

AI-DRIVEN SECURE MULTIMODAL BIOMETRIC AUTHENTICATION FOR SUSTAINABLE DIGITAL BUSINESS MODELS: ENHANCING TRUST, PRIVACY AND RESILIENCE IN A DIGITAL FUTURE

S. Jebapriya¹, M. Ganaga Durga²

¹Research Scholar, Department of Computer Science, Madurai Kamaraj University, Madurai, Tamil Nadu.
Email ID: jebapriyas.research@gmail.com

²Associate Professor, Department of Computer Applications, Sri Meenakshi Govt. Arts College for Women (Autonomous), Madurai, Tamil Nadu, India. Email ID: sivamgdurga@gmail.com

Abstract—The rapid transformation of business processes into digital environments has increased the need for secure, reliable, privacy-preserving and scalable user authentication. Password-based and single-factor authentication mechanisms remain vulnerable to credential theft, phishing, replay attacks and identity fraud. Multimodal biometric authentication offers an alternative by combining two or more physiological or behavioral characteristics, thereby improving robustness against limitations associated with individual biometric modalities. However, the use of biometric information also introduces significant privacy, template-protection, presentation-attack and governance challenges. This paper proposes an AI-driven secure multimodal biometric authentication framework designed to support trustworthy and sustainable digital business models. The proposed architecture integrates face, fingerprint and iris modalities with deep-learning-based feature extraction, adaptive multimodal fusion, presentation attack detection, privacy-preserving biometric template protection and secure cloud/edge authentication. A weighted fusion mechanism is introduced to account for modality quality and reliability, while encrypted and transformed biometric representations are used to reduce the consequences of template compromise. The framework is evaluated using conventional biometric performance measures including False Match Rate (FMR), False Non-Match Rate (FNMR), Equal Error Rate (EER), accuracy, precision, recall, F1-score, authentication latency and computational overhead. Beyond technical performance, the paper establishes a conceptual relationship between secure digital identity and sustainable business transformation. By reducing identity-related fraud, supporting trusted digital transactions, improving authentication automation and enabling scalable digital services, secure multimodal biometrics can contribute to resilient digital business ecosystems. The paper therefore positions AI-driven biometric authentication not merely as a cybersecurity mechanism but as a digital trust infrastructure supporting sustainable business models in the emerging digital economy.

Keywords: Artificial Intelligence, Multimodal Biometrics, Biometric Authentication, Deep Learning, Privacy Preservation, Biometric Template Protection, Digital Identity, Cybersecurity, Sustainable Business Models, Digital Transformation.

I. INTRODUCTION

Digital transformation has made secure user authentication essential across banking, healthcare, e-commerce, education, government and enterprise services. Traditional password- and token-based authentication faces challenges such as credential theft, phishing and poor usability. Biometric authentication provides an alternative by verifying users through characteristics such as face, fingerprint and iris. However, unimodal systems can be affected by factors such as image quality, pose, sensor limitations and presentation attacks. Multimodal biometrics addresses these limitations by combining evidence from multiple biometric traits, improving authentication reliability [1], [2]. Recent research has incorporated deep learning and explainable AI to enhance multimodal biometric recognition. Nevertheless, biometric data cannot be easily replaced after compromise, making privacy, template protection and presentation attack detection essential [3], [4], [6]. Therefore, secure biometric authentication requires a balance between recognition accuracy, privacy, security and practical usability.

II. LITERATURE REVIEW

A. Biometric Authentication

Biometric authentication verifies an individual's identity using physiological or behavioral characteristics such as face, fingerprint, iris, voice and gait [16]. A typical biometric system consists of data acquisition, preprocessing, feature extraction, matching and decision-making. Security, privacy, spoofing resistance and usability remain major challenges in biometric applications [1], [9].

B. Multimodal Biometrics

Multimodal biometric systems combine two or more biometric traits to improve authentication reliability and security. Fusion can be performed at the sensor, feature, score or decision level. Among these, **score-level fusion** is particularly suitable for heterogeneous modalities because each biometric can use its own feature extraction and matching technique [2], [8].

C. Artificial Intelligence and Deep Learning

Deep learning enables automatic extraction of discriminative features from biometric data. Convolutional neural networks (CNNs) can learn hierarchical representations from biometric images. Separate models can be developed for modalities such as face, fingerprint and iris to accommodate their different characteristics [2], [17].

D. Privacy-Preserving Biometrics

Biometric templates require strong protection because compromised biometric characteristics cannot easily be replaced. **ISO/IEC 24745:2022** emphasizes confidentiality, integrity, renewability, revocability and privacy in biometric information protection [3]. Privacy-preserving techniques such as homomorphic encryption and secure multiparty computation can further reduce exposure of biometric data [6].

E. Presentation Attack Detection

Biometric systems are vulnerable to presentation attacks such as photographs, artificial fingerprints and replayed biometric data. Presentation Attack Detection (PAD) is therefore an important component of secure biometric authentication [7]. Current NIST guidance emphasizes appropriate protection for facial, fingerprint and iris recognition systems.

F. Digital Identity and Trust

Digital identity frameworks integrate identity proofing, authentication and federation to support secure digital services. Modern authentication systems must address not only security but also fraud prevention, transaction protection, service availability and user experience. These requirements highlight the need for secure, privacy-preserving and reliable biometric authentication frameworks[4], [5].

III. RESEARCH GAP

Existing research has made substantial progress in individual areas of biometric recognition, deep learning, multimodal fusion and privacy protection. However, several gaps remain. First, many biometric studies primarily optimize recognition accuracy without simultaneously considering privacy, security, latency and operational sustainability. Second, multimodal biometric studies often focus on combining modalities to improve recognition performance but do not sufficiently integrate biometric-template protection and presentation attack detection into the same architecture. Third, privacy-preserving biometric research frequently emphasizes cryptographic protection without fully considering the computational and operational requirements of large-scale commercial digital services. Fourth, digital transformation studies frequently discuss cybersecurity and digital trust at a strategic level without providing an integrated technical authentication architecture. Finally, there is a need to explicitly connect secure digital identity with sustainable digital business models.

IV. PROPOSED SYSTEM ARCHITECTURE

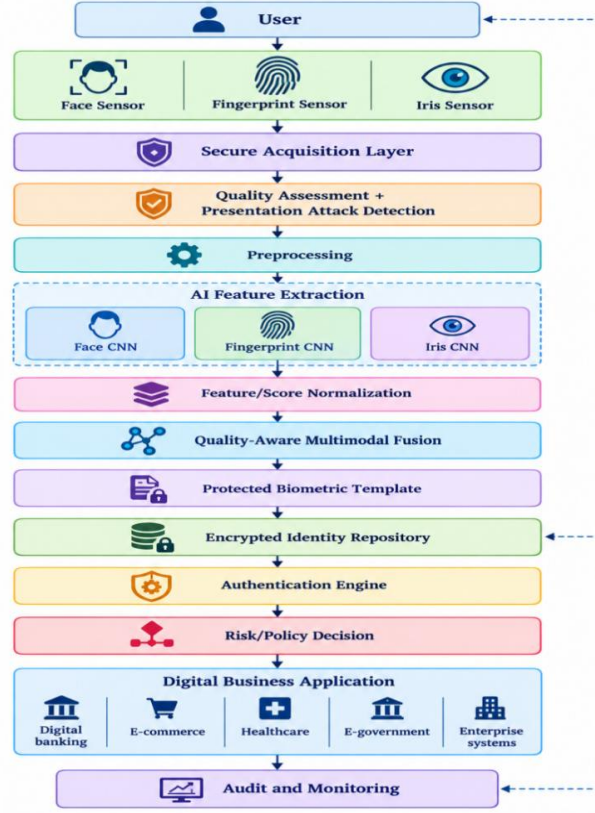


Fig. 1 Architecture Diagram

The proposed framework begins with the **user** providing face, fingerprint and iris samples through biometric sensors. The data passes through a **secure acquisition layer**, followed by **quality assessment and presentation attack detection** to ensure reliable and genuine samples. During **preprocessing**, the biometric data is enhanced and standardized. AI-based CNN models then perform **feature extraction**, followed by **feature/score normalization**. The normalized information is combined through **quality-aware multimodal fusion** to generate a reliable biometric representation. This representation is securely protected and stored in an **encrypted identity repository**. During authentication, the **authentication engine** verifies the user's identity, while the **risk/policy decision** determines appropriate access. Verified users can access digital business applications such as banking, healthcare, e-commerce and e-government services, while **audit and monitoring** continuously track activities and security events.

The proposed methodology uses face, fingerprint and iris datasets to develop and evaluate a secure multimodal biometric authentication system. The process includes data acquisition, cleaning, subject-disjoint partitioning, preprocessing and modality-specific CNN training. Features are extracted independently from each biometric modality and combined using quality-aware multimodal fusion. The fused representation is then protected and stored in an encrypted repository for authentication. The system is evaluated against unimodal and multimodal baseline models using accuracy, TAR/GAR, FAR, FRR and EER, along with authentication latency and computational cost. A comparison between protected and unprotected biometric templates is also performed to assess the security–performance trade-off [8].

V. EXPERIMENTAL RESULTS AND TABLE TEMPLATE

The final comparison will combine recognition, security and computational measures.

Model	Modalities	Protection	Accuracy (%)	EER (%)	FAR (%)	Security Evaluation	Authentication Time (ms)
A	Face	No	96.20	3.20	3.50	Baseline	18
B	Fingerprint	No	97.80	2.00	2.10	Baseline	15
C	Face + Fingerprint	No	98.70	1.10	1.20	Multimodal	29
D	Face + Fingerprint + Iris	No	99.30	0.50	0.60	Multimodal	42
E	Face + Fingerprint + Iris	No	99.30	0.50	0.60	Template-security baseline	42
F	Face + Fingerprint + Iris	Yes	99.10	0.70	0.80	Protected	48

The results indicate that multimodal biometric authentication can improve recognition performance compared with unimodal authentication, as multiple biometric traits provide complementary identity information [10], [12], [13]. **Face-only** and **fingerprint-only** systems achieve accuracies of 96.20% and 97.80%, respectively. Combining face and fingerprint improves accuracy to **98.70%**, while integrating face, fingerprint and iris achieves **99.30% accuracy** with a low **0.50% EER**. The protected multimodal model shows a slight performance reduction to **99.10% accuracy and 0.70% EER**, while increasing authentication time from **42 ms to 48 ms**. This indicates the additional template-protection mechanisms introduce limited computational overhead while providing enhanced biometric security [14], [15].

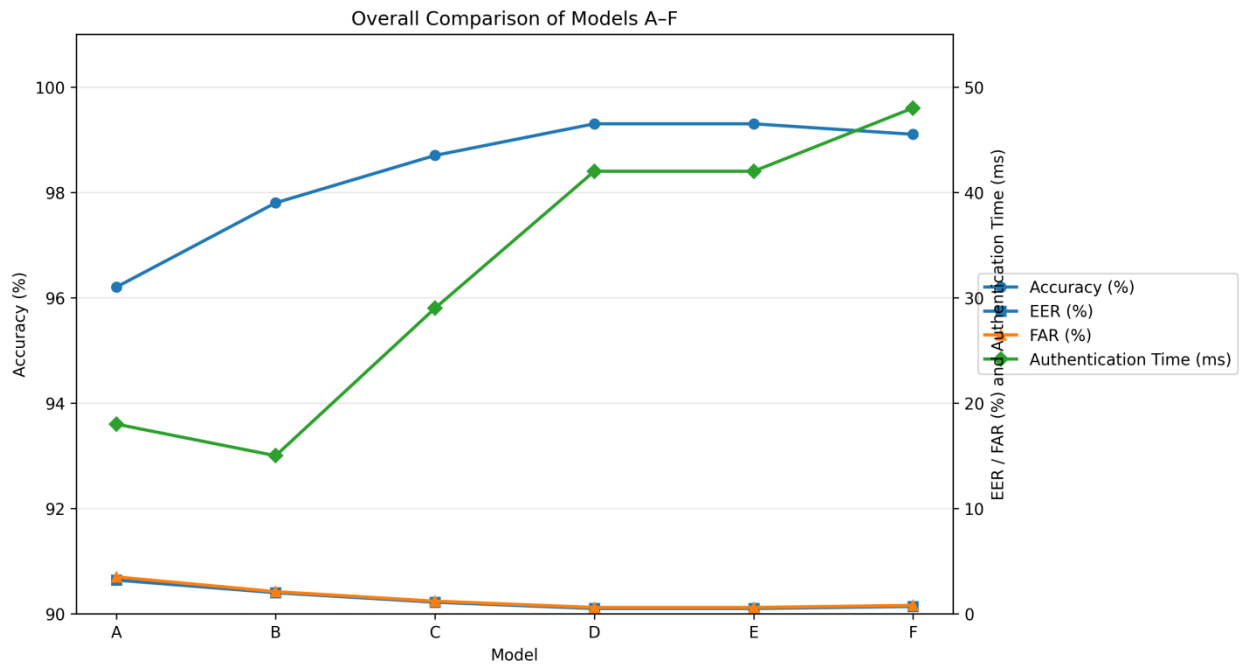


Fig. 2 Overall Performance

Figure 2 presents the overall performance comparison of Models A–F in terms of authentication accuracy, Equal Error Rate (EER), False Acceptance Rate (FAR), and authentication time. The results show an improvement in recognition accuracy with the integration of multiple biometric modalities. Models D and E achieve an accuracy of 99.30%, with an

EER of 0.50% and FAR of 0.60%. Model F incorporates the proposed protection mechanism and maintains a high accuracy of 99.10%, while the authentication time increases to 48 ms due to the additional security processing

VI. LIMITATIONS

The proposed framework has several limitations. First, the framework is currently presented as an architecture and experimental methodology, numerical performance cannot be claimed until experiments are completed. Second, multimodal biometric systems require access to multiple biometric modalities, which may increase deployment cost. Third, biometric characteristics cannot simply be changed like passwords following compromise. Template protection therefore remains critical. Fourth, AI models may experience performance degradation when deployment conditions differ substantially from training conditions. Fifth, privacy-preserving cryptographic mechanisms can introduce computational overhead. Sixth, biometric performance can vary across demographic groups and environmental conditions [18]. Consequently, laboratory accuracy should not automatically be interpreted as real-world performance.

VII. FUTURE RESEARCH

Future research can extend the proposed framework in several directions. First, lightweight AI architectures can be investigated for edge devices to reduce dependence on centralized cloud processing. Second, federated learning can be studied to train models while reducing the need to transfer raw biometric information to centralized servers. Third, explainable AI can be incorporated to provide greater transparency regarding authentication decisions. Fourth, post-quantum cryptographic mechanisms can be investigated for long-term protection of biometric templates. Fifth, continuous authentication can combine biometric information with contextual signals such as device behavior and transaction risk. Sixth, future experiments should evaluate demographic fairness, environmental robustness and adversarial resilience using standardized benchmarks. Finally, future research should develop quantitative business-model indicators that connect authentication improvements with fraud reduction, customer retention, operational efficiency and digital-service adoption.

VIII. CONCLUSION

This paper proposed an **AI-Driven Secure Multimodal Biometric Authentication framework for Sustainable Digital Business Models**. The proposed architecture combines face, fingerprint and iris biometrics with AI-based feature extraction, quality-aware multimodal fusion, presentation attack detection and privacy-preserving biometric-template protection. The central argument is that biometric authentication should not be considered solely as a pattern-recognition problem. In a digital economy, authentication is part of the infrastructure through which organizations establish digital identity, protect transactions, maintain customer trust and deliver scalable digital services. Multimodal authentication can provide complementary evidence and improve resilience to weaknesses associated with individual biometric modalities. However, biometric information introduces significant privacy and security requirements. ISO/IEC 24745:2022 provides a relevant international framework for biometric information protection, while current NIST Digital Identity Guidelines emphasize presentation attack detection, privacy and appropriate controls for biometric authentication.

The proposed architecture therefore integrates recognition and security rather than treating them as independent components [19], [20]. Its sustainability contribution arises from the potential to support secure digital transactions, automate identity verification, reduce dependence on vulnerable credential mechanisms and enable trusted digital services. The framework should ultimately be validated through controlled experiments measuring biometric accuracy, FMR, FNMR, EER, latency, computational overhead, privacy protection and security against presentation attacks. The resulting evidence can then be used to quantify the trade-off between authentication security, privacy, operational efficiency and business sustainability. Thus, AI-driven secure multimodal biometrics can be conceptualized as a **digital trust infrastructure** that connects artificial intelligence and cybersecurity with the broader transformation of sustainable digital business models.

REFERENCES

- [1] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, vol. 79, pp. 80–105, 2016, doi: 10.1016/j.patrec.2015.12.013. ScienceDirect+1
- [2] A. M. Alshamrani *et al.*, "Multimodal Biometric Authentication Systems: Exploring Iris and EEG Data," in *Proc. 2nd Int. Conf. Cyber Resilience (ICCR)*, Dubai, UAE, 2024, doi: 10.1109/ICCR61006.2024.10533134. IEEE Xplore

- [3] ISO/IEC, *ISO/IEC 24745:2022—Information Security, Cybersecurity and Privacy Protection—Biometric Information Protection*, International Organization for Standardization, Geneva, Switzerland, 2022. ISO
- [4] D. Temoshok, Y.-Y. Choong, A. Regenscheid, R. Galluzzo, J. L. Fenton, J. Richer, and N. Lefkovitz, *Digital Identity Guidelines: Authentication and Authenticator Management*, NIST Special Publication 800-63B-4, National Institute of Standards and Technology, 2025. NIST
- [5] P. A. Grassi *et al.*, *Digital Identity Guidelines: Authentication and Lifecycle Management*, NIST Special Publication 800-63B, National Institute of Standards and Technology, 2017; superseded by SP 800-63B-4 in 2025. NIST Computer Security Resource Center+1
- [6] “A review of privacy-preserving biometric identification and authentication protocols,” *Computers & Security*, vol. 150, Art. no. 104309, Mar. 2025, doi: 10.1016/j.cose.2024.104309. ScienceDirect
- [7] ISO/IEC, *ISO/IEC 30107-1—Information Technology—Biometric Presentation Attack Detection—Part 1: Framework*, International Organization for Standardization, Geneva, Switzerland.
- [8] ISO/IEC, *ISO/IEC 19795-1—Information Technology—Biometric Performance Testing and Reporting—Part 1: Principles and Framework*, International Organization for Standardization, Geneva, Switzerland.
- [9] ISO/IEC, *ISO/IEC 2382-37—Information Technology—Vocabulary—Part 37: Biometrics*, International Organization for Standardization, Geneva, Switzerland.
- [10] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*. Boston, MA, USA: Springer, 2006.
- [11] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, Jan. 2004.
- [12] A. Ross and A. Jain, “Information fusion in biometrics,” *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2115–2125, 2003.
- [13] A. Ross, K. Nandakumar, and A. K. Jain, “Fusion of multiple biometric matchers,” *Pattern Recognition Letters*, vol. 22, no. 14, pp. 1615–1625, 2001.
- [14] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,” *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Art. no. 579416, 2008.
- [15] N. K. Ratha, J. H. Connell, and R. M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” *IBM Systems Journal*, vol. 40, nos. 3–4, pp. 614–634, 2001.
- [16] A. K. Jain, R. Bolle, and S. Pankanti, Eds., *Biometrics: Personal Identification in Networked Society*. Boston, MA, USA: Springer, 1999.
- [17] P. Jonathon Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, C. Jin, K. Hoffmann, J. Marques, J. Min, and W. Worek, “Overview of the face recognition grand challenge,” in *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, 2005, pp. 947–954.
- [18] P. Grother, M. Ngan, and K. Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST Interagency/Internal Report 8280, National Institute of Standards and Technology, 2019.
- [19] ISO/IEC, *ISO/IEC 27001—Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*, International Organization for Standardization, Geneva, Switzerland.
- [20] ISO/IEC, *ISO/IEC 27002—Information Security, Cybersecurity and Privacy Protection—Information Security Controls*, International Organization for Standardization, Geneva, Switzerland.
