicians for real-time patient monitoring. Mobile applications and connected devices may notify doctors and nurses to mitigate security hazards and crucial issues (Su et al., 2024).

The IoMT facilitates the dependable processing of information, enhances workflow efficiency, minimizes waste, and mitigates the likelihood of errors. The IoMT enables real-time medical treatment, substantially reducing the need for physicians' physical presence. In IoMT MDM, data confidentiality regulations necessitate communication barriers due to atypical physical settings and the increasing potential for security violations, among other factors, which must be addressed; BC technology has been employed in sensitive situations (Khan & AbaOud, 2023).

Numerous medical institutions lack reliable or robust networks to support IoMT devices effectively. The vast volume of data transferred might hinder clinicians' ability to access information about patients when required, leading to inefficiencies (Zhang et al., 2023). BC enables patients to establish regulations to access their medical data, allowing particular academics to access certain sections of their medical history for a predetermined duration (Muhammad et al., 2021). Patients may link to other hospitals using BC technology and effortlessly record their medical information. Intelligent agreements (IA) are employed to guarantee the confidentiality and safety of the BC. A BC is primarily a digital ledger of transactions copied and reproduced over the entire network of the BC's computer system (Taloba et al., 2023).

This work proficiently delineated an application-centric structure for big data networks based on the research of extant big data systems tailored to unique applications. The study indicates many issues within the healthcare sector regarding medical data transmission and access. This study proposes that the SMMDM address these issues, facilitating the secure exchange of multi-modal data using Internet-based healthcare information. The IoMT-based safety platform employs BC technology to facilitate data flow and administration across interconnected nodes.

2 PROPOSED SMMDM FRAMEWORK

IoMT devices can offer real-time sensor information from patients for interpretation in MDM. The safety and privacy of health-related data transmission is a significant concern for IoMT devices across several product domains. This article proposed using BC in the IoMT to construct an SMMDM. The proposed solution effectively meets the optimum confidentiality and safety criteria for IoMT-MDM. The BC key has been utilized in an application in the medical network that enables the secure generation of notifications about medical information for verified healthcare practitioners.

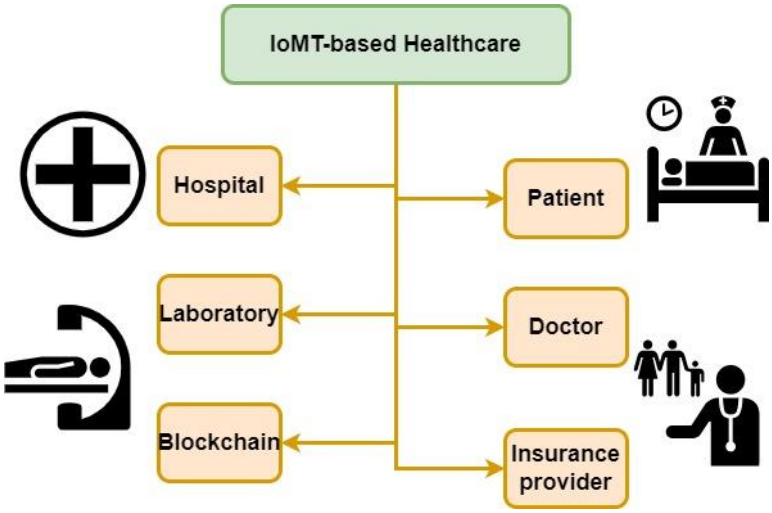

Figure 1: IoMT-based Healthcare System

The computer-based, digital medical system, IoMT, is shown in Figure 1. This paper advocates for integrating IoMT, BC, and Cloud platforms into healthcare and MDM systems. The vital patient statistics are monitored securely in intelligent and remote healthcare facilities. BC architecture enables secure data exchange. Figure 1 presents many uses of BC technology in medical care. JavaScript and HTML have been employed to enhance the user interface on the Internet. The IoMT processes individualized services for patients on a BC framework. Only authorized administrators of computers may manage the IoT devices linked to the sensor-based healthcare component.

BC is a novel framework for digitizing healthcare records, whereby managing recorded and decentralized data security poses significant challenges. The IoMT comprises devices connected to the Internet that provide health-related services. Ensuring the security of health-related findings is essential since medical research entails collecting, storing, and using extensive amounts of individual medical data, which may be sensitive and embarrassing. Information from diverse sources, comprising medical records, patient queries, and administrative files used for billing or management purposes, may be acquired according to the standards. Information safety refers to the protective measures used throughout the information lifecycle to prevent unwanted access and corruption.

Security measures include information encryption, hacker prevention, and key management methods that offer data safety across all applications and environments. It constitutes an interconnected healthcare system framework, including software programs and medical equipment. Cooperation among devices and sensors enables healthcare facilities, often situated in distant areas, to enhance efficiency in handling workflows and medical procedures. The IoMT merges the digital and physical realms to improve diagnostic and treatment processes, improving patient health and facilitating immediate health changes. Medical encounters may profoundly impact both patients and professionals.

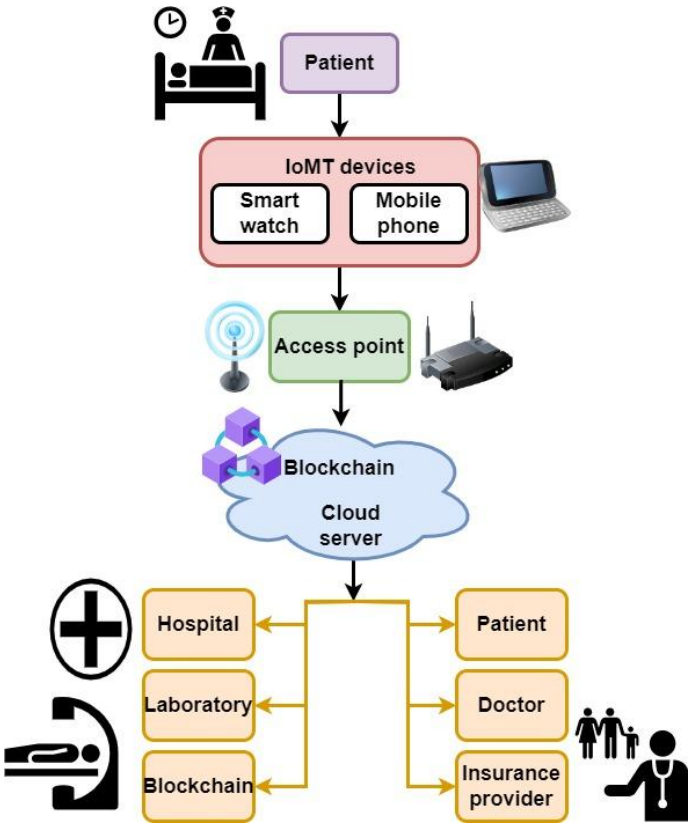

Figure 2: Secured Multi-Modal Medical Data Management System using BC and IoMT

Figure 2 illustrates the suggested SMMDM methodology using BC and IoMT. This article proposed a system for safeguarding observed patient health information via a BC paradigm to ensure data security. Encryption is a very beneficial data security strategy for medical establishments. Encrypting information both in transit and at rest complicates the decryption of medical data for health providers and commercial partners, even with granted access. The regulation mandates that medical professionals and personnel determine the necessary techniques for encryption and other security measures based on the organization's workflow and other requirements, therefore without expressly obligating medical facilities to use encrypted data protocols. A decentralized BC-based approach encounters certain challenges associated with the centralized cloud technique.

A BC-based data structure is a securely linked, virtually immutable block that stores essential patient-based information. One method to limit admission to information is via encryption. While information encryption is not technically mandated by the security legislation governing cryptography, it must be implemented if a risk assessment is deemed a prudent and adequate protective measure. If encryption is insufficient or required, a solution must still be identified to accomplish the same objective. Initially, it may be quite vexing since it represents a superior method of preserving information. If hackers lack the decryption key, they cannot access the stolen information. It is important to ensure the secure maintenance of health information. Records must be maintained at all times for public scrutiny and access. Only authorized personnel are permitted to report their

information. Health record data must not be disclosed without the patient's permission unless permitted by law.

Patients must safeguard their confidentiality and integrity with pharmacists and healthcare providers. Alternatively, the sufferer is unable to seek counsel or disseminate their insights. Violating an individual's privacy would undermine the patient's trust in any physician and adversely affect the relationship and assurance. Each person is entitled to respect and consideration, particularly with mutual decision-making and independence for patients. Empathy, investment of time with patients, active listening and guidance, and problem-solving may foster a reliable and respected connection. BC technology consists of interconnected computers and all participants. Physicians have been visually represented in distant places, and they observe and communicate with patients using the BC framework. The physician examines the diagnosis unit reports. Medical experts at the diagnosis center provide online health records (OHRs), which are later applied to patients' histories. In some healthcare facilities, immediate statistical information is sent and analyzed on the distributed database.

The physician employs many wearable gadgets to monitor the patient. Smartwatches and phones can monitor patient body alterations and transmit this information to the physician in real time. The physician thereafter advises the patient appropriately. Caregivers may access patients' medical histories. Medical data and therapies are sent to each patient's networking node and accessed on the distributed database. Patients hospitalized in healthcare institutions may get treatment from many doctors, nurses, or other medical professionals. All practitioners document patient maintenance information to guarantee optimal outcomes are consistently managed. The prominent use of healthcare records is likely these papers. Healthcare organizations may ascertain their strengths and weaknesses via client satisfaction inquiries, complaints, and additional information sources. When patients provide data, like pain stages and employment status, medical organizations may ascertain which procedures are most effective. Collecting health data enables healthcare institutions to develop comprehensive patient profiles, tailor care, progress treatment, strengthen physician-patient relationships, and boost health outcomes. Healthcare practitioners monitor wearable gadgets. These gadgets have sensors that continuously monitor the patient and transmit valuable healthcare data to healthcare experts via the IoMT.

3 RESULTS AND DISCUSSION

The experimental findings of the proposed SMMDM approach were conducted using samples acquired from healthcare institutes. In this simulated scenario, 50 samples were collected for analysis; moreover, the information processing was evaluated for 2.5 seconds with variations in reaction periods.

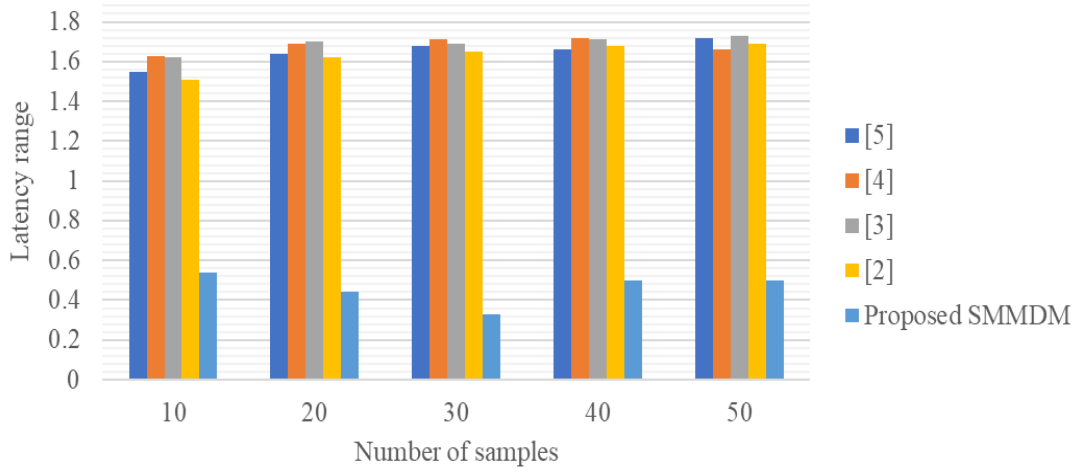

Figure 3: Comparison of Latency Range Versus Number of Samples among the State-of-the-art Approaches and the Proposed SMMDM

Figure 3 compares the latency range versus the number of samples among the advanced methods and the proposed SMMDM. Across all sample sizes (10, 20, 30, 40, and 50), the suggested SMMDM consistently demonstrates considerably reduced latency values, indicating its better efficiency. For instance, for 10 samples, SMMDM attains a latency of 0.54, but the subsequent best approach (Arul et al., 2021) records a delay of 1.51. This pattern persists with increasing samples, while SMMDM consistently exhibits the lowest latency (e.g., 0.33 at 30 samples and 0.5 at 50 samples). The findings illustrate the scalability and resilience of SMMDM in minimizing latency, making it far more successful than current methodologies.

4 CONCLUSION

This research introduces a Secured Multi-Modal Medical Data Management System (SMMDM) using BC and the IoMT. The proposed SMMDM guarantees secure data management between personal servers, medical implants, and between cloud and personal servers. The IoMT-based security architecture utilizes BC to transmit information and manage networked nodes safely. The BC key has been used in a healthcare application network, facilitating the secure creation of alerts from patient OHRs for authenticated healthcare professionals. Across all sample sizes (10, 20, 30, 40, and 50), the suggested SMMDM consistently demonstrates considerably reduced latency values, indicating its better efficiency than other state-of-the-art methods.

REFERENCES

[1] Girardi, F., De Gennaro, G., Colizzi, L., & Convertini, N. (2020). Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain. *Electronics*, *9*(6), 884. https://doi.org/10.3390/electronics9060884

[2] Arul, R., Al-Otaibi, Y. D., Alnumay, W. S., Tariq, U., Shoaib, U., & Piran, M. J. (2021). Multi-modal secure healthcare data dissemination framework using blockchain in IoMT. *Personal and Ubiquitous Computing*, 1-13. https://doi.org/10.1007/s00779-021-01527-2

[3] Ding, X., Zhang, Y., Li, J., Mao, B., Guo, Y., & Li, G. (2023). A feasibility study of multi-mode intelligent fusion medical data transmission technology of industrial Internet of Things combined with medical Internet of Things. *Internet of Things*, *21*, 100689. https://doi.org/10.1016/j.iot.2023.100689

[4] Su, C., Wen, J., Kang, J., Wang, Y., Su, Y., Pan, H., ... & Hossain, M. S. (2024). Hybrid RAG-Empowered Multi-Modal LLM for Secure Data Management in Internet of Medical Things: A Diffusion-Based Contract Approach. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2024.3521425

[5] Khan, M. F., & AbaOud, M. (2023). Blockchain-Integrated security for real-time patient monitoring in the Internet of Medical Things using Federated Learning. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3326155

[6] Zhang, Y., Zhang, X., Shi, Y., Su, L., Yu, J., Chen, Y., & Pan, Z. (2023, August). SC-Chain: A Multi-modal Collaborative Storage System for Medical Resources. In *International Conference on Blockchain and Trustworthy Systems* (pp. 209-222). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-8104-5_16

[7] Muhammad, G., Alshehri, F., Karray, F., El Saddik, A., Alsulaiman, M., & Falk, T. H. (2021). A comprehensive survey on multi-modal medical signals fusion for smart healthcare systems. *Information Fusion*, *76*, 355-375. https://doi.org/10.1016/j.inffus.2021.06.007

[8] Taloba, A. I., Elhadad, A., Rayan, A., Abd El-Aziz, R. M., Salem, M., Alzahrani, A. A., ... & Park, C. (2023). A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. *Alexandria Engineering Journal*, *65*, 263-274. https://doi.org/10.1016/j.aej.2022.09.031