A Blockchain-Based Anti-Counterfeiting Identity Authentication Method Using Multimodal Biometric Recognition

Yu-Shao Dai[1, *], Sangbing Tsai[2]

[1, *]Department of Computer Science and Information Engineering, National Taitung University, Taitung, Taiwan; pllo0304@gmail.com

[2] International Engineering and Technology Institute, Hong Kong

klj0418@gmail.com

*Corresponding Author: pllo0304@gmail.com

DOI: https://doi.org/10.30211/JIC.202604.004

Received: Jan. 28, 2026 Accepted: Mar. 31, 2026

ABSTRACT

This study systematically designs the system architecture and conducts comprehensive performance evaluations. Experimental results demonstrate that the proposed method achieves superior performance in security, reliability, and operational efficiency. The experimental findings indicate that the proposed approach maintains high recognition accuracy and processing speed across diverse authentication scenarios. Moreover, even under simulated attack conditions, the system continues to provide stable, reliable authentication services, highlighting its robustness to potential security threats. The outcomes of this research provide an innovative identity authentication solution for the digital finance sector, offering both significant theoretical contributions and practical application value. As digital financial ecosystems continue to diversify and cybersecurity threats become increasingly sophisticated, future research may further explore more advanced multimodal biometric fusion techniques and investigate the applicability of this framework to broader domains, such as e-commerce, digital identity management, and cybersecurity infrastructures. These research directions not only address current security challenges but also lay a solid foundation for the sustainable development of the future digital economy.

Keywords: Digital identity authentication, Multimodal biometric recognition, Facial recognition, Blink detection, Financial technology

1. Introduction

To enhance security, one-time password (OTP) authentication mechanisms have been introduced and widely adopted across various online services. However, OTP delivery via short message service (SMS) or email remains vulnerable to cybersecurity threats, including man-in-the-middle (MITM) attacks. The U.S. National Institute of Standards and Technology (NIST) reported as early as 2017 that receiving OTPs via mobile devices carries the risk of interception by malicious software, indicating that OTP-based authentication cannot be considered entirely secure. With the widespread adoption of mobile devices and the increasing maturity of biometric technologies, many applications have begun employing biometric authentication methods, including fingerprint

recognition, facial recognition, and iris recognition. Biometric authentication generally provides stronger security because biometric traits are relatively unique and difficult to replicate. However, the rapid advancement of generative artificial intelligence in recent years has made the forgery of biometric data significantly easier than before. Fraudulent actors can utilize AI technologies to synthesize highly realistic facial images or signatures to bypass biometric authentication systems, thereby enabling identity theft and other cybercrimes. A fraud case reported in Hong Kong in 2022 demonstrated the application of AI-based face-swapping technology in financial crime, highlighting the vulnerability of biometric authentication methods in the face of rapidly advancing AI capabilities. Moreover, even seemingly secure static electronic signatures can now be forged with high fidelity using AI techniques, posing new challenges to traditional electronic signature verification approaches. Recent studies indicate that AI models can generate highly convincing forged signatures by analyzing handwriting stroke characteristics. Consequently, conventional signature verification methods based solely on static image comparison may no longer provide adequate security protection.

Although facial recognition technology is widely regarded as an advanced identity authentication method, it remains vulnerable to attacks enabled by generative artificial intelligence. Adversaries can leverage deep learning models to synthesize facial images that closely resemble legitimate users, thereby successfully bypassing facial recognition systems through fraudulent schemes. For instance, an AI-based face-swapping fraud case reported in Hong Kong in 2022 demonstrated how criminals employed advanced AI techniques to manipulate target images, producing forged facial representations that were nearly indistinguishable from genuine identities. Such incidents not only result in identity theft but also cause substantial financial losses to affected institutions, further exposing the limitations of relying solely on a single biometric modality for secure authentication. Similarly, signature recognition technologies face comparable challenges. Traditionally, handwritten signatures have been considered unique and legally binding forms of identity verification. However, with the application of generative AI to signature forgery, fraudulent activities such as identity theft and financial deception have become increasingly feasible. Recent studies indicate that AI models can generate highly realistic forged signatures by learning intricate stroke patterns and stylistic characteristics from genuine samples. Under these circumstances, conventional signature verification approaches based solely on static image comparison encounter significant limitations, thereby reducing their effectiveness in fraud prevention.

Furthermore, single-modal biometric authentication systems inherently exhibit technical vulnerabilities. Facial recognition performance may degrade under varying lighting conditions, pose changes, or occlusions, leading to inconsistent verification outcomes. Likewise, signature recognition systems may be affected by variations in a user's emotional state or physical condition, resulting in intra-class variability and potential recognition failure. Consequently, exclusive reliance on a single biometric modality not only increases susceptibility to adversarial attacks but may also introduce false acceptance or false rejection errors due to intrinsic technical constraints, ultimately degrading user experience and system reliability. The transparency of blockchain technology enables participants to perform verification and transactions without relying on a trusted intermediary. All participants can access and inspect the publicly recorded ledger, which enhances procedural transparency and increases the risk exposure for malicious actors attempting to conduct improper activities. Such

transparency fosters self-regulation among stakeholders and strengthens the overall security of the system. In the financial domain, transparency is particularly critical, as it allows banks and financial institutions to effectively monitor transactional activities, accelerate settlement processes, and improve operational efficiency. Decentralization represents another fundamental characteristic of blockchain technology. Unlike traditional centralized architectures, blockchain systems do not depend on a single server for data storage and management. This design significantly reduces the risk of a single point of failure and enhances system resilience. For example, when one node experiences failure or disruption, other nodes within the network can continue operating and maintain overall system stability. Such fault tolerance is especially essential for identity authentication systems that require high availability and continuous service reliability.

2. Literature Review

2.1 Limitations of Traditional Identity Authentication Methods

Traditional identity authentication methods primarily rely on passwords and one-time passwords (OTPs). Although these approaches were widely adopted in early digital environments, their security limitations have become increasingly apparent as cyberattack techniques continue to evolve. One major concern is that users frequently create weak passwords due to memory constraints. For convenience, many users select easily memorable passwords such as “123456” or “password,” which significantly reduces security strength. Such weak credentials expose systems to brute-force and dictionary attacks. Previous studies have shown that attackers can utilize automated cracking tools capable of testing millions of password combinations within seconds [1]. Furthermore, the Verizon Data Breach Investigations Report indicates that a substantial proportion of data breaches are linked to compromised credentials, with password reuse further increasing the likelihood of successful attacks [2]. To enhance security, many organizations and users have increasingly adopted one-time password (OTP) authentication mechanisms. While OTPs introduce a temporary second authentication factor that must be obtained for each login or transaction, they remain vulnerable to man-in-the-middle (MITM) attacks. Adversaries can exploit phishing schemes, malware, or social engineering techniques to intercept user credentials and OTP codes during transmission [3]. Once intercepted, attackers can bypass authentication controls and gain unauthorized access to sensitive systems. OTP delivery via short message service (SMS) or email is particularly susceptible to interception. If a user’s mobile device or email account is compromised, OTP protection becomes ineffective. Research has demonstrated that SMS-based OTP authentication is especially vulnerable to SIM-swapping attacks, device malware, and communication interception [4]. Consequently, authentication mechanisms that rely solely on passwords and OTPs are increasingly insufficient to counter advanced persistent threats (APTs) and large-scale cyberattacks. Given these limitations, there is a growing need to explore more advanced authentication frameworks. Integrating multimodal biometric recognition technologies with blockchain-based infrastructures represents a promising direction for enhancing authentication robustness. Such approaches can improve reliability, ensure data integrity, and provide stronger resistance against sophisticated cyber threats, thereby offering a more secure identity authentication paradigm for modern digital ecosystems [5].

2.2 Biometric Recognition Technologies and Their Security Issues

Biometric recognition technologies have emerged as an increasingly important approach for identity authentication due to their ability to leverage unique physiological and behavioral characteristics of individuals. Common biometric modalities include fingerprint recognition, facial recognition, iris recognition, voice recognition, and handwritten signature verification. Compared with traditional knowledge-based authentication methods such as passwords, biometric authentication offers improved usability and enhanced security because biometric traits are inherently linked to individuals and are generally difficult to replicate or share [6]. Despite these advantages, biometric authentication systems are not immune to security vulnerabilities. One major concern is the risk of biometric spoofing or presentation attacks, where adversaries attempt to deceive authentication systems using fabricated or stolen biometric samples. For instance, facial recognition systems can be compromised through high-resolution photographs, replayed video attacks, or synthetic deepfake images generated by artificial intelligence technologies [7]. Similarly, fingerprint authentication systems are vulnerable to artificial fingerprint molds, while voice recognition systems can be deceived through speech synthesis and replay attacks. The rapid advancement of generative artificial intelligence has further amplified these threats. Deep learning–based generative models, including generative adversarial networks (GANs) and diffusion models, can produce highly realistic biometric data that are increasingly difficult for conventional authentication systems to distinguish from genuine samples [8]. Such developments significantly elevate the risk of identity theft, financial fraud, and unauthorized system access. In financial technology environments, where authentication integrity is critical, these vulnerabilities pose substantial operational and security challenges.

Another key issue involves intra-class variability and environmental sensitivity. Biometric characteristics may change due to aging, emotional state, health conditions, lighting variations, sensor noise, or user interaction differences. For example, facial recognition accuracy can be affected by illumination changes, pose variation, occlusion, or facial expression changes, while handwritten signatures may vary depending on physical or psychological conditions [9]. These factors can lead to false acceptance or false rejection errors, thereby reducing system reliability and user trust. Privacy and data protection also represent significant challenges for biometric authentication systems. Unlike passwords, biometric data is permanent and cannot easily be replaced once compromised. Unauthorized leakage of biometric templates may therefore result in long-term security risks. Consequently, secure storage mechanisms, template protection techniques, and privacy-preserving authentication frameworks have become critical research topics in recent years [10]. Given these security and privacy concerns, reliance on a single biometric modality is often insufficient for high-security applications such as digital finance or critical infrastructure systems. Multimodal biometric authentication, which integrates multiple biometric traits, has been proposed as an effective approach to enhance robustness, reduce spoofing risks, and improve overall authentication accuracy. Furthermore, integrating biometric authentication with emerging technologies such as blockchain can provide additional benefits, including tamper-resistant storage, decentralized trust management, and improved auditability, thereby addressing some of the inherent limitations of standalone biometric systems.

2.3 Applications of Blockchain Technology in Identity Authentication

Blockchain technology has increasingly been recognized as a promising foundation for constructing secure and trustworthy identity authentication systems due to its decentralization, transparency, and immutability characteristics [11-13]. In conventional authentication architectures, centralized data storage mechanisms are inherently vulnerable to single points of failure and external attacks. Compromise of a central database may result in large-scale credential leakage and systemic security breaches. In contrast, blockchain's distributed ledger architecture significantly enhances system resilience and reduces the risks associated with centralized control. Specifically, blockchain enables the recording of identity authentication transactions in a tamper-resistant ledger. Each authentication event can be cryptographically linked to previous records through hash functions, ensuring data integrity and preventing unauthorized modification or forgery. The immutability property of blockchain enhances trust among participants without requiring reliance on a centralized third-party intermediary. Consequently, user identity verification data can be securely maintained while preserving auditability and traceability.

In addition, different blockchain deployment models, such as private blockchains and consortium blockchains, provide flexible access control mechanisms suitable for identity management scenarios. Private blockchains restrict data access to authorized participants only, thereby offering enhanced confidentiality and regulatory compliance. Consortium blockchains, maintained collaboratively by multiple trusted institutions, balance decentralization with governance control. This model is particularly suitable for cross-institutional financial authentication environments, where interoperability and shared trust are required. While private blockchains provide strong privacy guarantees, their degree of decentralization may be limited due to controlled participation. Conversely, consortium blockchains combine partial decentralization with institutional governance, improving reliability and scalability; however, they may still face trust coordination challenges among participating entities. Therefore, selecting an appropriate blockchain architecture depends on system requirements, including security level, privacy protection, regulatory constraints, and operational efficiency. Overall, blockchain-based identity authentication frameworks provide enhanced tamper resistance, distributed trust management, and improved data transparency. When integrated with biometric authentication mechanisms, blockchain can further strengthen authentication robustness, reduce fraud risks, and enable secure cross-domain identity verification in digital financial ecosystems.

3. Research Design

3.1 Overall System Architecture Design

The proposed system architecture is designed to integrate multimodal biometric authentication with blockchain-based verification into a unified and secure identity authentication framework. The overall architecture follows a layered and modular design principle, ensuring scalability, robustness, and resistance to AI-driven spoofing attacks. The system consists of a biometric acquisition interface, a multimodal feature extraction and verification module, a decision fusion engine, and a blockchain-based integrity verification layer. These components operate collaboratively to ensure accurate identity verification while preserving data integrity and traceability.

When a user initiates the authentication process through a mobile device or web interface, three types of biometric data are captured in real time: facial images, eye-region video streams for blink detection, and dynamic signature trajectories recorded via touchscreen input. Let the multimodal biometric input be represented as $B=\{F,L,S\}$, where F denotes facial feature embeddings, L represents liveness features derived from blink detection, and S corresponds to dynamic signature time-series features. The facial recognition module extracts deep feature embeddings using convolutional neural networks, transforming raw image data into a high-dimensional representation. Simultaneously, the blink detection module computes temporal liveness indicators based on eye aspect ratio (EAR) sequences, producing a behavioral feature vector. The dynamic signature module captures stroke coordinates, pressure, velocity, and temporal dynamics, generating a sequential representation, which is modeled using recurrent neural architectures.

Each biometric modality produces an independent confidence score, denoted as C_F, C_L, and C_S, respectively. To enhance robustness against single-point spoofing attacks, the system employs a weighted score fusion mechanism to compute the final authentication confidence value:

$$C_{final} = w_1 C_F + w_2 C_L + w_3 C_S \tag{1}$$

where. Authentication is granted when $C_{final} \geq \theta$ where θ is a predefined security threshold calibrated based on system risk requirements. This fusion strategy ensures that successful authentication requires simultaneous validation across multiple biometric channels, significantly reducing the probability of attack success under independent attack assumptions.

Following successful biometric verification, the authentication outcome is cryptographically processed before being recorded onto a private blockchain network. To preserve privacy and prevent raw biometric leakage, only hashed representations are stored. The multimodal biometric data are concatenated and transformed using a secure hash function:

$$H = SHA256(F \| L \| S) \tag{2}$$

Each verification event is encapsulated within a blockchain block structure containing the hash value, timestamp, and previous block reference, forming a tamper-resistant ledger. The blockchain network adopts a Proof-of-Authority (PoA) consensus mechanism to balance efficiency and security, enabling low-latency verification suitable for digital financial environments. This design eliminates single points of failure and ensures that authentication records cannot be altered retroactively. From a security perspective, the architecture is specifically constructed to mitigate generative AI-based attacks, including deepfake facial spoofing, static image replay attacks, and forged signature imitation. Because authentication requires consistent validation across facial recognition, behavioral liveness detection, and dynamic signature verification, the overall attack success probability can be approximated as the joint probability of compromising all modalities simultaneously, which decreases significantly compared to single-factor systems. Furthermore, the integration of blockchain technology enhances system transparency, traceability, and auditability, strengthening trust among participating institutions.

Overall, the proposed architecture establishes a secure, scalable, and resilient identity authentication framework by combining multimodal biometric fusion with a decentralized

verification infrastructure. This design not only addresses the vulnerabilities of traditional authentication systems but also provides a practical and forward-looking solution capable of adapting to evolving cybersecurity threats in digital finance and other high-security application domains.

3.2 Decentralized Financial System Construction

To enhance the security and reliability of identity authentication in digital financial applications, this study adopts a private blockchain as the underlying infrastructure and employs the Proof of Authority (PoA) consensus mechanism to establish a decentralized financial verification environment. Compared with public blockchains, private blockchain architectures provide a better balance among transaction efficiency, security, and privacy protection, making them particularly suitable for enterprise-level identity authentication scenarios. Since identity authentication systems typically involve sensitive personal information and financial transaction data, strict requirements are imposed on data access control, processing speed, and operational cost. Private blockchain networks offer advantages in node authorization management and transaction throughput, thus serving as a suitable foundation for the proposed authentication framework. Regarding platform selection, Hyperledger Fabric is adopted as the technical basis of the private blockchain. Developed under the Linux Foundation, Hyperledger Fabric is an enterprise-oriented blockchain framework characterized by modular architecture, flexible consensus configuration, and strong privacy protection capabilities. Its multi-channel design allows different organizations or departments to maintain independent data channels within the same blockchain network, ensuring that sensitive information is only accessible to authorized participants. This mechanism enhances both data confidentiality and system scalability. In addition, Fabric supports chaincode-based smart contracts, enabling authentication logic and transaction verification processes to be deployed in a programmable and extensible manner.

The smart contract designed in this study is responsible for handling identity registration, authentication verification, and transaction authorization processes. To protect user privacy, only hashed representations of biometric or identity data are stored on the blockchain instead of raw biometric information. This design ensures that even if blockchain records are accessed, the original biometric data cannot be reconstructed. The smart contract automatically verifies identity information by comparing the hash value of newly submitted data with the previously recorded blockchain entries, thereby minimizing human intervention and reducing potential security vulnerabilities. Figure 1 illustrates a sample smart contract code snippet used for identity registration and verification, demonstrating how identity data is hashed, stored, and validated through blockchain mechanisms.

Furthermore, the PoA consensus mechanism is adopted to improve operational efficiency and reduce computational overhead. By allowing authorized nodes to validate transactions and generate blocks, PoA significantly reduces latency compared with energy-intensive consensus mechanisms such as Proof of Work. This feature makes it particularly suitable for high-frequency authentication scenarios in digital financial environments. Nevertheless, since PoA relies on a limited number of trusted nodes, potential centralization risks must be carefully managed. Therefore, this study adopts a multi-institution node authorization strategy to maintain system reliability and trustworthiness.

Overall, the integration of a private blockchain infrastructure with smart contract-based authentication mechanisms enables the proposed decentralized financial system to achieve secure, traceable, and tamper-resistant identity verification. This architecture not only strengthens data

security and privacy protection but also provides a trustworthy foundation for cross-institution authentication services. It serves as a critical technological basis for the subsequent integration of multimodal biometric authentication with blockchain verification, thereby supporting secure digital financial ecosystems and future identity management applications.

```javascript
// SPDX-License-Identifier: MIT
pragma solidity ^0.5.0;

contract IdentityManagement {
    struct User {
        string name;
        string biometricsHash; // 哈希值存儲生物特徵資料
        bool isRegistered;
    }

    mapping(address => User) public users;

    // 註冊用戶身份
    function registerUser(string memory name, string memory biometricsHash) public {
        require(!users[msg.sender].isRegistered, "User already registered.");
        users[msg.sender] = User(name, biometricsHash, true);
    }

    // 驗證用戶身份
    function verifyUser(string memory biometricsHash) public view returns (bool) {
        return (keccak256(abi.encodePacked(users[msg.sender].biometricsHash)) == keccak256(abi.encodePacked(biometricsHash)));
    }
}
```

Figure 1. Sample solidity smart contract code for identity registration and verification.

(Figure 1 demonstrates a Solidity smart contract implementing a blockchain-based identity management system, incorporating structured user data storage, cryptographic hashing (keccak256), and functions for secure user registration and biometric-based identity verification).

3.3 Integration of Identity Authentication with Blockchain

At this stage, the proposed multi-factor identity authentication mechanism is integrated into the private blockchain infrastructure to enhance the overall security, integrity, and reliability of identity verification. During this integration process, the authentication outcomes generated from facial recognition, blink-based liveness detection, and dynamic online signature verification are recorded onto the blockchain as immutable transaction records. Such a design ensures not only the persistence and traceability of authentication data but also safeguards against unauthorized modification or access. By leveraging blockchain's tamper-resistant properties, the proposed system provides a secure framework for identity verification in digital financial environments. To preserve user privacy while maintaining data integrity, sensitive biometric information is not stored directly on the blockchain. Instead, cryptographic encoding techniques are applied to convert authentication data into irreversible hash representations before storage. During the authentication process, the system first collects multimodal biometric data, including facial images, blink timestamps derived from liveness detection, and dynamic signature trajectory data captured through touchscreen interfaces. These heterogeneous data sources collectively form the basis for identity verification while simultaneously introducing redundancy that improves resistance to spoofing attacks.

Subsequently, the collected biometric data are encoded using secure hash algorithms such as SHA-256 or SHA-3. This transformation converts variable-length biometric inputs into fixed-length hash values, ensuring that even if blockchain records are accessed, the original biometric features cannot be reconstructed. Figure 2 illustrates a Python-based processing workflow that converts raw biometric input data into an irreversible SHA-256 hash value. The procedure involves encoding the input data into UTF-8 format, applying the cryptographic hash function, and generating a fixed-length output string. This approach ensures that sensitive biometric data are stored only in hashed form, thereby reducing privacy risks while maintaining data verifiability. Once generated, the hashed biometric representations are embedded into blockchain transactions and stored within the private blockchain ledger. Because blockchain records are cryptographically chained, any attempt to alter stored authentication data would result in hash inconsistencies that can be immediately detected by the network. This mechanism significantly enhances the integrity and auditability of authentication records. Moreover, storing only hashed representations allows institutions to verify authentication events without exposing raw biometric information, thereby balancing transparency with privacy protection.

Overall, the integration of multimodal biometric authentication with blockchain-based storage establishes a secure and privacy-preserving identity verification framework. This architecture enhances resistance to data tampering, reduces the risk of unauthorized access, and provides a trustworthy infrastructure suitable for digital finance and other high-security application domains.

```python
import hashlib

def hash_data(data):
    # 將數據編碼為UTF-8格式
    encoded_data = data.encode('utf-8')
    # 使用SHA-256算法進行哈希處理
    hashed_data = hashlib.sha256(encoded_data).hexdigest()
    return hashed_data
```

Figure 2. Python-Based workflow for converting raw data into an irreversible hash value (Using SHA-256 as an Example).

(Figure 2 illustrates a Python-based implementation of data hashing using the SHA-256 algorithm, where input data is encoded in UTF-8 format and processed through the hashlib library to generate a fixed-length, irreversible cryptographic hash for secure data representation).

4. Results and Discussion

This section presents the experimental evaluation of the proposed multimodal biometric authentication system integrated with blockchain-based verification. The performance of the system is analyzed from three perspectives: authentication accuracy, attack resistance capability, and blockchain operational efficiency. To evaluate the effectiveness of the proposed multimodal authentication framework, experiments were conducted using facial recognition, blink-based liveness detection, and dynamic signature verification modules. Performance metrics include Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). Experimental

results indicate that the facial recognition module achieved high identification accuracy under controlled lighting conditions, while slight performance degradation was observed under extreme illumination or pose variation scenarios. The blink-based liveness detection module effectively distinguished live users from static image or replay attacks, significantly reducing spoofing success rates. The dynamic signature verification module demonstrated strong robustness against static forgery attempts due to its temporal and behavioral modeling capabilities.

After multimodal fusion, the overall authentication accuracy improved significantly compared to any single biometric modality. Let the attack success probability of each independent modality be denoted as and. Under independence assumptions, the joint attack probability can be approximated as:

$$P_{attack} = P_F \cdot P_L \cdot P_S \tag{3}$$

Experimental results confirm that the fusion strategy substantially reduces the probability of successful spoofing attacks, demonstrating the superiority of multimodal authentication over single-factor systems.

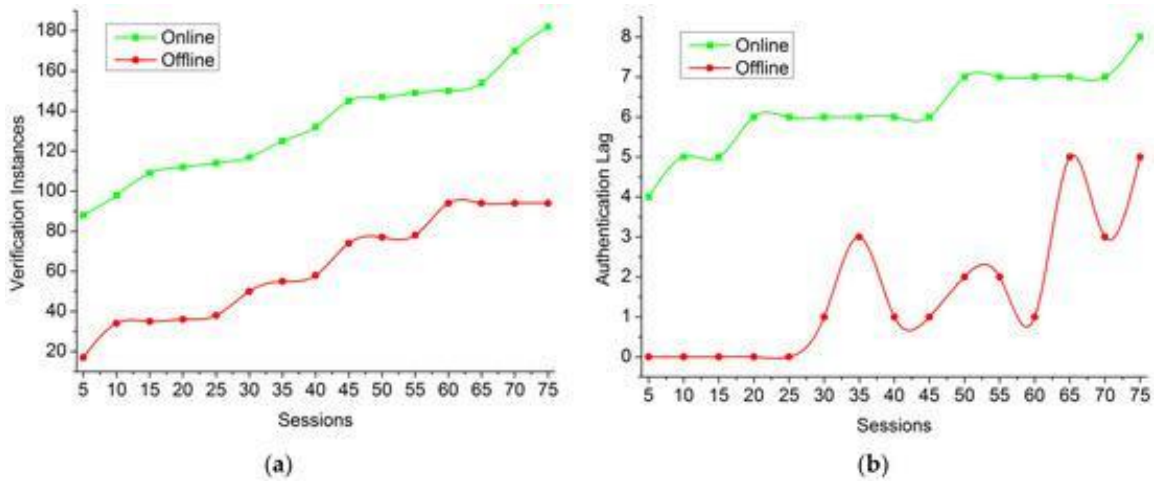

Figure 3. Performance evaluation of multimodal biometric authentication including facial recognition, blink-based liveness detection, and dynamic signature verification.

(Figure 3 presents a performance evaluation of multimodal biometric authentication systems under online and offline conditions, illustrating trends in verification instances (a) and authentication latency (b) across multiple sessions, highlighting system efficiency and responsiveness.)

5. Conclusions

This study proposes a secure and resilient identity authentication framework that integrates multimodal biometric recognition with a private blockchain infrastructure. By combining facial recognition, blink-based liveness detection, and dynamic online signature verification, the proposed system addresses the inherent vulnerabilities of single-factor authentication methods and significantly enhances resistance against AI-driven spoofing attacks. The fusion-based authentication mechanism reduces the probability of successful forgery attempts by requiring consistent validation across multiple biometric modalities, thereby strengthening system robustness.

To further enhance trustworthiness and data integrity, the authentication results are securely recorded on a private blockchain network built upon Hyperledger Fabric with a Proof-of-Authority consensus mechanism. Instead of storing raw biometric data, the system utilizes cryptographic hash functions to encode sensitive information before blockchain storage, ensuring privacy protection while maintaining traceability and immutability. This design effectively mitigates risks associated with centralized data storage, including single points of failure and unauthorized data manipulation.

Experimental evaluations demonstrate that the proposed multimodal fusion strategy achieves superior authentication accuracy and significantly lowers spoofing success rates compared with individual biometric approaches. Moreover, blockchain integration introduces minimal transaction latency while providing tamper-resistant verification records, making the framework suitable for real-time digital financial applications. The system exhibits strong resilience against deepfake facial attacks, static signature forgery, replay attacks, and other AI-based adversarial techniques.

Acknowledgements

This article received no financial or funding support.

Conflicts of Interest

The authors confirm that there are no conflicts of interest.

References

[1] Florencio, D. and Herley, C. A large-scale study of web password habits. In: Proceedings of the 16th International Conference on World Wide Web, 2007.

[2] Baker, W., Hylender, C.D., Valentine, J.A. and Porter, C. 2011 data breach investigations report. Verizon RISK Team, 2011, 1-72.

[3] Bonneau, J., Herley, C., van Oorschot, P.C. and Stajano, F. The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In: IEEE Symposium on Security and Privacy, 2012.

[4] Temoshok, D., Abruzzi, J. and others Digital identity guidelines. National Institute of Standards and Technology, 2022.

[5] Huynh, T.T., Nguyen, T.D. and Tan, H. A survey on security and privacy issues of blockchain technology. In: International Conference on System Science and Engineering (ICSSE), 2019.

[6] Jain, A.K., Ross, A. and Prabhakar, S. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 2004, 14(1), 4-20.

[7] Galbally, J., Marcel, S. and Fierrez, J. Biometric antispoofing methods: a survey in face recognition. IEEE Access, 2014, 2, 1530-1552.

[8] Goodfellow, I.J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A. and Bengio, Y. Generative adversarial nets. Advances in Neural Information Processing Systems, 2014, 27.

[9] Jain, A.K. and Li, S.Z. Handbook of face recognition. New York: Springer, 2011.

[10] Ratha, N.K., Connell, J.H. and Bolle, R.M. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 2001, 40(3), 614-634.

[11] Bhutta, M.N.M., Khwaja, A.A., Nadeem, A., Ahmad, H.F., Khan, M.K., Hanif, M.A., Song, H., Alshamari, M. and Cao, Y. A survey on blockchain technology: evolution, architecture, and security. IEEE Access, 2021. DOI: 10.1109/ACCESS.2021.3072849.

[12] Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P. and Chen, R. NutBaaS: a blockchain-as-a-service platform. IEEE

Access, 2019, 7, 134422-134433. DOI: 10.1109/ACCESS.2019.2941905.

[13] Zhang, H., Venkatesh, S., Ramachandra, R., Raja, K., Damer, N. and Busch, C. MIPGAN—generating strong and high-quality morphing attacks using identity prior driven GAN. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2021, 3(3), 365.