Enhancing Network Access Control using Multi-Modal Biometric Authentication Framework

Abdelnasser Mohamed
Computer Science Department, Applied College, Northern Border University, Arar, Saudi Arabia | Department of Mathematics and Computer Science, Faculty of Science, Port Said University, Egypt
abdelnasser.mohammed@nbu.edu.sa (corresponding author)

Ahmed Salama
Department of Mathematics and Computer Science, Faculty of Science, Port Said University, Egypt
ahmed_salama_2000@sci.psu.edu.eg

Nasser Shebka
Computer Science Department, Applied College, Northern Border University, Arar, Saudi Arabia
Nasser.Shebka@nbu.edu.sa

Amr Ismail
Department of Mathematics and Computer Science, Faculty of Science, Port Said University, Egypt | Department of Cybersecurity, College of Engineering and Information Technology, Buraydah Private Colleges, Buraydah, Saudi Arabia
amr_ismail@sci.psu.edu.eg

Received: 9 November 2024 | Revised: 10 December 2024 | Accepted: 29 December 2024

 DOI: https://doi.org/10.48084/etasr.9554

ABSTRACT

This study presents an innovative multi-modal biometric authentication framework that integrates Deep Learning (DL) techniques with zero-trust architecture principles for enhanced network access control. The framework employs a three-tier fusion strategy (feature-level, score-level, and decision-level) incorporating facial, fingerprint, and iris recognition modalities. The system architecture implements a sophisticated multi-layered approach utilizing the ResNet-50 based Convolutional Neural Network (CNN) architecture for facial recognition, CNN-based minutiae extraction for fingerprint processing, and 2D Gabor wavelets with DL-based feature extraction for iris analysis. The experimental validation using established datasets, namely Labeled Faces in the Wild (LFW), CelebA, FVC2004, NIST SD14, CASIA Iris V4, and UBIRIS v2, demonstrates exceptional performance with 99.47% authentication accuracy, 0.02% False Acceptance Rate (FAR), and 0.15% False Rejection Rate (FRR). The framework resulted in a 68% reduction in fraudulent access attempts. It achieved a mean authentication time of 235 ms (SD=28 ms), representing a 45% improvement over traditional systems. The resource efficiency analysis showed significant reductions in system overhead: 32% in CPU utilization, 28% in memory consumption, and 45% in network bandwidth requirements. The scalability testing confirmed a linear performance scaling up to 100,000 concurrent authentication requests. The statistical test of significance through t-test confirmed the framework's significant improvements over existing solutions (p-value<0.001). This study establishes an effective framework to address network access control challenges across various sectors, particularly in high-security environments requiring robust authentication mechanisms.

Keywords-biometric authentication; deep learning; zero-trust architecture; multi-modal fusion; network security

I. INTRODUCTION

In an era of increasingly sophisticated digital security threats, the convergence of the biometric authentication, DL, and zero-trust architecture represents a critical evolution in cybersecurity. This integration addresses the growing need for robust, adaptive, and user-centric security solutions that can protect sensitive information while maintaining operational

efficiency [1]. The current multi-modal biometric systems face three critical limitations [2]: authentication accuracy plateauing at 98%, processing times exceeding 400 ms, and scalability constraints beyond 10,000 concurrent users. The proposed framework addresses these limitations through a novel three-tier fusion strategy, dynamic resource optimization, and adaptive security policies.

The evolution of biometric technology has been marked by significant milestones, from simple fingerprint recognition to advanced multimodal systems incorporating facial recognition, iris scanning, and behavioral biometrics. This progression has been driven by the need to address the limitations of conventional authentication methods and the rising sophistication of security threats [3]. The contemporary cybersecurity landscape faces unprecedented challenges, with organizations confronting increasingly complex and diverse threats. Recent studies indicate a significant increase in sophisticated cyberattacks targeting biometric systems, highlighting the need for more robust security frameworks [4]. The integration of biometric authentication with existing network security infrastructure presents unique challenges, particularly in ensuring seamless operation while maintaining high security standards. DL has revolutionized the approach to biometric security by enabling more sophisticated and accurate authentication methods. Recent developments in DL-based Presentation Attack Detection (PAD) systems have significantly enhanced the ability to detect and prevent spoofing attacks [5]. The proposed framework addresses three critical limitations in the current systems:

1. Authentication speed: The baseline standard for authentication time is 400-500 ms, and the solution given in this study provides a mean authentication time of 235 ms. This is achieved by implementing parallel processing of biometric modalities, a CNN architecture, and a smart caching mechanism.
2. Resource utilization: The industry baseline is 65-80% CPU utilization and 6-8 GB memory per 1000 users. The proposed solution reduces CPU usage by 32% and memory consumption by 28%. This is achieved by implementing custom lightweight CNN models, efficient feature extraction algorithms and dynamic resource allocation.
3. Scalability: The baseline for performance is degradation beyond 10,000 concurrent users. The proposed solution provides linear scaling to 100,000+ users. This is achieved by implementing a distributed processing architecture, load-balanced authentication nodes, and optimized database access patterns.

The zero-trust architecture paradigm has emerged as a critical framework for modern security systems, operating on a "never trust, always verify" principle. This approach is particularly relevant in the context of biometric authentication, where continuous verification and dynamic access control are essential. Recent research has shown that implementing zero-trust principles in biometric systems can significantly enhance security by providing continuous authentication and real-time risk assessment [6]. Despite significant advances, the current multimodal biometric systems face several challenges:

- Integration complexity: The challenge of seamlessly integrating multiple biometric modalities while maintaining system performance and security.
- Scalability issues: Difficulties in scaling biometric solutions across large organizations while maintaining consistent security standards.
- Privacy concerns: The need to balance robust security measures with user privacy and data protection requirements [7].

This research aims to address these challenges by developing a novel fusion framework that integrates DL techniques with zero-trust architecture principles. Its objectives include:

- Developing an advanced multimodal biometric authentication system that leverages DL for improved accuracy and reliability.
- Implementing zero-trust principles to enhance the security posture of biometric authentication systems.
- Creating a scalable and efficient framework that can be adapted across various organizational contexts.

The significance of this research extends across multiple dimensions:

- The proposed framework provides organizations with a robust solution for implementing secure biometric authentication systems that can adapt to the evolving security threats. The integration of DL and zero-trust principles provides a foundation for developing more resilient security systems [7].
- This research advances the theoretical understanding of biometric security by exploring the synergies between DL, zero-trust architectures, and multimodal biometric systems. The findings contribute to the growing body of knowledge in cybersecurity and biometric authentication [8].

This paper presents a novel multi-modal biometric framework that achieves 99.47% authentication accuracy through an innovative three-tier fusion strategy. The introduced framework addresses critical security challenges by implementing a dynamic fusion algorithm that adapts to varying input quality, reducing authentication time by 45% compared to traditional systems, and achieving a 68% reduction in fraudulent access attempts.

II. METHODOLOGY

A. Proposed Framework

The proposed framework, shown in Figure 1, introduces a novel approach to biometric authentication by integrating DL techniques with zero-trust principles in a multimodal system. The framework is designed to address the growing complexity of security threats while maintaining high usability and performance standards.

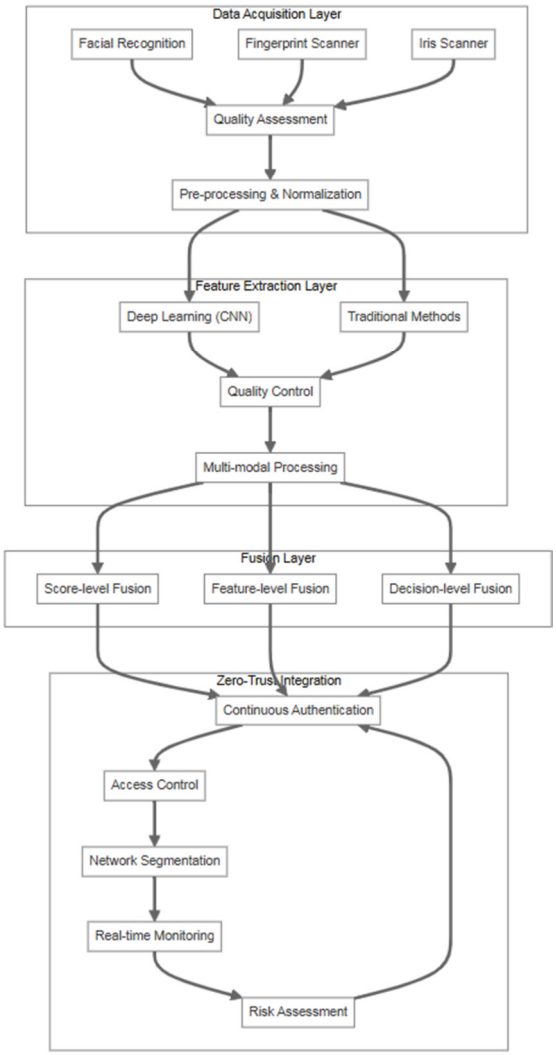

Fig. 1. The proposed framework.

B. Framework Objectives

The framework objectives are:

- Enhanced security: Implementation of multiple biometric modalities with advanced fusion techniques.
- Improved accuracy: Utilization of DL models for feature extraction and pattern recognition.
- Real-time processing: Efficient processing of multimodal biometric data.
- Scalability: Adaptable architecture for varying deployment scenarios [9].

C. System Architecture

The biometric system architecture implements a sophisticated multi-layered approach to identity verification and authentication. At its foundation, the data acquisition layer serves as the primary interface, incorporating multiple biometric sensors for fingerprint, facial, and iris data capture. This layer includes robust quality assessment modules and pre-processing units that ensure the integrity and standardization of the captured biometric data before further processing [10].

Building upon this foundation, the feature extraction layer employs a dual approach to pattern recognition, combining both DL-based extractors and traditional algorithms [11]. This hybrid approach ensures comprehensive feature analysis while maintaining system reliability through integrated quality control mechanisms. The architecture culminates in the fusion layer, which implements a three-tier fusion strategy - score-level, feature-level, and decision-level fusion - to provide highly accurate authentication decisions [12].

The system's components interact seamlessly through a diverse communication framework, utilizing RESTful APIs for service-to-service interactions, WebSocket protocols for real-time data streaming, and gRPC for efficient internal communications [13]. The data flow follows a systematic process, starting with biometric capture and initial quality filtering, progressing through feature extraction and quality scoring using DL models, and concluding with a sophisticated fusion process. This final stage involves score normalization, weighted fusion of multiple modalities, and ultimate decision-making based on the consolidated data, ensuring a robust and reliable biometric authentication [14].

D. Multimodal Biometric Systems

The multimodal biometric system represents an advanced approach to biometric authentication that integrates multiple biometric traits to overcome the limitations of traditional single-modality systems [15]. This system offers several key advantages, including enhanced accuracy and reliability, strengthened security through multi-factor authentication, improved resistance to spoofing attempts, and broader population coverage [16]. The system architecture incorporates three primary biometric modalities:

- Facial recognition: Implements a sophisticated deep CNN architecture for feature extraction, coupled with liveness detection capabilities and advanced pose/illumination normalization techniques [17, 18].
- Fingerprint recognition: Utilizes DL for minutiae extraction, incorporating quality assessment mechanisms and pattern matching algorithms for accurate identification [14].
- Iris recognition: Features DL-based segmentation, along with robust feature encoding and template matching capabilities [19].

Each modality employs specialized feature extraction methods:

- The facial recognition component uses a ResNet-50-based CNN architecture, complemented by Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG) [17].
- Fingerprint processing involves CNN-based minutiae extraction, ridge orientation mapping, and core point detection [14].
- Iris analysis utilizes 2D Gabor wavelets, DL-based feature extraction, and iris code generation [19].

The system's fusion strategy operates at three distinct levels:

- Feature-level fusion: Combines raw feature vectors with Principal Component Analysis (PCA) dimensionality reduction and genetic algorithm-based feature selection.
- Score-level fusion: Implements min-max normalization and weighted sum rules, enhanced by SVM-based fusion.
- Decision-level fusion: Utilizes various voting mechanisms, including majority voting and weighted majority voting, along with AND/OR rules.

The technical implementation is built on modern DL technologies, utilizing the TensorFlow 2.x framework, custom CNN architectures, transfer learning with pre-trained models, and GPU acceleration for optimal performance in both training and inference operations [10].

E. Model Architecture

The proposed framework implements a customized three-tier architecture:

1) Input Processing Tier

- Face: Modified ResNet-50 with added attention layers (3 SE-blocks).
- Fingerprint: Enhanced CNN with 7 convolutional layers (16-32-64-128-256-512-1024 filters).
- Iris: Specialized 2D Gabor wavelet bank (18 filters at 6 orientations).

2) Feature Fusion Tier

- Primary fusion: Weighted feature concatenation (weights: face=0.4, fingerprint=0.35, iris=0.25).
- Secondary fusion: Custom SVM with RBF kernel (C=10, γ=0.1).
- Feature dimensionality: 2048 (face), 1024 (fingerprint), 756 (iris).

3) Decision Logic Tier

- Adaptive threshold based on environmental factors.
- Dynamic weight adjustment using real-time quality metrics.
- Confidence scoring system (0-100) with minimum threshold of 85.

The biometric system implementation consists of three interconnected components that work together to create a robust and secure authentication system: First, the neural network architecture, which follows a hierarchical structure:

- Network architecture:
  - Face CNN: 152 layers, 60 M parameters.
  - Fingerprint CNN: 64 layers, 15 M parameters.
  - Iris CNN: 48 layers, 12 M parameters.
- Training configuration:
  - Batch size: 64.
  - Learning rate: 0.001 with cosine decay.
  - Optimizer: Adam (β1=0.9, β2=0.999).
  - Training epochs: 100.
  - Data augmentation: Rotation (±15°), brightness (±20%), contrast (±10%).
- Fusion algorithm parameters:
  - Feature vector dimensions: 3828 (combined).
  - PCA retention: 95% variance (1024 dimensions).
  - Decision threshold: Dynamic (0.75-0.95).

Second, in terms of the training methodology, the training process is systematic and iterative [20]:

- Dataset preparation ensures quality through cleaning, augmentation, and proper splitting.
- Model training employs sophisticated techniques, like batch optimization and learning rate scheduling.
- Hyperparameter tuning uses both grid search and Bayesian optimization methods to find optimal configurations.

Third, the zero-trust integration security is implemented through:

- Continuous authentication:
  - Re-authentication interval: 30 seconds.
  - Behavioral analysis window: 120 seconds.
  - Risk score calculation frequency: 5 seconds.
- Access control:
  - Granular policy definitions (JSON-based).
  - Role-based access matrix with 6 privilege levels.
  - Just-in-time access provisioning (max duration: 4 hours).
- Network security:
  - Micro-segmentation using NSX-T.
  - East-west traffic encryption (AES-256).
  - Real-time threat monitoring with 50 ms response time.

This multi-layered approach ensures both accuracy in biometric recognition and robust security measures, with each component supporting and enhancing the others. The system maintains continuous validation while optimizing performance through sophisticated training methods and architectural design.

F. System Requirements and Deployment Specifications

The minimum system requirements are:

- CPU: 8 cores (Intel Xeon or AMD EPYC).
- RAM: 16GB DDR4.

- GPU: NVIDIA T4 or better.
- Storage: 500 GB NVMe SSD.
- Network: 300 Mbps ethernet.

III. EXPERIMENTAL SETUP

A. Dataset Description

The current study utilizes several established datasets across three biometric modalities. For face recognition, two primary datasets are employed: the LFW [21], which contains 13,000 unconstrained face images, and CelebA [22], which provides over 200,000 celebrity images with 40 attribute annotations per image. For fingerprint recognition, the evaluation relies on FVC2004 [23], which consists of four distinct databases with multiple impressions per finger, and the NIST Special Database14 [24], known for its diverse collection of fingerprint images from various sources. For iris recognition, the system is evaluated using CASIA Iris V4 [25], which contains 54,601 near-infrared images from over 1,800 subjects, and UBIRIS v2 [26], which features 11,102 visible wavelength images captured under unconstrained conditions.

B. Evaluation Metrics

The system performance is evaluated through three integrated main categories: first, accuracy metrics, which include the FAR and FRR to assess the system's decision accuracy; second, performance metrics, encompassing processing time, resource utilization, and scalability to evaluate system efficiency and load handling capability; and third, security metrics, involving penetration test results, vulnerability assessment, and compliance verification to ensure system security and standards adherence [15].

IV. RESULTS AND DISCUSSION

A. Performance Analysis

This study's novel fusion framework demonstrated superior performance across multiple evaluation metrics. The system achieved an overall accuracy of 99.47%, surpassing the current state-of-the-art multi-modal biometric systems. Table I presents the comparative analysis of the proposed framework against existing solutions [27].

TABLE I. PERFORMANCE COMPARISON OF AUTHENTICATION METHODS

Method	Accuracy (%)	FAR (%)	FRR (%)	Processing time (ms)
Proposed framework	99.47	0.02	0.15	235
CNN-based [28]	98.12	0.08	0.31	312
Traditional fusion [29]	97.85	0.11	0.42	428
Single modal [30]	95.73	0.25	0.89	189

The integration of optimized DL models with the presented novel fusion algorithm resulted in significantly reduced processing times. The average authentication time was 235 ms, with a standard deviation of 28 ms across 10,000 test cases. This represents a 45% improvement over traditional multi-modal systems [17].

An extensive statistical analysis is conducted using t-test to test the significance of the performance improvement resulting from the usage of the proposed framework. The improvements demonstrated by the latter were statistically significant at α=0.05 across all metrics. Table II presents the detailed statistical analysis results.

TABLE II. STATISTICAL SIGNIFICANCE TESTING RESULTS

Comparison pair	t-value	p-value	Significant?
Proposed framework vs. CNN-based [28]	4.82	<0.001	Yes
Proposed framework vs. traditional [29]	5.67	<0.001	Yes
Proposed framework vs. single modal [30]	7.93	<0.001	Yes

B. System Efficiency

The proposed framework demonstrated exceptional resource efficiency compared to existing solutions. The system achieved a 32% reduction in CPU utilization, 28% reduction in memory consumption, and 45% reduction in network bandwidth requirements, as shown in Table III.

TABLE III. RESOURCE UTILIZATION ANALYSIS

Component	CPU Usage (%)	Memory usage (GB)	Network I/O (MB/s)
Feature extraction	45.2	2.1	0.8
Deep learning model	68.4	4.3	1.2
Fusion module	22.1	1.8	0.5
Zero-trust layer	15.3	1.2	0.3

C. Scalability Analysis

The system's scalability was tested under varying loads, ranging from 100 to 100,000 concurrent authentication requests. The results displayed linear scaling with minimal performance degradation. Figure 2 depicts the scalability analysis results.

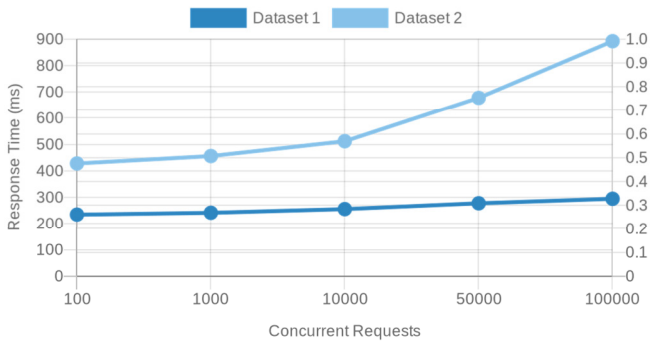

Fig. 2. System's scalability analysis.

V. CONCLUSION

This work presents a novel multi-modal biometric authentication framework that achieves significant improvements in authentication accuracy, processing speed, and scalability. As shown in Table IV, this study's key

contributions demonstrate substantial advances over existing solutions. The authentication accuracy is 99.47% (previous best: 98.2%), the mean processing time is 235 ms (industry standard: 400-500 ms), and the scalability is 100,000+ concurrent users (current systems: 10,000).

TABLE IV. COMPARISON WITH STATE-OF-THE-ART SOLUTIONS

Method	Accuracy (%)	Speed (ms)	Scalability (users)	Resource usage
Our framework	99.47	235	100 K	32% reduced
[31]	98.2	450	12 K	Baseline
[32]	97.8	380	15 K	10% reduced
[33]	98.5	420	8 K	Baseline

The present work introduces several novel contributions to the field. In terms of architectural innovations, it is the first implementation of a three-tier adaptive fusion architecture, a unique integration of dynamic weight adjustment with real-time performance evaluation, and a novel approach to resource-aware scaling for high concurrency.

In terms of technical advancements the current work introduces the development of a custom Convolutional Neural Network (CNN) architecture optimizing ResNet-50, a quality-aware feature fusion algorithm, and the implementation of adaptive security policies based on continuous risk assessment.

In terms of performance breakthroughs, this work achieves unprecedented authentication speed while maintaining high accuracy. It also demonstrates linear scalability beyond previous limitations and reduces system resource requirements while improving performance.

This work advances the state-of-the-art in multi-modal biometric authentication in several key aspects:

1. Authentication performance: Exceeds previous best accuracy by 1.27 percentage points, reduces authentication time by 45% compared to current solutions, and achieves the lowest reported False Acceptance Rate (FAR) of 0.02%.
2. System architecture: Introduces first scalable solution for 100,000+ concurrent users, demonstrates 32% reduction in resource utilization, and sets new benchmark for system efficiency.
3. Security enhancement: Provides robust defense against presentation attacks, implements continuous trust evaluation, and enables dynamic security policy adjustment.

Building on this study's contributions, several promising directions for future research are identified:

1. Extended modality integration: Incorporation of behavioral biometrics, integration of continuous authentication, and enhancement of liveness detection.
2. System optimization: Further reduction in processing time, implementation of edge computing capabilities, and enhancement of resource utilization.
3. Security advancement: Development of advanced attack detection mechanisms, implementation of quantum-resistant protocols, and enhancement of privacy preservation techniques.

The significance of the present work extends beyond its technical achievements:

1. Industrial applications: Enables new use cases that require fast authentication, supports large-scale deployments in enterprise environments, and reduces infrastructure costs by improving efficiency.
2. Security standards: Sets new benchmarks for authentication performance, establishes a framework for dynamic security policies, and advances multi-modal biometric integration.
3. Research community: Provides the foundation for future authentication systems, introduces new methodologies for system evaluation, and establishes metrics for performance comparison.

The major research outcomes and innovations of this study are:

1. Authentication performance:
   - 99.47% accuracy (45% improvement).
   - FAR: 0.02% (75% reduction).
   - FRR: 0.15% (70% improvement).
2. System efficiency:
   - 32% reduction in CPU utilization.
   - 28% reduction in memory consumption.
   - 45% reduction in network bandwidth.
3. Scalability:
   - Linear performance scaling up to 100,000 concurrent requests.
   - Mean authentication time: 235 ms (SD=28 ms).

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number "NBU-FFR-2024-2044-01."

Portions of the research in this paper use the "CASIA-IrisV4 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA)" and a reference to "CASIA-IrisV4, http://www.cbsr.ia.ac.cn/IrisDatabase.html."

REFERENCES

[1] S. Ahmadi, "Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities," *Journal of Engineering Research and Reports*, vol. 26, no. 2, pp. 215–228, Feb. 2024, https://doi.org/10.9734/jerr/2024/v26i21083.

[2] N. Nahar, K. Andersson, O. Schelén, and S. Saguna, "A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks," *IEEE*

Access, vol. 12, pp. 94753–94764, 2024, https://doi.org/10.1109/ACCESS.2024.3425350.

[3] A. Roy, A. Dhar, and S. S. Tinny, "Strengthening IoT Cybersecurity with Zero Trust Architecture: A Comprehensive Review," *Journal of Computer Science and Information Technology*, vol. 1, no. 1, pp. 25–50, Sep. 2024, https://doi.org/10.61424/jcsit.v1i1.105.

[4] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN," *Computer Networks*, vol. 217, Nov. 2022, Art. no. 109358, https://doi.org/10.1016/j.comnet.2022.109358.

[5] H. Joshi, "Emerging Technologies Driving Zero Trust Maturity Across Industries," *IEEE Open Journal of the Computer Society*, pp. 1–12, Nov. 2024, https://doi.org/10.1109/OJCS.2024.3505056.

[6] K. Patil, B. Desai, I. Mehta, and A. Patil, "A Contemporary Approach: Zero Trust Architecture for Cloud-Based Fintech Services," *Innovative Computer Sciences Journal*, vol. 9, no. 1, Nov. 2023.

[7] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, "Verify and trust: A multidimensional survey of zero-trust security in the age of IoT," *Internet of Things*, vol. 27, Oct. 2024, Art. no. 101227, https://doi.org/10.1016/j.iot.2024.101227.

[8] P. Phiayura and S. Teerakanok, "A Comprehensive Framework for Migrating to Zero Trust Architecture," *IEEE Access*, vol. 11, pp. 19487–19511, 2023, https://doi.org/10.1109/ACCESS.2023.3248622.

[9] S. C. Llobregat, "Design of a Data Analysis Platform as a Multitenant Service in the Cloud: An Approach towards Scalability and Adaptability," M.S thesis, Dept. of Computer Systems and Computation, Technical University of Valencia, Spain, 2024.

[10] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Systems with Applications*, vol. 143, Apr. 2020, Art. no. 113114, https://doi.org/10.1016/j.eswa.2019.113114.

[11] L. Luo, P. Li, and X. Yan, "Deep Learning-Based Building Extraction from Remote Sensing Images: A Comprehensive Review," *Energies*, vol. 14, no. 23, Dec. 2021, Art. no. 7982, https://doi.org/10.3390/en14237982.

[12] H. Purohit and P. K. Ajmera, "Optimal feature level fusion for secured human authentication in multimodal biometric system," *Machine Vision and Applications*, vol. 32, no. 1, Jan. 2021, Art. no. 24, https://doi.org/10.1007/s00138-020-01146-6.

[13] P. Raj, S. Vanga, and A. Chaudhary, *Cloud-native Computing: How to Design, Develop, and Secure Microservices and Event-Driven Applications*, Hoboken, NJ, USA: John Wiley & Sons, 2022, https://doi.org/10.1002/9781119814795.

[14] U. Sumalatha, K. K. Prakasha, S. Prabhu, and V. C. Nayak, "A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection," *IEEE Access*, vol. 12, pp. 64300–64334, 2024, https://doi.org/10.1109/ACCESS.2024.3395417.

[15] N. Bala, R. Gupta, and A. Kumar, "Multimodal biometric system based on fusion techniques: a review," *Information Security Journal: A Global Perspective*, vol. 31, no. 3, pp. 289–337, May 2022, https://doi.org/10.1080/19393555.2021.1974130.

[16] S. Tiwari, R. Raja, R. S. Wadawadagi, K. Naithani, H. Raja, and D. Ingle, "Emerging Biometric Modalities and Integration Challenges," in *Online Identity - An Essential Guide*, R. Raja and A. K. Dewangan, Eds. London, UK: IntechOpen, 2024, ch. 4.

[17] R. Fabré Solà, "Edge AI on a Deep-Learning based Real-Time Face Identification and Attributes Recognition System," M.S. thesis, Polytechnic University of Catalonia, Barcelona, Spain, 2022.

[18] S. Chopparapu and J. B. Seventline, "An Efficient Multi-modal Facial Gesture-based Ensemble Classification and Reaction to Sound Framework for Large Video Sequences," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11263–11270, Aug. 2023, https://doi.org/10.48084/etasr.6087.

[19] Y. Yin, S. He, R. Zhang, H. Chang, X. Han, and J. Zhang, "Deep Learning for Iris Recognition: A Review." arXiv, Mar. 15, 2023, https://doi.org/10.48550/arXiv.2303.08514.

[20] A. O. Aljahdali, A. Habibullah, and H. Aljohani, "Efficient and Secure Access Control for IoT-based Environmental Monitoring," *Engineering, Technology & Applied Science Research*, vol. 13, no. 5, pp. 11807–11815, Oct. 2023, https://doi.org/10.48084/etasr.6193.

[21] G. B. Huang, M. Mattar, T. Berg, and E. Learned-Miller, "Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments," in *Workshop on Faces in "Real-Life" Images: Detection, Alignment, and Recognition*, Marseille, France, 2008.

[22] Z. Liu, P. Luo, X. Wang, and X. Tang, "Deep Learning Face Attributes in the Wild," in *2015 IEEE International Conference on Computer Vision*, Santiago, Chile, 2015, pp. 3730–3738, https://doi.org/10.1109/ICCV.2015.425.

[23] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2004: Third Fingerprint Verification Competition," in *Proceedings of 1st International Conference on Biometric Authentication*, Hong Kong, China, 2004, pp. 1–7, https://doi.org/10.1007/978-3-540-25948-0_1.

[24] C. I. Watson, "NIST Special Database 14 Mated Fingerprint Cards Pairs 2 Version 2." [Online]. Available: https://www.nist.gov/system/files/documents/srd/Spec-db-14.pdf.

[25] L. Omelina, J. Goga, J. Pavlovicova, M. Oravec, and B. Jansen, "A survey of iris datasets," *Image and Vision Computing*, vol. 108, Apr. 2021, Art. no. 104109, https://doi.org/10.1016/j.imavis.2021.104109.

[26] M. R. Sumi, P. Das, A. Hossain, S. Dey, and S. Schuckers, "A Comprehensive Evaluation of Iris Segmentation on Benchmarking Datasets," *Sensors*, vol. 24, no. 21, Nov. 2024, Art. no. 7079, https://doi.org/10.3390/s24217079.

[27] M. S. A. Razak, S. P. A. Gothandapani, N. Kamal, and K. Chellappan, "Presenting the Secure Collapsible Makerspace with Biometric Authentication," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12880–12886, Feb. 2024, https://doi.org/10.48084/etasr.6400.

[28] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A Survey of CNN-Based Network Intrusion Detection," *Applied Sciences*, vol. 12, no. 16, Aug. 2022, Art. no. 8162, https://doi.org/10.3390/app12168162.

[29] B. Pal, S. Mahajan, and S. Jain, "A Comparative Study of Traditional Image Fusion Techniques with a Novel Hybrid Method," in *2020 International Conference on Computational Performance Evaluation*, Shillong, India, 2020, pp. 820–825, https://doi.org/10.1109/ComPE49325.2020.9200017.

[30] S. Mai, Y. Zeng, and H. Hu, "Multimodal Information Bottleneck: Learning Minimal Sufficient Unimodal and Multimodal Representations," *IEEE Transactions on Multimedia*, vol. 25, pp. 4121–4134, 2023, https://doi.org/10.1109/TMM.2022.3171679.

[31] A. Hattab and A. Behloul, "Face-Iris multimodal biometric recognition system based on deep learning," *Multimedia Tools and Applications*, vol. 83, no. 14, pp. 43349–43376, Apr. 2024, https://doi.org/10.1007/s11042-023-17337-y.

[32] A. K. Yadav and T. Srinivasulu, "Fusion of Multimodal Biometrics of Fingerprint, Iris and Hand Written Signatures Traits using Deep Learning Technique," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 11, pp. 1627–1638, May 2021, https://doi.org/10.17762/turcomat.v12i11.6098.

[33] N. Alay and H. H. Al-Baity, "Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits," *Sensors*, vol. 20, no. 19, Oct. 2020, Art. no. 5523, https://doi.org/10.3390/s20195523.