Journal of Information Technology Management
ISSN-OnLine: 2980-7972
University of Tehran

Blockchain-Based Smart Multimodal Biometric Multimedia Transmission

Ghada Alhudhud *

*Corresponding author, Professor, Department of Data Science and Artificial Intelligence, Faculty of Information Technology, Al-Ahilya Amman University, Amman, Jordan. E-mail: g.alhudhud@ammanu.edu.jo

Marwan Al-Akaidi

Professor, Vice Chancellor and CEO Wigwe University, Isiokpo, Nigeria. E-mail: Marwan.alakaidi@wigweuniversity.edu.ng

Journal of Information Technology Management, 2025, Vol. 18, Issue 2, pp. 110-119
Published by the University of Tehran, College of Management
doi: https://doi.org/10.22059/jitm.2026.107233
Article Type: Research Paper

Received: December 07, 2025
Received in revised form: January 17, 2026
Accepted: February 21, 2026
Published online: March 01, 2026

Abstract

In recent years, the rapid growth of freely accessible digital and multimedia content, coupled with declining trust in online security, has created an urgent need for more reliable and efficient transmis-sion frameworks. Conventional protection methods—such as passwords and periodically updated encryption keys—have proven inadequate against escalating cyber threats, identity spoofing, and da-ta breaches. This study presents a novel framework that integrates blockchain technology with seam-less biometric authentication to ensure secure data transmission. The system employs multimodal biometric and facial recognition techniques to encrypt multimedia content, while a blockchain ledger verifies, traces, and records all data exchanges within a self-sufficient validation environment. Through architectural design, simulation, and threat modeling, results show that combining multi-modal biometric fusion with blockchain significantly enhances authentication reliability and data integrity, minimizing manipulation and unauthorized access. Unlike traditional systems, the pro-posed framework strengthens data consistency, user identity assurance, and protection from cyberat-tacks—delivering a superior user experience well-suited for next-generation multimedia applica-tions.

Keywords: Blockchain, Multimodal Biometrics, Multimedia Security, Decentralized Storage, Encryption, Access Control

Introduction

The evolution of digital audio-visual communication has been driven largely by the Internet, which—together with numerous mobile applications—has merged diverse communication paradigms to enable real-time global interaction. However, alongside these benefits come growing concerns about security and privacy. The unauthorized transmission of sensitive medical, personal, and surveillance data, as well as issues of content tampering, identity theft, and privacy violations, represent major challenges in the digital era (Aswathy & Tyagi, 2022).

Although remote access enables faster and easier content sharing, it also increases exposure to privacy risks and cyber threats. Multimedia systems often rely on user data through behavioral and biometric patterns—such as fingerprints, voice, facial, and iris recognition—for authentication. Among these, voice and facial recognition are especially popular due to their ease of integration and non-intrusive nature. Our earlier work (Alhudhud & Alhalabi, 2023) introduced a voice-biometric security framework that proved effective for authentication and content protection. Yet, unimodal biometric systems (those using a single trait) remain vulnerable to spoofing, user exclusion, and environmental inconsistencies, leading to reduced accuracy (Kothinti, 2024).

To address these limitations, this paper proposes a multimodal biometric authentication framework that combines fingerprint and facial recognition for stronger, more inclusive security. Multimodal systems offer greater resistance to spoofing, lower error rates, and improved reliability under real-world conditions by creating richer identity profiles through multiple biometric sources.

At the core of this approach lies blockchain technology, serving as an immutable ledger for verifying content integrity and managing access control. Biometric hashes, encryption keys, and metadata are validated across distributed nodes, while smart contracts regulate content decryption and access—ensuring that only authenticated users can retrieve multimedia data.

The integrated model securely manages multimedia transmission through multimodal encryption and blockchain validation. Its performance is assessed via theoretical modeling, architectural design, and blockchain-based verification. Ultimately, this framework enhances trust and transparency in digital communication, addressing key gaps in current multimedia security (Dick & Wessel, 2023).

Literature Review

Blockchain for Secure Transmission

Blockchain technology has transformed how digital transactions are recorded and managed. Its immutable and transparent ledger, maintained through peer consensus, eliminates the need for centralized intermediaries. Within multimedia systems, blockchain addresses key challenges such as unauthorized access, identity spoofing, and content tampering. For instance, Kumar et al. (2019) introduced Advanced Decentralized Digital Blockchain systems that authenticate users without a central authority and record every multimedia transaction through smart contracts, ensuring compliance with authentication and credentialing protocols. The use of blockchain in areas like dental record exchange, digital rights management, and patient documentation has shown strong potential. However, its integration with real-time biometric authentication, particularly multimodal biometric systems, remains a developing area of study. Numerous variables are involved in green supply chain management and investigating any intervening variable can influence a diverse set of others. Blockchain, as an emerging technology of the fourth generation of the industry, comes with a variety of distinctive characteristics (Sadeghi et al., 2023).

Multimodal Biometric Authentication

Multimodal biometrics employs two or more physiological (fingerprint, face, iris) or behavioral (voice, gait, keystroke) traits for authentication. Compared to unimodal systems, which rely on a single trait and are more susceptible to spoofing and errors, multimodal systems offer higher accuracy, improved resilience, and enhanced security. Common combinations include fingerprint and facial recognition, or voice and iris verification, chosen based on user convenience and application context (Mohammed & Ali, 2024).

Biometric authentication can occur in several contexts: *in-person modalities* during physical presence or via video-based verification tools such as Zoom or Microsoft Teams, referred to as *remote in-person modalities*. Additionally, cross-border frameworks now permit biometric capture and verification without geographic limitations, supported by trusted authorities. These innovations expand the scope of secure, verifiable digital interactions while maintaining compliance with legal and ethical standards.

System Architecture

The proposed architecture integrates blockchain validation alongside multimodal biometric authentication to enable secure, decentralized, and intelligent multimedia distribution. This dual-layer framework addresses key weaknesses in distribution control, verification, and auditability. By leveraging blockchain for identity validation and incorporating multiple biometric traits—such as fingerprints and facial recognition—the system ensures

confidentiality, integrity, and robust access control across distributed digital environments (Salem et al., 2024).

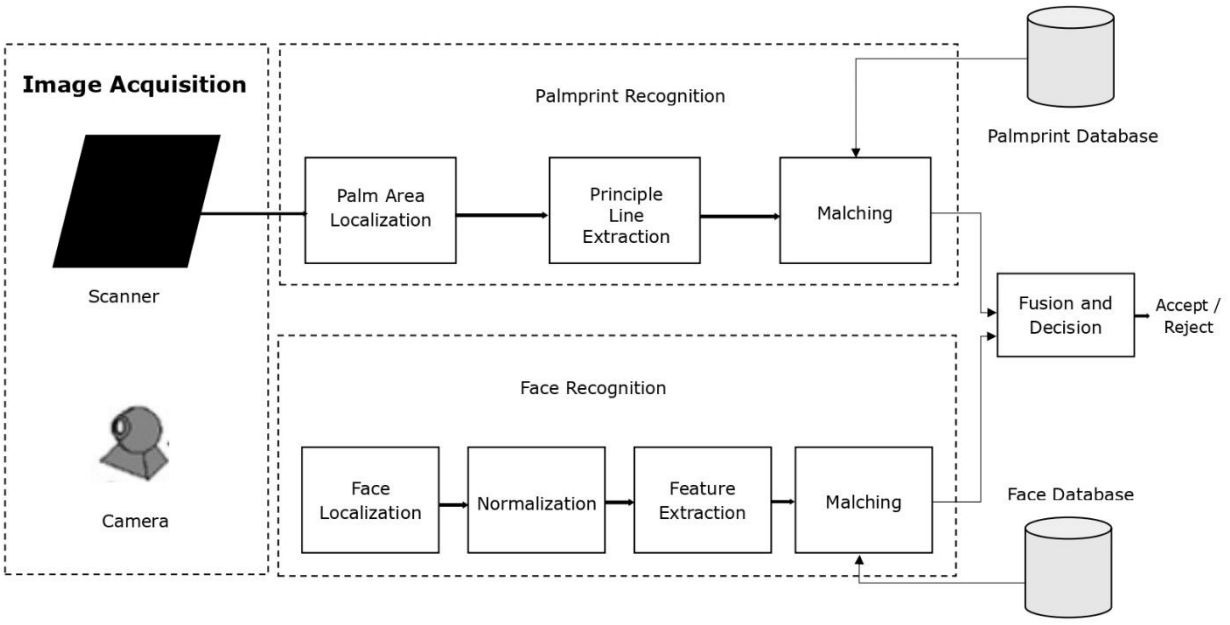

Figure 1. System Overview

System Implementation

As illustrated in Figure 1, the system follows a structured process encompassing registration, biometric capture, feature fusion, encryption, block validation, secure transmission, and final decryption of multimedia and blockchain data.

In the first stage, the user's facial and fingerprint biometrics are captured by the Multimodal Biometric Module. Facial data are processed using a lightweight Convolutional Neural Network (CNN), specifically *MobileNetV2*, known for producing efficient and accurate facial embeddings. Simultaneously, fingerprint images undergo enhancement using minutiae-based encoding and Gabor filtering to preserve ridge and pore details for reliable identity validation (Gudala et al., 2022).

The Feature Fusion Layer combines biometric vectors through score-level fusion, assigning adaptive weights based on the quality and reliability of each input. This generates a robust, composite proof of identity resistant to spoofing and false matches.

Next, the Encryption Engine uses a biometric fusion algorithm to derive a unique biometric key, which encrypts multimedia data with AES-256. Only the corresponding user can decrypt the content, ensuring that intercepted data remains inaccessible without matching biometric credentials.

A permissioned blockchain records metadata such as cryptographic hash values, automates access control, and logs all verification and interaction events via smart contracts—enhancing transparency and eliminating the need for central oversight.

Finally, at the Recipient Node, decryption occurs automatically once the provided biometrics match the regenerated identity key. This end-to-end architecture, supported by blockchain validation, guarantees that multimedia content remains both user-authenticated and blockchain-verified, effectively preventing unauthorized access and tampering (Verma et al., 2025).

Methodology

A mixed-methods approach combining theoretical modeling, simulation, and comparative analysis is used to evaluate the proposed system. Theoretical modeling defines the system architecture and explains interactions between biometric and encryption components integrated with blockchain. Simulations test system performance, resilience against attacks, and biometric accuracy under controlled conditions using synthetic datasets and attack scenarios (Soni et al., 2022). Finally, comparative analysis assesses system performance against existing authentication and data integrity models, emphasizing integration, transmission efficiency, and reliability.

Biometric Data Acquisition & Fusion

Biometric acquisition begins with capturing facial and fingerprint data, processed through specialized algorithms to extract distinctive features. Facial recognition employs a MobileNetV2-based Convolutional Neural Network (CNN) for efficient encoding of spatial and geometric features. Simultaneously, fingerprint recognition uses minutiae-based analysis and Gabor filtering to enhance ridge and pore clarity while reducing noise (Wahab et al., 2024).

The collected data undergo score-level fusion, where the system assigns confidence-based weights to facial and fingerprint matchers, generating a unified authentication score. This weighted fusion minimizes false acceptance and rejection rates, improves overall accuracy, and enhances usability—balancing security with convenience for end users.

Blockchain Integration

Blockchain serves as a decentralized trust layer, enhancing transparency, traceability, and immutability in multimedia transmission. Smart contracts deployed on the Ethereum testnet manage user authentication, access control, and data ownership.

During each transmission, the user is authenticated via multimodal biometrics. Once verified, the system encrypts the multimedia file using a biometric-generated key (Moradiet al., 2022). A digital signature—comprising a cryptographic hash, metadata, and access permissions—is recorded on the blockchain as an immutable block. Each block contains details such as user identity, time, date, and receiver information. Any unauthorized alteration or access attempt becomes immediately auditable.

This decentralized structure eliminates single points of failure typical of centralized authentication systems, ensuring stronger data integrity and transparent access management.

Security Model

Comprehensive attack simulations were conducted to evaluate the system's robustness against various cyber threats. These included user spoofing through fake biometrics, interception or modification of multimedia data, and attempts to exfiltrate decryption keys. The framework consistently maintained data confidentiality, integrity, and access control throughout all simulations (Omotunde & Ahmed, 2023).

Results confirm that integrating blockchain with biometric encryption mitigates vulnerabilities common in traditional systems, providing a secure, tamper-resistant environment for multimedia transmission and authentication.

Results

To analyse the proposed framework of Blockchain-Based Smart Multimodal Biometric Multimedia Transmission, it was subjected to the rigours of simulation modelling to ascertain its authentication precision, security, and overall reliability. The simulations employed single biometric systems, face and fingerprint recognition, and compared them against the proposed model integrating multiple biometric systems.

It can be seen from the results in Table 1 that the improvement in recognition performance is due to the application of multimodal fusion systems. The fingerprint model obtained an accuracy of 94.4 with an FAR of 2.1 and an FRR of 3.5; the model is infinitely better than nothing. The face model achieves an accuracy of 93.8 due to light imbalance, expression variations, and deterioration of the image, accompanied by FAR and FRR, but it is achievable. On the other hand, the multimodal biometric system demonstrates an accuracy of 98.7, with FAR and FRR of 0.8 and 1.3, respectively, and sheer performance. These results confirm the fusion of fingerprint and facial features to overcome spoof attacks and attain noise robustness (Jomaa, Islam, Mathkour, & Al-Ahmadi, 2022).

Table 1. Authentication Accuracy

Biometric Type	FAR (%)	FRR (%)	Accuracy (%)
Fingerprint only	2.1	3.5	94.4
Face only	3.0	4.2	93.8
Multimodal (fusion)	0.8	1.3	98.7

Alongside biometric operation outcomes, the integration with the blockchain was also evaluated for the completeness of tracing and auditing multimedia transactions. An example of a log record for blockchain transactions is illustrated in Figure 2, depicting all the events of the transmission of the content with the corresponding stored cryptographic hash, timestamp, and verification status. This record is tamper-proof, and thus any attempts at unauthorised access will be instantaneously flagged (Khumalo et al., 2024).

The security threat assessment in Table 2 reveals the decisive benefits of the proposed architecture in comparison to traditional omnipotent silo systems. Conventional systems are still prone to spoofing, replay, and other attacks, while the proposed architecture with the blockchain diminishes risk potentials through decentralization, immutable documenting log systems, and biometric fusion keying. Additionally, breaches of prohibitive access are much lower than in traditional systems, which explains the strength of the hybrid security. In essence, the analysis illustrates that the proposed architecture not only advances authentication accuracy but also significantly enhances the reliability and security of multimedia transmission.

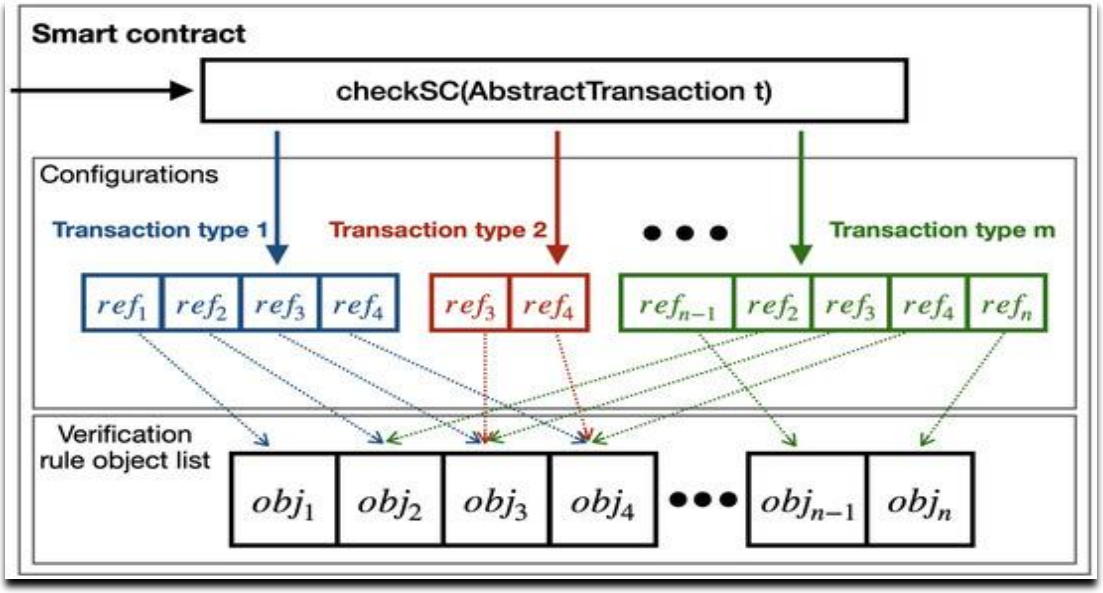

Figure 2. Blockchain Transaction Log

Table 2. Security Threat Evaluation

Threat Type	Traditional System	Proposed System
Spoofing	Vulnerable	Resilient
Replay Attacks	Moderate Risk	Low Risk
Data Tampering	High Risk	Negligible
Unauthorized Access	Frequent	Rare

Discussion

In the proposed architecture, integrating multimodal biometric authentication with blockchain technology provides an improvement over traditional systems with single-mode biometric and central architecture circuits. The system performs better due to the combined use of fingerprint and facial recognition, showing improved accuracy, spoofing resistance, and inclusivity towards different user classes. The combined use of biometric modalities lowers the false acceptance and rejection rates, thus improving the system's operational and environmental robustness. Additionally, the system ensures maximum end-to-end content protection, since biometric-derived cryptographic keys are used to uniquely secure every transmission session.

In the blockchain domain, the framework utilises the immutability, distributed consensus, and transparency of blockchain technology to enforce data integrity and auditability. Smart contracts provide rule-based automated access control, while content hashes and associated metadata are stored permanently on-chain for tamper-evident validation. This distributed system architecture removes the dependency on an individual trusted third party, thus improving the overall security and internal threat resilience of the system due to the absence of a single point of failure (Berger et al., 2021).

Though blockchain technology has many applications and benefits, several obstacles need to be overcome, particularly when storing and processing large and complex multimedia files. Concerns include the speed at which the blockchain records transactions and how expensive a real-time application would be to run. Compounding these, biometric fusion processing is complex and could lead to long system delays, which would affect the overall user application, particularly on resource-limited devices. Final primary concerns are the compliance with the regulations of the General Data Protection Regulation (GDPR), particularly while collecting sensitive biometric data, and the processes complying with global data privacy regulations (Bertolaccini et al., 2023).

In the subsequent integration of research, we hope to utilise and access the Interplanetary File System (IPFS) to assign decentralised and multimedia storage, which would address blockchain bandwidth concerns. Other future directions include behavioural biometrics (such as keystroke dynamics and gait biometrics) to strengthen and enhance the usability of the

system within highly dynamic variations, as well as edge-based inference models to facilitate rapid, real-time biometric processing for mobile and IoT devices.

Conclusion

The proposed system integrates multimodal biometric authentication systems with blockchain validation for securing multimedia content during transmission using biometric-based encryption keys, which provides confidentiality, auditability, and traceability for multimedia data transfers. The incorporated biometric systems are harder to spoof and impersonate due to the improved performance synergy gained from the fusion of fingerprint and face biometric systems. Hypothetically, the proposed framework resolves the critical and evolving security issues with the transmission of multimedia content during the use of fingerprint and face recognition biometrics through the encrypted blockchain system.

This, in an age of increasing sophistication in cyber threats, data breaches, and blockless cyber vulnerability, gives a framework for secure and decentralised real-time communication with layered access control. The framework reduces the shortcomings of security systems that are reliant on a single biometric or password. As a result, the system would foster the next generation of security systems, which are primarily focused on trust, privacy, and scalability. This is particularly true for mobile systems and in cases where cloud-based technology is employed.

Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Alhudhud, G., Alsaeed, D., & Alsaeed, R. (2023). Secure multimedia exchange using voice biometric-based system. *Advanced Studies Euro-Tbilisi Mathematical Journal*.

Aswathy, S. U., & Tyagi, A. K. (2022). Privacy breaches through cyber vulnerabilities: Critical issues, open challenges, and possible countermeasures for the future. In *Security and privacy-preserving techniques in wireless robotics* (pp. 163-210). CRC Press.

Berger, C., Eichhammer, P., Reiser, H. P., Domaschka, J., Hauck, F. J., & Habiger, G. (2021). A survey on resilience in the IoT: Taxonomy, classification, and discussion of resilience mechanisms. *ACM Computing Surveys (CSUR)*, *54*(7), 1-39.

Bertolaccini, L., Falcoz, P. E., Brunelli, A., Batirel, H., Furak, J., Passani, S., & Szanto, Z. (2023). The significance of general data protection regulation in the compliant data contribution to the European Society of Thoracic Surgeons database. *European Journal of Cardio-Thoracic Surgery*, *64*(3), ezad289.

Dick, L., & Wessel, J. (2023). *The duality of transparency in strategic communication: Reputation management during a crisis in the social media industry*. [Publisher/Institution if available].

Gudala, L., Reddy, A. K., Sadhu, A. K. R., & Venkataramanan, S. (2022). Leveraging biometric authentication and blockchain technology for enhanced security in identity and access management systems. *Journal of Artificial Intelligence Research*, *2*(2), 21-50.

Jomaa, R. M., Islam, M. S., Mathkour, H., & Al-Ahmadi, S. (2022). A multilayer system to boost the robustness of fingerprint authentication against presentation attacks by fusion with heart-signal. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5132-5143.

Khumalo, N. M., Nleya, S. M., Marabada, N., Ndlovu, S., Dube, S. S., & Ncube, N. (2024, November). *Tamper-resistant document management system integrated with blockchain technology*. Paper presented at the 2024 3rd Zimbabwe Conference of Information and Communication Technologies (ZCICT), IEEE.

Kothinti, R. R. (2024). Artificial intelligence in healthcare: Revolutionizing precision medicine, predictive analytics, and ethical considerations in autonomous diagnostics. *World Journal of Advanced Research and Reviews*, *19*(3), 3395-3406.

Mohammed, S. M., & Ali, O. (2024). Human biometric identification: Application and evaluation. *International Journal of Engineering and Computer Science (IJECS)*, *6*(2), 131-152.

Moradi, M., Moradkhani, M., & Tavakoli, M. B. (2022). A real-time biometric encryption scheme based on fuzzy logic for IoT. *Journal of Sensors*, *2022*, Article 4336822.

Omotunde, H., & Ahmed, M. (2023). A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. *Mesopotamian Journal of CyberSecurity*, *2023*, 115-133.

Sadeghi, Z. , Jahanyan, S. and Shahin, A. (2023). Mapping the Interactive Model of Relationships between Blockchain-Related Variables in the Green Supply Chain: DEMATEL-ISM Approach. *Industrial Management Journal*, 15(2), 244-271. doi: 10.22059/imj.2023.350889.1008001

Salem, S. H. G., Hassan, A. Y., Moustafa, M. S., & Hassan, M. N. (2024). Blockchain-based biometric identity management. *Cluster Computing*, *27*(3), 3741-3752.

Soni, P., Pradhan, J., Pal, A. K., & Islam, S. H. (2022). Cybersecurity attack-resilience authentication mechanism for intelligent healthcare system. *IEEE Transactions on Industrial Informatics*, *19*(1), 830-840.

Verma, A., Bhardwaj, A., & Kumar, A. (2025, July). *An integrated blockchain-based framework for enhancing security and transparency in video conferencing*. Paper presented at the 2025 International Conference on Computing Technologies & Data Communication (ICCTDC), IEEE.

Wahab, A., Khan, T. M., Iqbal, S., AlShammari, B., Alhaqbani, B., & Razzak, I. (2024). Latent fingerprint enhancement for accurate minutiae detection. *Procedia Computer Science*, *246*, 1558-1567.

Bibliographic information of this paper for citing:

Alhudhud, Ghada & Al-Akaidi, Marwan (2026). Blockchain-Based Smart Multimodal Biometric Multimedia Transmission. *Journal of Information Technology Management*, 18 (2), 110-119. https://doi.org/10.22059/jitm.2026.107233