Blockchain and Biometric Systems Integration for IoMT Security

Ilham Laabab, Abdellatif Ezzouhairi, Nour El Madhoun, Muhammad Haris Khan

Blockchain and Biometric Systems Integration for IoMT Security

Ilham Laabab*, Abdellatif Ezzouhairi*, Nour El Madhoun†‡, Muhammad Haris Khan§
* LISA Laboratory, National School of Applied Sciences, Fez, Morocco
† LISITE Laboratory, Isep, 10 Rue de Vanves, 92130, Issy-les-Moulineaux, France
‡ Sorbonne Université, CNRS, LIP6, 4 place Jussieu, 75005, Paris, France
§ Kineton, C.so Orbassano, 416/10, 10137, Turin, Italy
Email: {ilham.laabab, abdellatif.ezzouhairi}@usmba.ac.ma; nour.el-madhoun@isep.fr; muhammad.khan@kineton.it

***Abstract*—In the rapidly evolving landscape of the Internet of Medical Things (IoMT), the demand for robust and trustworthy identification systems has become paramount due to the sensitive nature of healthcare data. Traditional identification methods, such as passwords, tokens and smart cards, are increasingly being replaced by advanced biometric systems, which provide a higher level of security and protection. The rapid advancements in biometric technology, with its potential to uniquely identify individuals, have driven its integration into a wide range of healthcare applications. Meanwhile, blockchain, a decentralized and immutable ledger technology, offers a powerful solution to address critical challenges in IoMT systems, including data security, privacy and trust. The integration of biometric systems with blockchain introduces innovative approaches for secure identity management and authentication, enhancing both security and trustworthiness in digital healthcare environments. This paper explores biometric systems and blockchain technology and their convergence within IoMT systems, focusing on how this combination strengthens the security and trustworthiness of healthcare systems. It also presents a comparative analysis of existing approaches and provides insights into their practical applications and potential for future advancements in secure IoMT systems.**

***Index Terms*—Biometrics, Blockchain, Internet of Medical Things, IoMT, Security.**

I. Introduction

In recent years, the Internet of Medical Things (IoMT) has attracted considerable attention from academia as well as the healthcare industry. These systems aim to collect remote data from patients through wearable sensors and devices [1], enabling real-time health monitoring, remote diagnostics and personalized treatments. However, the transmission of sensitive health data across IoMT networks introduces security and privacy concerns, such as hacking, data breaches and unauthorized access, which can compromise the quality of healthcare services, patient safety and ultimately undermine trust in digital healthcare solutions. To effectively address these challenges, innovative security mechanisms are necessary to safeguard data and ensure efficient and secure user authentication, thereby maintaining the integrity and reliability of IoMT systems.

Traditional authentication methods, such as passwords and PINs, rely on knowledge-based security, which can be easily compromised through phishing and brute-force attacks or can be forgotten or stolen [2]. Thus, these methods provide limited protection, especially in healthcare environments where data privacy is paramount.

Biometric authentication, or simply biometrics [3], has emerged as a promising solution to the aforementioned challenges. It opens up novel possibilities for enhancing security by providing a unique and hard-to-replicate identification method. Unlike conventional authentication methods, biometric traits are difficult to duplicate and require the physical presence of the individual [4], making it a more efficient solution for securing sensitive data in increasingly complex digital systems like IoMT systems.

Blockchain is a breakthrough technology that ensures decentralization, immutability, transparency and data integrity and promotes a higher level of security [5]. In IoMT systems, blockchain's decentralized nature eliminates the reliance on central authorities, ensuring that all interactions with medical data are recorded in an immutable and transparent manner, preventing unauthorized data modifications and strengthening overall data security [6] [7].

Integrating blockchain with biometrics can provide new insights for identity management, authentication and security [5]. Blockchain-driven biometric authentication systems enable secure, immutable and transparent identity verification. This integration facilitates secure, real-time identity verification within IoMT systems, offering enhanced protection against fraud, unauthorized access and privacy breaches in healthcare environments.

This paper is organized as follows: Section II provides an overview of biometrics in IoMT. Section III presents blockchain technology in IoMT, discussing its architecture, advantages and applications. In Section IV, we provide an insightful explanation of how biometrics and blockchain technologies can be integrated within IoMT systems to enhance healthcare security and privacy. Section V presents a comparative analysis of various systems that integrate biometrics and blockchain technologies in IoMT. The last section concludes this paper.

II. Biometrics in IoMT

Biometric systems are advanced technologies that identify and authenticate individuals based on their unique biological and behavioral characteristics. These systems are increasingly

used in various fields, particularly in IoT, due to their high accuracy in personal identification [8].

A. Classification of Biometric Traits

Biometric traits fall into two main categories: physiological and behavioral traits [9]. Physiological traits refer to physical characteristics that are inherent to an individual, such as fingerprints, facial recognition, iris patterns, Electrocardiogram (ECG) and finger-vein. These traits are generally stable and unique, making them reliable for identification purposes. Behavioral traits, on the other hand, are related to patterns in a person's actions, such as voice recognition, gait, signature dynamics and keystroke patterns. Although they may vary over time, they still offer a valuable means of identification when analyzed correctly. The combination of physiological and behavioral traits makes biometric systems more secure and reliable for verifying identity across various applications compared to conventional methods [10]. Such biometric traits and their applications in IoMT are illustrated in Table I.

TABLE I
BIOMETRIC TRAITS AND THEIR APPLICATIONS IN IOMT

Biometric trait	**Type**	**Description**	**Application in IoMT**
Fingerprint	Physiological	Unique pattern of ridges and valleys on fingers	Patient identification and access control in healthcare systems
Facial recognition	Physiological	Analysis of facial features, including the distance between eyes, nose shape, and jawline	Patient Identification
Iris patterns	Physiological	Detailed texture of the iris, unique to each individual	Secure access to medical devices or personal health records
ECG (Electrocardiogram)	Physiological	Measures the unique electrical activity of the heart	Used for continuous health monitoring and secure authentication in medical systems
Finger-vein	Physiological	Used Unique patterns of veins, typically in the hand or finger	Provides secure access to health records or medical devices

B. Biometric Authentication Frameworks in IoMT

In this section, we underline some of the recent advances in the application of biometrics to secure IoMT networks. For instance, a framework is presented by Kabel et al. [11] to secure IoMT networks using cancellable ECG biometric recognition. It proposes a hybrid method that combines blind signal separation and lightweight encryption to produce cancellable biometric templates. These templates are non-invertible, ensuring that even if compromised, the original ECG signals remain secure. This approach enhances user privacy while ensuring robust authentication. The proposed system was tested on two datasets (ECG-ID and MIT-BIH), demonstrating promising results with high security and efficiency, offering an innovative solution for authenticating users in IoMT networks while safeguarding sensitive medical data. Similarly, Hamidi [2] proposed a smart healthcare system based on the IoT that uses biometric authentication (e.g., fingerprint, facial recognition) to ensure secure access to healthcare data. The system provides a more secure and user-friendly alternative to traditional password-based access methods. The results demonstrate that the biometric-based approach effectively enhances user privacy and security, making it suitable for applications like patient monitoring and remote healthcare.

Xin et al. [12] introduced a multimodal biometric authentication system for IoMT, combining face, fingerprint and Finger Vein (FV) recognition to improve security and accuracy. By using feature-level fusion with Fisher vectors, the system addresses the limitations of unimodal methods. The system also incorporates liveness detection to prevent identity spoofing. With k-Nearest Neighbors (kNN) as the optimal classifier, the system significantly enhances both security and recognition, making it highly suitable for IoMT platforms.

III. BLOCKCHAIN IN IOMT (B-IOMT)

A. Architecture of B-IoMT

The architecture of the Blockchain-enabled Internet of Medical Things (B-IoMT) comprises five distinct layers, organized from bottom to top, as shown in Fig. 1. These layers are the Perception layer, Network layer, Blockchain layer, Computing layer and Application layer.

1) Perception Layer: this is the device layer where IoMT nodes, such as wearable devices, smart implants and medical sensors, gather real-time data from patients. These devices continuously monitor vital signs, track medical conditions and collect other health-related information, forming the foundation of connected healthcare.

2) Network Layer: this layer integrates a range of communication technologies (e.g., Wi-Fi, Zigbee, LoRaWAN) to ensure seamless connectivity and data transmission between sensors and actuators in the system.

3) Blockchain Layer: serving as the core layer, it manages secure and trustworthy interactions across underlying layers. It regulates data access between cloud providers, enabling authorized parties to securely share patient information, regardless of its location. Through blockchain's decentralized, immutable ledger, it ensures transparency, trust and controlled access to patient data, supporting seamless cloud integration while safeguarding data privacy and security throughout the IoMT system.

4) Computing Layer: responsible for data processing and storage services, this layer supports scalable data management and enhances decision-making within the IoMT system.

5) Application Layer: it is the topmost layer, focusing on delivering specific healthcare applications and services to end-users. This layer encompasses the user-facing applications and interfaces that interact directly with patients, healthcare providers and other stakeholders.

B. Advantages of B-IoMT

The integration of blockchain technology into the IoMT offers transformative advantages for healthcare systems. We discuss these advantages in the following aspects:

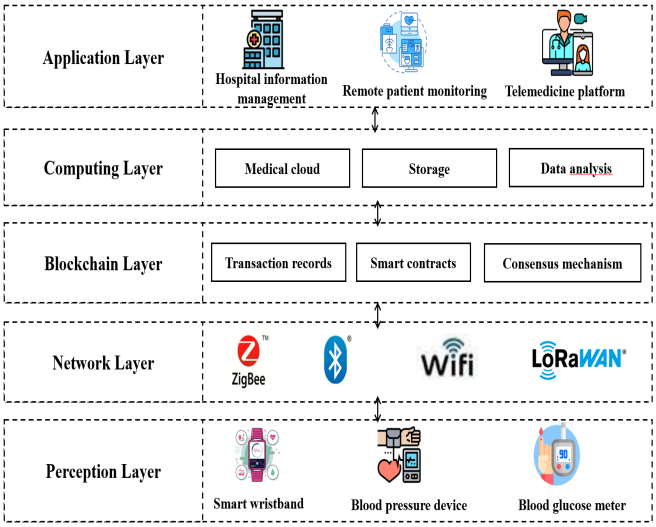

Fig. 1. B-IoMT Architecture Layers

1) Privacy Preservation: it is a critical aspect of safeguarding sensitive patient data and ensuring confidentiality in healthcare systems. Blockchain's decentralized architecture provides enhanced privacy by allowing only authorized parties to access specific data through cryptographic techniques.

2) Transparency: in Blockchain-based IoMT systems, each transaction, whether related to patient data access, device activity, or health monitoring, is recorded in a transparent and tamper-proof manner. This ensures that all actions are traceable. Therefore, blockchain enhances transparency throughout the entire lifecycle of medical devices.

3) Security: sensitive medical data are encrypted and stored across a network of distributed nodes, making it highly resistant to hacking and data breaches. Blockchain's mechanisms ensure that only authorized users can access or modify data, with each transaction being time-stamped and immutable to prevent tampering. Additionally, smart contracts enforce automatic security protocols, such as access control, to restrict data interaction to authorized individuals or devices.

C. Applications of B-IoMT

In this section, we delve into some prominent applications of B-IoMT. These include:

1) Remote Patient Monitoring (RPM): IoMT devices, such as wearable sensors, track patients' vital signs in real time. However, as the use of these devices increases, concerns regarding data privacy and security become more prominent. Blockchain technology addresses these challenges by offering a decentralized, tamper-resistant way to securely log and share data with healthcare professionals.

2) Secure Electronic Health Records (EHR): as the healthcare sector advances toward digitalization, traditional centralized storage systems have become increasingly vulnerable to critical risks such as unauthorized access, data breaches and falsification of patient data. Blockchain offers a powerful solution to these issues by providing a decentralized, tamper-proof ledger for storing and managing patient data. This enhances privacy, data integrity and access control among healthcare providers.

3) Drug Supply Chain Management: ensuring the safety and integrity of pharmaceuticals is a major concern in the healthcare environment, as counterfeit drugs pose significant risks to patient safety. With the growing complexity of global supply chains, it becomes increasingly challenging to track the origin, handling and authenticity of drugs. Blockchain, as an innovative solution, provides a decentralized, tamper-proof system that enables pharmaceutical products to be securely tracked from manufacturer to patient. Moreover, each transaction along the supply chain is immutably recorded, preventing counterfeiting, ensuring proper handling and verifying the authenticity of drugs.

IV. Biometrics and Blockchain Integration in IoMT

The integration of biometrics and blockchain technologies in the IoMT represents a significant advancement in healthcare security and privacy. Biometrics, which is unique to each individual, offers a robust method for authentication, ensuring that only authorized users can access sensitive medical data. This is particularly crucial in IoMT environments where devices collect and transmit personal health information. On the other hand, blockchain technology provides a decentralized and secure framework that can enhance the integrity and transparency of data sharing among various healthcare stakeholders. This integration reduces the risk of data manipulation and unauthorized access. It also facilitates seamless sharing of medical records for telemedicine and remote monitoring. Additionally, it supports smart contracts to automate processes like insurance claims and drug delivery, thereby improving operational efficiency and reducing errors.

V. Comparative Study

Over the past few years, there has been growing interest in integrating blockchain technology with biometrics within the IoMT. Although a few articles have contributed to the understanding of the role of blockchain-enabled biometrics in the IoMT system, they place a strong emphasis on its effectiveness in enhancing security and authentication. Table II illustrates a comparative analysis of some key case studies that highlight this integration.

For instance, Barka et al. [13] presented a biometric-based blockchain system for secure access to Electronic Health Records (EHRs), using fingerprint biometrics. This system integrates biometric authentication with blockchain smart contracts, ensuring secure synchronization and access management across healthcare providers. The results underline the effectiveness of this approach in securely managing access to EHRs. Additionally, Sarier [14] presented a Privacy-Preserving Biometric Authentication (PPBA) protocol designed for smart healthcare using blockchain technology. The main contribution of the authors is the development of an efficient and GDPR

TABLE II
COMPARATIVE ANALYSIS OF BLOCKCHAIN BASED BIOMETRIC SYSTEMS IN IOMT

Criteria	Study 1: BBEHR (Blockchain-Based Biometric EHR)	Study 2: PPBA (Privacy-Preserving Biometric Authentication)	Study 3: FV Biometrics Framework (Finger Vein with Blockchain)
Main Contribution	Develop a system that integrates fingerprint biometrics with blockchain smart contracts for securing EHR access control and ensuring recoverable access to EHRs	Present a GDPR-compliant biometric authentication system using fingerprints integrated with Monero blockchain for anonymous authentication with zero-knowledge proofs	Develop a secure framework combining finger vein biometrics with blockchain, AES encryption, and steganography to ensure patient authentication and data security.
Biometric Type	Fingerprint	Fingerprint	Finger Vein
Blockchain Network	Ethereum	Monero	Custom blockchain
Blockchain Network Type	Public	Public	Custom/private blockchain
Performance Metrics	High security with fingerprint recovery and access validation	High GDPR compliance, low overhead, high resistance to hill climbing attacks, secure biometric anonymity.	high resistance to spoofing and brute-force attacks.

(General Data Protection Regulation)-compliant system that integrates biometric authentication with blockchain for securing patient identities and health data. This protocol is based on anonymous patient authentication using Zero-Knowledge Proofs (ZKP) and ElGamal encryption, ensuring privacy, security and integrity of the biometric data while preventing brute-force attacks like hill-climbing. The authors implemented the system on the Monero blockchain, showing that it allows secure, anonymous verification of patients without disclosing sensitive information. Performance evaluations indicated that the proposed system outperforms existing methods, ensuring high efficiency and protection against attacks, even for low-entropy biometric data.

Moreover, Mohsin et al. [15] proposed a secure framework for patient authentication using FV biometrics, Radio Frequency Identification (RFID), blockchain, AES (Advanced Encryption Standard) encryption and PSO (Particle Swarm Optimization)-based steganography to enhance data security. The authors developed a hybrid biometric model that combines FV and RFID features to increase randomness and protection. Blockchain ensures data integrity, while steganography conceals sensitive biometric information. The system was tested on 6000 FV images, demonstrating high resistance to spoofing and brute-force attacks, with an improvement in securing biometric data during transmission. It also supports decentralized networks, providing high availability and robust security for healthcare applications.

VI. CONCLUSION

The IoMT often requires advanced security solutions to safeguard sensitive medical data and ensure reliable access to healthcare services. Integrating biometric systems provides a robust method for authentication, leveraging unique biological and behavioral traits to verify user identities and access to medical devices. Combining blockchain technology with biometrics further strengthens these systems, addressing complex security challenges. In this paper, we first introduced a global overview of biometrics and blockchain technologies, their integration into IoMT systems, and how this integration enhances healthcare security and privacy. Afterward, we presented a comparative analysis of various systems that integrate these technologies.

REFERENCES

[1] S. Sudevan and M. Joseph, "Internet of things: incorporation into healthcare monitoring," *2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), IEEE*, pp. 1–4, 2019.

[2] H. Hamidi, "An approach to develop the smart health using internet of things and authentication based on biometric technology," *Future generation computer systems, Elsevier*, vol. 91, pp. 434–449, 2019.

[3] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 4–20, 2004.

[4] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE transactions on information forensics and security*, vol. 1, no. 2, pp. 125–143, 2006.

[5] S. Sharma and R. Dwivedi, "A survey on blockchain deployment for biometric systems," *IET blockchain, Wiley Online Library*, 2024.

[6] N. El Madhoun and B. Hammi, "Blockchain technology in the healthcare sector: overview and security analysis," *2024 IEEE 14th annual computing and communication workshop and conference (CCWC)*, pp. 0439–0446, 2024.

[7] D. Maldonado-Ruiz, A. Pulval-Dady, Y. Shi, Z. Wang, N. El Madhoun, and J. Torres, "Nestedchain:"blockchain-inside-a-blockchain" new generation prototype," *Annals of Telecommunications, Springer*, pp. 1–19, 2024.

[8] A. I. Awad, A. Babu, E. Barka, and K. Shuaib, "Ai-powered biometrics for internet of things security: A review and future vision," *Journal of Information Security and Applications, Elsevier*, vol. 82, p. 103748, 2024.

[9] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for internet-of-things security: A review," *Sensors, MDPI*, vol. 21, no. 18, p. 6163, 2021.

[10] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications policy, Elsevier*, vol. 41, no. 10, pp. 1027–1038, 2017.

[11] S. A. El-Moneim Kabel, G. M. El-Banby, L. A. Abou Elazm, W. El-Shafai, N. A. El-Bahnasawy, F. E. A. El-Samie, A. A. Elazm, A. I. Siam, and M. A. Abdelhamed, "Securing internet-of-medical-things networks using cancellable ecg recognition," *Scientific Reports, Nature Publishing Group UK London*, vol. 14, no. 1, p. 10871, 2024.

[12] Y. Xin, L. Kong, Z. Liu, C. Wang, H. Zhu, M. Gao, C. Zhao, and X. Xu, "Multimodal feature-level fusion for biometrics identification system on iomt platform," *IEEE Access*, vol. 6, pp. 21418–21426, 2018.

[13] E. Barka, M. Al Baqari, C. A. Kerrache, and J. Herrera-Tapia, "Implementation of a biometric-based blockchain system for preserving privacy, security, and access control in healthcare records," *Journal of Sensor and Actuator Networks, MDPI*, vol. 11, no. 4, p. 85, 2022.

[14] N. D. Sarier, "Privacy preserving biometric authentication on the blockchain for smart healthcare," *Pervasive and Mobile Computing, Elsevier*, vol. 86, p. 101683, 2022.

[15] A. H. Mohsin, A. Zaidan, B. Zaidan, O. S. Albahri, A. S. Albahri, M. Alsalem, and K. Mohammed, "Based blockchain-pso-aes techniques in finger vein biometrics: A novel verification secure framework for patient authentication," *Computer Standards & Interfaces, Elsevier*, vol. 66, p. 103343, 2019.