FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 3, February, 2026, pp 132 – 138
DOI: https://doi.org/10.33003/fjs-2026-1004-4650

A COMPREHENSIVE REVIEW OF BLOCKCHAIN-ENABLED MULTIMODAL BIOMETRIC AUTHENTICATION FOR PRIVACY-PRESERVING ACCESS CONTROL IN NEXT-GENERATION E-HEALTH SYSTEMS

*** Oyenike Seun Babalola and Afolayan. A. Obiniyi**

Federal University Lokoja, Kogi State

* Corresponding authors' email: babalolaoyenike8@gmail.com

ABSTRACT

The next-generation e-health systems, which include electronic health records (EHRs), telemedicine platforms, and Internet of Medical Things (IoMT) environments, need a strong access control system that protects sensitive medical data while maintaining user privacy. The conventional access control systems face security risks because of credential theft, spoofing attacks, and their reliance on centralized trust, and their inability to scale. Blockchain-enabled multimodal biometric authentication provides a secure and decentralized solution for access control in e-health systems, according to current technological advancements. This paper provides an extensive assessment of blockchain-based multimodal biometric authentication systems, which deliver privacy-protecting access control solutions for future e-health systems. The review further examines central techniques for protecting biometric templates, zero-knowledge proofs, homomorphic encryption, and secure off-chain storage systems. The research assessed existing methods by comparing efficiency for access control, ability to protect user data, capacity to handle growing user needs, ability to work with other systems, and compliance with the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) regulations. The research identifies open challenges that need resolution, which include biometric data revocability, latency constraints, cross-platform interoperability, and limited real-world deployments. The study presents upcoming research paths that will investigate lightweight blockchain systems, post-quantum cryptography, cross-chain medical identity management, and adaptive access control systems in extensive e-health environments. The review demonstrates that blockchain-based multimodal biometric authentication serves as a suitable foundation that enables secure access control through decentralized systems that protect user privacy in upcoming e-health technologies.

Keywords: Access-control, Authentication, E-health System, Biometrics, Blockchain, Privacy-Preserving, Security

INTRODUCTION

The digitalization process of healthcare systems has accelerated remarkably, which has been mainly caused by the introduction of cloud-based electronic health records (EHRs), Internet of Medical Things (IoMT) devices operating in real-time, telemedicine platforms, and medical data exchanges among different institutions (Alawiye,2024). Even more so, the fast growth of digital health infrastructures has made them more susceptible to cyber-attacks, unauthorized access, and data leaks. The use of traditional authentication methods like passwords, ID cards, or PINs is no longer sufficient, mainly due to susceptibility to theft, guessing, social engineering, and insider compromise (Suleski *et al.,* 2023).

Among security measures, biometric authentication seems to be the most appealing one since it is based on the characteristics that people possess and are difficult to change or imitate, thus being the most reliable. However, unimodal biometric systems (e.g., fingerprint-only or face-only) are still facing issues like high error rates, aging factors, spoof attacks, and variations of environmental conditions. Additionally, the storage of biometric templates in a centralized database raises concerns about privacy and permanence, as once the biometric data is compromised, it cannot be changed or revoked (Zaidi & Mallik, 2025). Blockchain technology is a great solution for biometric door locks and cardless security systems due to its decentralization, immutability, and numerous security features. The combination of blockchain technology and multimodal biometric systems, which encompass various traits such as fingerprints, facial recognition, and Electrocardiogram (ECG), among other modalities, offers a powerful privacy-preserving infrastructure well-suited to the future of e-health systems (Ghafourian *et al.,* 2023; Babu *et al.,* 2025).

Background and Motivation

The rapid digitization of healthcare services and the growing reliance on electronic health records have intensified concerns related to security, privacy, and access control. Traditional authentication mechanisms are increasingly inadequate in addressing evolving cyber threats and the stringent confidentiality requirements of e-health systems. This section provides the necessary background and motivation for adopting multimodal biometric authentication and blockchain technology as complementary solutions for secure, reliable, and privacy-preserving healthcare access.

Healthcare institutions and centers are becoming increasingly popular for cybercriminals due to the huge economic value of the data and the still very weak security measures. Unauthorized access, hacking of credentials, and insider threats are still the main problems that the traditional user authentication methods are facing (Javaid *et al.,* 2023). Healthcare data is very delicate, very long-lasting, and very difficult to revoke: the need for strong authentication methods is crucial. Authentication methods that rely on passwords, PIN codes, or similar techniques are still dominant but at the same time, they are highly vulnerable to being stolen, reused, or attacked. This is mainly attributed to the poor practices in making passwords and the compromising of the credentials. There are limitations in unimodal biometrics, such as the quality of sensor capture that can be quite poor, the usability of the system being reduced for people with disabilities, and the system being easily fooled by the presentation or spoofing

attacks. Other limitations include the performance drop due to ageing or health-related issues, and the risk that a biometric template gets compromised. All these limitations together greatly lessen the dependability of the single-factor and unimodal authentication methods in the healthcare sector which in turn drives the increasing acceptance of multimodal biometric authentication systems that are characterized by better robustness and security (Wang *et al.,* 2021). Multimodal biometric authentication systems are based on the use of several biometric features, such as face, fingerprint, iris, or gait, resulting in more secure identity verification and higher reliability. These systems have been shown to perform better in terms of recognition accuracy with lower error rates and greater robustness when facing diverse environmental and operational conditions, thanks to the combination of sources of information from different modalities (Muhammad, 2025). In addition to this, the combination of biometric traits also makes it harder for attackers to spoof or perform presentation attacks, as the attacker would have to compromise all the biometric channels simultaneously, thus making the system suitable for high-security applications such as healthcare access control.

Why Blockchain

The very nature of blockchain technology gives it a series of big advantages that make it ideal for e-health systems to secure access control. For instance, in the first place, the decentralized trust model is the one eliminating single points of failure, the next immutability makes logging and tamper detection reliable; finally, smart contracts will automatically collect the rule-based access control. Furthermore, blockchain is still in centralized databases, where privacy and confidentiality on the part of the users are maintained, while cryptographic techniques protect sensitive information from being altered by unauthorized persons. If it were to be combined with multimodal biometric authentication, then one could have secure, transparent, and privacy-preserving e-health access solutions that are in complete accordance with data protection and patient confidentiality requirements (Tripathi *et al.,*2023).

Motivation for Integration

Combining multimodal biometric authentication with blockchain technology not only provides a secure but also a scalable solution to access control in modern e-health systems. The use of multimodal biometrics not only ensures safety but also reliable identity authentication at the same time, while the use of blockchain technology not only mitigates the different insider threats through decentralized trust management but also provides immutable audit trails. Moreover, blockchain-based access logging not only aids but also supports compliance with regulatory requirements such as the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability (HIPAA), whereas smart contracts not only enforce transparency but also regulate access control based on rules. Therefore, by uniting these technologies, a solid digital trust architecture is made, which can still accommodate the coming healthcare ecosystems that will demand secure, privacy-preserving, and interoperable identity management (Abbas ***et al.,* 2026**).

Multimodal Biometric Authentication in E-Health

Multimodal biometric authentication requires two or more biometric modalities to be utilized, such as fingerprint, iris, facial recognition, voice, or electrocardiogram (ECG) signals to establish the identity of an individual. In contrast to single biometric systems, which are mostly subject to noise, spoofing attacks, and intra-class variations, multimodal systems take advantage of complementary biometric information to enhance accuracy, reliability, and robustness. The improved performance makes multimodal biometric authentication especially appropriate for e-health areas, where secure identity verification is of paramount importance to safeguarding sensitive medical data as well as controlling access to healthcare services. (Kozierkiewicz *et al.*,2025).

Biometric authentication systems in healthcare use an array of physiological and behavioral traits such as fingerprint and finger-vein patterns, face, iris, retina, and sclera recognition, ECG and PPG signals, palmprint and palm-vein, and voice and gait characteristics. The combination of several biometric modalities plays a major role in improving authentication accuracy and reliability, particularly in emergency and clinical situations where single biometric traits might be compromised by noise, injury, or environmental factors (Shaheed *et al.,* 2021).

At different stages of the authentication pipeline in multimodal biometric systems, fusion can take place among sensor, feature, score, and decision levels. Each of the integration techniques has its own advantages and disadvantages in terms of computational complexity and recognition performance (Bala *et al.,* 2022). Among these techniques, feature-level fusion has been the most popular choice. It is because it allows the integration of diverse and complementary biometric representations into one feature space. Besides, when the use of deep learning models such as convolutional neural networks (CNNs) is combined with feature-level fusion, it can efficiently extract very hardy and discriminative features, leading to better recognition accuracy and robustness compared to score and decision-level fusion techniques (Jiao *et al.,* 2024). The development of biometric template protection approaches is a response to the privacy and security issues raised by biometric data storage. Cancelable biometrics, fuzzy vault and fuzzy commitment schemes, biometric hashing, and the use of cryptographic techniques to protect raw biometric templates from direct exposure are among the methods that have been proposed (Abdullahi *et al.,* 2024). Furthermore, the use of modern e-health systems increasingly relies on embedding privacy-preserving encryption techniques such as homomorphic encryption and secure off-chain storage architectures to protect sensitive biometric data while allowing authentication to occur (Khan *et al.,* 2022). These different techniques together make it impossible to reverse-engineer or misuse biometric templates even if there is a data breach. The different deep learning architectures like ResNet, DenseNet, FaceNet, and VGG are significant for the whole process of multimodal biometrics because they offer the extraction of extremely discriminative and invariant feature representations from biometric streams. These models turn out to be even more robust in impersonation attacks than the earlier ones, and noise in the environment commonly found in clinical and health care places can be managed quite efficiently (Bhairnallykar & Narawade, 2024). Through the ground of deep learning networks through end-to-end learning, real-time processing of biometrics is significantly made possible, thus enhancing the accuracy, dependability, and durability of authentication systems for e-health applications (Li *et al.,* 2023).

Blockchain-Enabled Biometric Access Control

Blockchain-based biometric access control unravels a decentralized and non-tampering mechanism for the management of the authentication and authorization processes in e-health systems. Multimodal biometric verification

combined with distributed ledger technology, such frameworks completely do away with the dependency on central authorities while at the same time securing the transparency and permanence of access records (Tawfik *et al.,* 2025). Access control systems based on blockchain technology also generate audit and traceable access logs for the most sensitive medical resources, which, in turn, make trust and accountability stronger in the management of healthcare data (Ullah *et al.,* 2024). The current section discusses blockchain as the authentication backbone, the function of smart contracts in access control, and the architectural components that guarantee access to healthcare while preserving privacy.

Blockchain is a decentralized authentication layer that allows the storage of data across the network, making it possible to have very easy and very clear access trails that can easily be verified, and automated access control policies that are done using smart contracts (Tripathi *et al.,* 2023). The smart contracts in blockchain-based e-health systems manage role-based access control and secure identity sharing among the healthcare providers without the need for a centralized authority. This decentralized model brings to light the benefits of reduced insider threats, no single point of failure, and no unauthorized data manipulation, all while providing auditability and accountability (Tawfik *et al.,* 2025). The blockchain layer, multimodal biometric authentication, smart contracts, and hybrid on-chain/off-chain storage components, together as shown in Figure 1, create a highly secure and tamper-proof access control system that can be used in e-health environments.

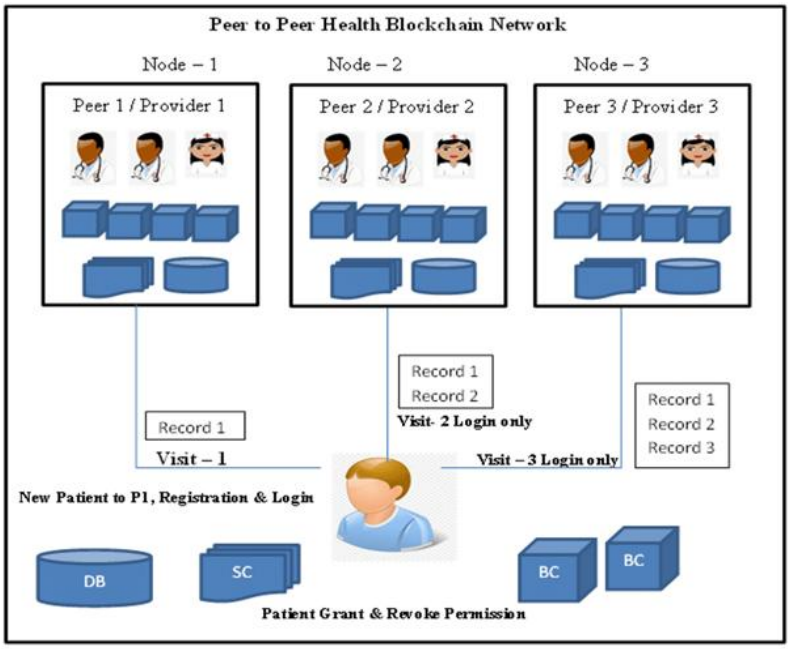

Figure 1. Architecture of Blockchain-Enabled Multimodal Biometric Authentication in E-Health Systems (Chelladurai & Pandian, 2022)

Consensus Mechanisms

The choice of consensus mechanisms impacts scalability, latency, and the main feature of blockchain-based identification systems, trust. Proof of Work (PoW) tasks the miners with solving difficult puzzles to guarantee the highest possible security: however, its latency and energy consumption make it very unsuitable for the healthcare sector. Other methods like Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Authority (PoA), and Practical Byzantine Fault Tolerance (PBFT) are not only more efficient but also faster in validating transactions and increasing throughput. In e-health systems, PoA and PBFT are often the preferred choices since they allow for authentication with low latency and work well in authority and trust-based hospital networks (Liu *et al.,* 2025).

Blockchain-based e-health systems make use of on-chain, off-chain, or hybrid storage architectures, depending on the factors of security and privacy. The use of the technology can draw on the performance of the application. One of the drawbacks of on-chain storage is that it can store only hashes and meta-data while off-chain storage can accommodate sensitive biometric templates and medical records. Thus, latency is reduced, and patient privacy is protected (Andrew *et al.*,2023). Hybrid storage architectures merge these methods, and consequently, they ensure regulatory compliance and access control that is both secure and efficient in the healthcare sector.

Through smart contract-based authorization, consensus-driven validation, and hybrid storage mechanisms, the blockchain-controlled access framework transforms into a complete authentication pipeline. Figure 2 shows the entire workflow of this process from the beginning to the end, revealing the interaction of multimodal biometric acquisition, blockchain validation, and secure data storage, in allowing privacy-preserving access to e-health services.

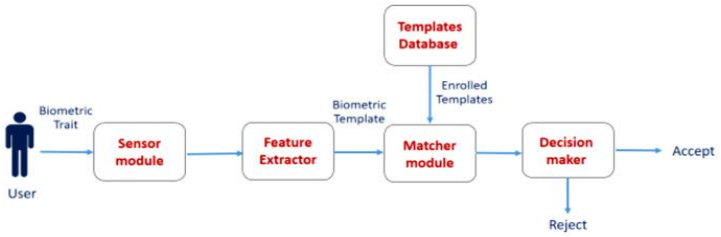

Figure 2: End-to-End Authentication Process Using Blockchain and Multimodal Biometrics (Salem et al., 2024)

A multimodal biometric data acquisition is the first stage in the whole authentication process. The user's physical or behavioral characteristics are then captured. The biometric features that are extracted are then put through a process during which they are merged into a single authentication template. This template is then secured using privacy-preserving methods BEFORE being sent out. The biometric representation that has been secured is next sent to the blockchain network, where smart contracts authenticate the requests based on the access policies that have been set beforehand. Consensus mechanisms confirm the transaction, meanwhile, delicate biometric data and medical records are managed through a combination of on-chain and off-chain storage. Health services are then opened for the user if they have been verified successfully, thereby they can enjoy secure, auditable, and privacy-preserving healthcare access (Anabor, 2022).

Privacy-Preserving Cryptographic Frameworks

The preservation of privacy is a very important factor in biometric-based e-health authentication systems since the biometric data is irreversible and sensitive. In response to these concerns, different types of cryptographic frameworks have been introduced to make it possible for secure authentication and access control without revealing the raw biometric templates. These methods adhere to privacy-by-design concepts by guaranteeing confidentiality, integrity, and constrained disclosure of biometric information during the authentication process. The most common of these methods are zero-knowledge proofs, homomorphic encryption, and error-tolerant template protection schemes (Mao *et al.,* 2023). Zero-knowledge proofs (ZKPs) grant a user the ability to prove the possession of valid biometric credentials or authentication rights without the underlying biometric data being revealed. This feature qualifies ZKPs as an ideal candidate for privacy-sensitive e-health applications where the confidentiality of patient data has to be maintained at all times. By permitting the validation process without the actual data being opened up, ZKPs lessen the likelihood of biometric data being misused while they are still being utilized in secure, auditable authentication workflows in decentralized systems such as blockchain-based healthcare platforms (Bhattacharya *et al.,* 2024).

Homomorphic encryption makes it possible to carry out operations such as biometric matching and similarity assessment right on the encrypted data. This allows for the processing of the biometrics without revealing the biometric templates, as the server performing the authentication has no access to any unencrypted data. This feature of e-health systems becomes even more important for the security of biometric data that is either stored or processed in the cloud or distributed blockchain networks, which are usually regarded as untrustworthy environments. Homomorphic encryption not only enables functional biometric verification but also guarantees user data privacy, as in the case of e-health systems (Yang *et al.,* 2023). Fuzzy vault and fuzzy commitment schemes are among the most reliable biometric template protection solutions. They are based on the premise that human beings cannot produce identical signs of their fingerprints or retina, and thus the systems must be designed in a way that can still acknowledge the variation of the pattern while preserving the security. They accomplish this task by tightly incorporating cryptographic keys with the biometric features, thus ensuring that the authentication process continues to be strong, even in the presence of the noise caused by aging, the effects of the sensors, or their inconsistencies. Fuzzy vaults and fuzzy commitment schemes have gained a lot of popularity in biometric systems owing to their anti-reverse engineering characteristics, which make it equally hard to recover the originals from the templates. Thus, they are also quite often used in various authentication scenarios in the healthcare sector (Rathgeb *et al.,* 2022).

State of the Art Approaches (2020–2025)

Utilization of Biometrics in e-health systems with Blockchain technology has been the primary focus of research activities in the field of biometric authentication improvement through accuracy, decentralization, and efficiency enhancement.

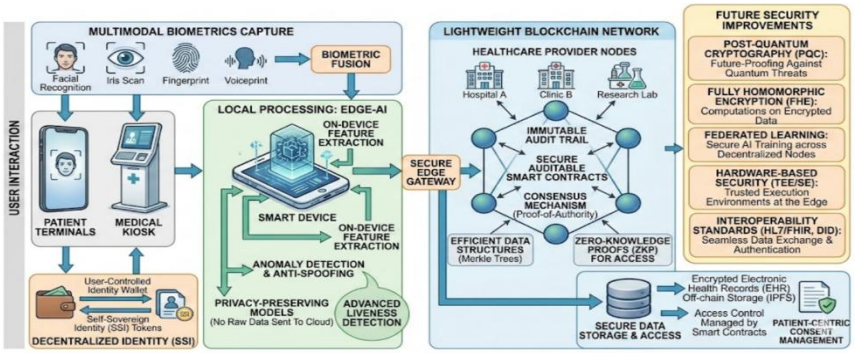

Figure 3: The Current State-of-the-art Approaches to Biometrics Health Systems with Blockchain Technology (Dwivedi, 2024)

The studies affirm that the use of blockchain, along with multiple biometric traits, increases the robustness and accuracy of the authentication process. For example, the combination of facial and dorsal-hand biometric authentication has resulted in a success rate of 99.8%, whereas the fingerprint-face fusion via feature-level CNNs has shown 98.4% accuracy that exemplifies the power of deep learning-based multimodal fusion (Sharma & Dwivedi, 2024). SSIs, via mobile biometric authentication, have gained acceptance as a reliable method to enable users to manage their biometric credentials without depending upon a centralized authority, thus enhancing privacy and trust in healthcare access control systems (Alrawili *et al.*, 2024). The merger of Edge-AI with light blockchain protocols has led to an enormous drop in system latency and has caused the authentication to be less than a millisecond due to the use of optimized consensus mechanisms (Gao & Yan, 2025). Moreover, on-device biometric processing, which uses Edge-AI models, not only reduces latency and bandwidth consumption but also considers such systems for real-time e-health applications.

MATERIALS AND METHODS

This study adopts a systematic literature review approach to examine blockchain-enabled multimodal biometric authentication for privacy-preserving access control in e-health systems. Relevant academic publications were collected from reputable databases, including IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar, and ACM Digital Library.

The search was conducted using key terms such as "blockchain in healthcare," "multimodal biometric authentication," "privacy-preserving biometrics," "e-health security," and "biometric template protection." Only peer-reviewed journal articles and conference papers published between 2020 and 2025 were considered to ensure the inclusion of recent advancements.

The inclusion criteria focused on studies that:

(i) integrate blockchain with biometric authentication,

(ii) address privacy and security in healthcare systems, and

(iii) propose or evaluate multimodal biometric techniques.

Studies that were outdated, lacked technical depth, or were not relevant to healthcare applications were excluded.

A total of selected studies were critically analyzed based on key evaluation metrics, including security strength, privacy preservation capability, scalability, computational efficiency, interoperability, and compliance with regulatory standards such as GDPR and HIPAA. The extracted data were synthesized and categorized into thematic areas, including biometric techniques, blockchain integration models, cryptographic frameworks, and application architectures, t o provide a comprehensive understanding of the current state of the art.

RESULTS AND DISCUSSION

Table 1: Summary of Selected Studies on Blockchain-Enabled Multimodal Biometric Authentication

Author(s)	Year	Biometrics Used	Blockchain Type	Key Technique	Key Findings
Sharma & Dwivedi	2024	Face + Dorsal Hand	Private Blockchain	CNN-based fusion	Achieved 99.8% accuracy
Alrawili et al.	2024	Mobile Biometrics	Blockchain-based SSI	Identity management	Improved user privacy and control
Gao & Yan	2025	Face + Fingerprint	Lightweight Blockchain	Edge-AI integration	Reduced latency to <1 ms
Tawfik et al.	2025	Multimodal	Distributed Ledger	Smart contracts	Enhanced secure access control
Ullah et al.	2024	Biometric + EHR	Blockchain	Audit logging	Improved traceability and trust

Table 2: Comparative Analysis of Existing Approaches

Feature	Traditional Methods	Unimodal Biometrics	Multimodal + Blockchain
Security	Low	Medium	High
Accuracy	Low	Moderate	Very High
Privacy	Weak	Moderate	Strong
Scalability	High	Moderate	Challenging
Resistance to Attack	Low	Medium	Very High
Auditability	None	Limited	Full (Blockchain-enabled)

The results of the reviewed studies are summarized in Tables 1 and 2. Table 1 presents an overview of key studies, highlighting the biometric modalities used, blockchain integration approaches, and major findings. The analysis shows that multimodal biometric systems integrated with blockchain technology consistently achieve higher authentication accuracy and improved privacy protection.

Table 2 provides a comparative analysis between traditional authentication methods, unimodal biometrics, and blockchain-enabled multimodal systems. It is evident that the integrated approach offers superior performance in terms of security, reliability, and resistance to attacks. Furthermore, recent studies demonstrate that the incorporation of Edge-AI and lightweight blockchain protocols significantly reduces latency, making these systems suitable for real-time healthcare applications. However, scalability and computational complexity remain key limitations. The findings confirm that blockchain-enabled multimodal biometric authentication represents a significant advancement over existing authentication mechanisms in e-health systems.

The findings from the reviewed studies (as summarized in Tables 1 and 2) indicate that blockchain-enabled multimodal biometric authentication significantly improves security, privacy, and reliability in e-health systems. The combination of multiple biometric traits enhances authentication accuracy and reduces false acceptance and rejection rates.

Additionally, the integration of blockchain introduces decentralization, eliminating single points of failure and enabling transparent, tamper-proof audit trails through smart contracts. Privacy-preserving techniques such as zero-knowledge proofs and homomorphic encryption further strengthen data protection during storage and processing. However, the results also reveal challenges related to scalability and computational overhead, particularly in large-

scale healthcare environments. Despite these limitations, the overall evidence demonstrates the effectiveness of blockchain-based multimodal biometric systems for secure healthcare access control.

Discussion

The findings from this review indicate that the integration of blockchain technology with multimodal biometric authentication offers a promising approach to addressing security and privacy challenges in e-health systems. Compared to traditional authentication mechanisms, multimodal biometrics provide higher accuracy and robustness by combining multiple sources of identity verification. Blockchain further strengthens this framework by ensuring decentralization, transparency, and immutability. This reduces the risks associated with centralized data storage, such as data breaches and insider attacks. Additionally, the use of smart contracts enhances automation and trust in access control decisions. Despite these advantages, several challenges remain. The high computational cost of deep learning-based biometric systems and the latency introduced by blockchain consensus mechanisms may affect real-time performance. Moreover, issues related to interoperability and compliance with regulatory standards require further attention.

Another critical concern is the irreversibility of biometric data. While cryptographic techniques offer protection, the inability to revoke compromised biometric information remains a limitation. Therefore, future systems must focus on developing revocable and cancelable biometric solutions. While significant progress has been made, further research and real-world implementation are necessary to fully realize the potential of blockchain-enabled biometric authentication in healthcare.

CONCLUSION

This paper has presented a comprehensive review of blockchain-enabled multimodal biometric authentication for privacy-presing access control in next-generation e-health systems. The study highlights how the integration of blockchain technology with multiple biometric modalities enhances security, privacy, and reliability in healthcare applications. The review shows that blockchain provides a decentralized and tamper-resistant framework, while multimodal biometrics improve authentication accuracy and robustness. Additionally, advanced cryptographic techniques further strengthen data protection and privacy preservation. However, challenges such as scalability, computational complexity, interoperability, and regulatory compliance continue to limit widespread adoption. Addressing these challenges will be critical for the successful deployment of such systems in real-world healthcare environments. Future research should focus on lightweight blockchain solutions, efficient biometric processing techniques, and large-scale practical implementations. These advancements will play a key role in developing secure, scalable, and privacy-preserving e-health systems.

REFERENCES

Abbas, S. R., Abbas, Z., Rehman, M. U., & Lee, S. W. (2026). *Blockchain for smart healthcare: A systematic review of security, interoperability, and AI–IoT integration.* Digital Health. Advance online publication. https://doi.org/10.1177/20552076261420

Abdullahi, S. M., Sun, S., Wang, B., Wei, N., & Wang, H. (2024). Biometric template attacks and recent protection mechanisms: A survey. *Information Fusion, 103*, 102144. https://doi.org/10.1016/j.inffus.2023.102144

Alawiye, T. (2024). *The impact of digital technology on healthcare delivery and patient outcomes. E-Health Telecommunication Systems and Networks, 13*, 13–22. https://doi.org/10.4236/etsn.2024.132002

Alrawili, R., AlQahtani, A. A. S., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. *Computers and Electrical Engineering, 119*(Part A), 109485. https://doi.org/10.1016/j.compeleceng.2024.109485

Anabor, J. O. (2022). Multimodal biometrics: For authorisation and authentication. In K. Daimi, G. Francia III, & L. H. Encinas (Eds.), *Breakthroughs in digital biometrics and forensics* (pp. [insert page range if known]). Springer. https://doi.org/10.1007/978-3-031-10706-1_2

Andrew, J., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications, 215*, 103633. https://doi.org/10.1016/j.jnca.2023.103633

Babu, A., Balasubramanian, K. R., Singh, A., Sureshbabu, M. R., & Natarajan, Y. (2025). *Decentralized digital identity: A blockchain and neural network approach.Premier Journal of Science.* https://doi.org/10.70389/PJS.100142

Bala, N., Gupta, R., & Kumar, A. (2022). Multimodal biometric system based on fusion techniques: A review. *Information Security Journal: A Global Perspective, 31*(3), 289–337. https://doi.org/10.1080/19393555.2021.1974130

Bhairnallykar, S. T., & Narawade, V. (2024). A comprehensive exploration of convolutional neural network architectures in deep learning. In Z. Illés, C. Verma, P. J. S. Gonçalves, & P. K. Singh (Eds.), *Proceedings of International Conference on Recent Innovations in Computing (ICRIC 2023)* (Lecture Notes in Electrical Engineering, Vol. 1195, pp. [insert page range if known]). Springer. https://doi.org/10.1007/978-981-97-3442-9_12

Bhattacharya, S., Seth, D. K., Panyam, S., &Gangrade, P. (2024). Enhancing digital privacy: The application of zero-knowledge proofs in authentication systems. *International Journal of Computer Trends and Technology, 72*(4), 34–41. https://doi.org/10.14445/22312803/IJCTT-V72I4P104

Gao, Z., & Yan, W. (2025). The real-time data processing framework for blockchain and edge computing. *Alexandria Engineering Journal, 120*, 50–61. https://doi.org/10.1016/j.aej.2025.01.092

Ghafourian, M., Sumer, B., Vera-Rodriguez, R., Fierrez, J., Tolosana, R., & Morales, A. (2023). *Combining blockchain and biometrics: A survey on technical aspects and a first legal analysis.arXiv*. https://doi.org/10.48550/arXiv.2302.10883

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023).*Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends.*Cyber Security and Applications, 1, Article 100016. https://doi.org/10.1016/j.csa.2023.100016

Jiao, T., Guo, C., Feng, X., Chen, Y., & Song, J. (2024). A comprehensive survey on deep learning multi-modal fusion: Methods, technologies and applications. *Computers, Materials & Continua*, *80*(1), 1–35. https://doi.org/10.32604/cmc.2024.053204

Khan, T., Tian, W., Ilager, S., &Buyya, R. (2022). Workload forecasting and energy state estimation in cloud data centres: ML-centric approach. *Future Generation Computer Systems, 128,* 320–332. https://doi.org/10.1016/j.future.2021.10.019

Kozierkiewicz, A., Graczyk, A., &Pimenidis, E. (2025). A multimodal approach to biometric authentication. In H. Jahankhani& B. Issac (Eds.), *Cybersecurity and human capabilities through symbiotic artificial intelligence (ICGS3 2023)* (pp. 481–496). Springer. https://doi.org/10.1007/978-3-031-82031-1_24

Li, S., Nguyen, H.-T., & Cheah, C. C. (2023). A theoretical framework for end-to-end learning of deep neural networks with applications to robotics. *IEEE Access*, *11*, 21992–22006. https://doi.org/10.1109/ACCESS.2023.3249280

Liu, J., Liu, C., Lin, M., & Xu, G. (2025). Comprehensive survey of blockchain consensus mechanisms: Analysis, applications, and future trends. *Computer Networks*, *272*, 111661. https://doi.org/10.1016/j.comnet.2025.111661

Mao, X., Chen, Y., Deng, C., & Zhou, X. (2023). A novel privacy-preserving biometric authentication scheme. *PLoS ONE*, *18*(5), e0286215. https://doi.org/10.1371/journal.pone.0286215

Muhammad, A. (2025, July).*Multimodal biometric authentication: Integrating fingerprints, face, and voice using AI: An AI-based approach to secure identity verification using fingerprint, face, and voice biometrics* (Preprint). https://doi.org/10.31224/4808

Rathgeb, C., Merkle, J., Scholz, J., Tams, B., &Nesterowicz, V. (2022). Deep face fuzzy vault: Implementation and performance. *Computers & Security*, *113*, 102539. https://doi.org/10.1016/j.cose.2021.102539

Shaheed, K., Mao, A., Qureshi, I., & others. (2021). A systematic review on physiological-based biometric recognition systems: Current and future trends. *Archives of Computational Methods in Engineering*, *28*, 4917–4960. https://doi.org/10.1007/s11831-021-09560-3

Shaikh, M., Wiil, U. K., & Ebrahimi, A. (2026). An overview and comparison of blockchain consensus mechanisms. *International Journal of Networked and Distributed Computing*, *14*, 4. https://doi.org/10.1007/s44227-025-00087-8

Sharma, S., & Dwivedi, R. (2024). A survey on blockchain deployment for biometric systems. *IET Blockchain*, *4*(2), 124–151. https://doi.org/10.1049/blc2.12063

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). *A review of multi-factor authentication in the Internet of Healthcare Things. DIGITAL HEALTH*, *9*, 20552076231177144. https://doi.org/10.1177/20552076231177144

Tawfik, A. M., Al-Ahwal, A., Tag Eldien, A. S., & Zayed, H. H. (2025). Blockchain-based access control and privacy preservation in healthcare: A comprehensive survey. *Cluster Computing*, *28*, 529. https://doi.org/10.1007/s10586-025-05308-x

Tripathi, G., Ahad, M. A., & Casalino, G. (2023).*A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges.*Decision Analytics Journal, 9, Article 100344. https://doi.org/10.1016/j.dajour.2023.100344

Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decision Analytics Journal*, *9*, 100344. https://doi.org/10.1016/j.dajour.2023.100344

Ullah, F., He, J., Zhu, N., Wajahat, A., Nazir, A., Qureshi, S., Pathan, M. S., & Dev, S. (2024). Blockchain-enabled EHR access auditing: Enhancing healthcare data security. *Heliyon*, *10*(16), e34407. https://doi.org/10.1016/j.heliyon.2024.e34407

Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021).*Attacks and defenses in user authentication systems: A survey.*Journal of Network and Computer Applications, 188, Article 103080. https://doi.org/10.1016/j.jnca.2021.103080

Yang, W., Wang, S., Cui, H., Tang, Z., & Li, Y. (2023). A review of homomorphic encryption for privacy-preserving biometrics. *Sensors*, *23*(7), 3566. https://doi.org/10.3390/s23073566

Zaidi, T., & Mallik, S. (2025). *Software applications for biometric informatics.* In S. L. Tripathi, V. E. Balas, M. Mahmud, & S. Banerjee (Eds.), *Machine learning models and architectures for biomedical signal processing* (pp. 475–486). Elsevier. https://doi.org/10.1016/B978-0-443-22158-3.00019-3

Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero-knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges, and opportunities. *Journal of Information Security and Applications*, *80*, 103678. https://doi.org/10.1016/j.jisa.2023.103678

Zouaghi, I., Barka, E., & Kerrache, C. A. (2022). *Privacy-preserving storage for blockchain-based e-health systems*. Future Generation Computer Systems, 128**,** 321–334. https://doi.org/10.1016/j.future.2021.10.019