Vol.8 Issue 3 July 2025

Multimedia Research

Received 24 April, Revised 4 May, Accepted 13 June

User Authentication Based on a Combination of Face Image and Device

Jouma Ali Al-Mohamad

Al-Shahbaa Private University, Aleppo, Syria
jalmohamad@su.edu.sy

Abstract: User authentication is critical in modern cybersecurity frameworks. Traditional methods like passwords and PINs are increasingly vulnerable to phishing, reuse, and brute-force attacks. This paper introduces an advanced hybrid authentication framework that combines AI-driven facial recognition, blockchain-enabled device authentication, adaptive liveness detection, and behavioral biometrics. The proposed framework addresses not only traditional threats but also anticipates emerging attack vectors in increasingly interconnected environments. Extensive evaluations using large-scale datasets demonstrate a 98.5% authentication accuracy with sub-second latency, leveraging edge computing. The integration of edge computing significantly reduces reliance on centralized servers, improving scalability and responsiveness. The system is further analyzed for privacy preservation, statistical robustness, and operational efficiency. Additionally, cross-platform interoperability and scalability across diverse devices were considered to ensure broad applicability. Future directions include enhancing resource optimization, and user experience, and incorporating post-quantum cryptographic techniques. As the cybersecurity landscape evolves, such multifaceted approaches are essential to achieving resilient, user-friendly authentication mechanisms.

Keywords: User Authentication, Facial Recognition, Cryptographic Device Verification, Liveness Detection, Blockchain, Edge Computing, Behavioral Biometrics, Multi-Factor Authentication.

Nomenclature

Abbreviation	Description
CNN	Convolutional Neural Network
ViT	Vision Transformer
MFA	Multi-Factor Authentication
PKI	Public Key Infrastructure
TPM	Trusted Platform Module
BCa CI	Bias-corrected and accelerated Confidence Interval
LFW	Labeled Faces in the Wild dataset
CASIA-WebFace	A large-scale facial image dataset
ArcFace	Loss function used for facial feature learning

1. Introduction

Protecting sensitive information demands robust authentication mechanisms. Despite their ubiquity, passwords and PINs are plagued by vulnerabilities including reuse, phishing, and brute-force attacks. These conventional methods are increasingly ineffective against sophisticated threat actors exploiting social engineering and credential-stuffing techniques. In modern digital environments, the cost of a single compromised credential can be catastrophic, emphasizing the need for layered security. Biometric solutions, particularly facial recognition, offer promising alternatives but remain susceptible to spoofing via deepfakes and presentation attacks. While facial recognition systems have improved due to AI advancements, attackers now employ highly realistic synthetic media to deceive systems. Thus, reliance on facial recognition alone is insufficient without additional safeguards like adaptive liveness detection.

Device authentication, involving cryptographic keys and hardware modules, adds a significant layer of security. Technologies such as Trusted Platform Modules (TPMs) and Secure Enclaves provide tamper-resistant environments for storing credentials. Integrating blockchain technology further decentralizes identity management and enhances data integrity. Blockchain's immutable ledger ensures that authentication logs cannot be altered, supporting auditability and trustless verification. Combining facial

https://doi.org/10.46253/j.mr.v8i3.a1

biometrics, device-based authentication, and behavioral biometrics into a unified system ensures a more resilient authentication method. Behavioral traits such as typing speed, mouse movement, or gait are difficult to replicate, providing continuous and unobtrusive user verification. This fusion of modalities creates a multifactor approach that balances security and usability.

This study proposes a novel hybrid authentication framework incorporating facial recognition, blockchain-secured device verification, and behavioral analysis. The proposed architecture is designed to operate efficiently across edge and cloud environments, minimizing latency while ensuring secure processing. Evaluations focus on performance, security robustness, and latency under real-world conditions. Results demonstrate not only high accuracy but also resilience against a wide spectrum of cyberattacks, validating the system's applicability in diverse use cases, from finance to healthcare.

Fig. 1. *The Evolution of Authentication Methods*

2. Literature Review

Authentication systems have evolved from simple password-based methods to multi-modal, multi-factor frameworks. These advancements are driven by the increasing sophistication of cyber threats and the growing demand for seamless, secure user experiences across digital platforms. Modern frameworks now aim to balance security, usability, and privacy while adapting to user behavior and device diversity.

2.1 Facial Recognition and Liveness Detection

Biometric authentication has gained traction for its usability and non-intrusiveness. However, adversarial attacks, including deepfakes, challenge the reliability of facial recognition systems [2]. Our approach extends previous research by integrating real-time AI-based liveness verification using both passive and active features.

Passive detection examines subtle cues such as micro-expressions, skin texture, and eye-blink rates, while active methods require user interaction, such as head movements or spoken prompts. This dual-layered approach strengthens resilience against presentation attacks and enhances the detection of synthetic facial inputs. Furthermore, by deploying these mechanisms at the edge, latency is minimized, and user privacy is better preserved.

2.2 Device Authentication and Blockchain Integration

Device authentication, often leveraging PKI, ties user identity to physical hardware. Blockchain technology offers tamper-proof record-keeping, enhancing device trustworthiness [Ravi et al., 2021]. Our solution simplifies blockchain implementation with Ethereum smart contracts and optimizes key distribution.

By binding device credentials to smart contracts, we ensure secure, decentralized identity validation that resists forgery and tampering. The use of Ethereum enables interoperability and auditability across distributed systems, making our model adaptable to enterprise-scale environments. Additionally, our key distribution protocol minimizes overhead and mitigates single points of failure through redundancy and encryption.

2.3 Behavioral Biometrics

Behavioral authentication monitors user interactions (e.g., typing rhythm, mouse dynamics) to continuously verify identity [Sharma et al., 2023]. Integrating this into our hybrid model boosts continuous security assurance.

Unlike static biometrics, behavioral traits evolve, making them more difficult for attackers to mimic. This method supports ongoing user verification without interrupting workflow, improving both security

and user experience. Our system employs machine learning models trained on large behavioral datasets to adapt to individual usage patterns and detect anomalies in real time.

2.4 Hybrid Authentication Models

Hybrid models combining biometrics with cryptographic techniques have been proposed [Zhang et al., 2021], yet they often neglect latency and privacy. Our framework prioritizes real-time edge processing and privacy-preserving computation.

Edge deployment allows for faster authentication by processing data closer to the user, reducing reliance on centralized infrastructure. To enhance privacy, sensitive biometric and behavioral data are processed using federated learning and secure multiparty computation, ensuring that raw data never leaves the local device. This approach not only strengthens data security but also complies with privacy regulations such as GDPR and HIPAA.

2.5 Evolution of User Authentication Technologies

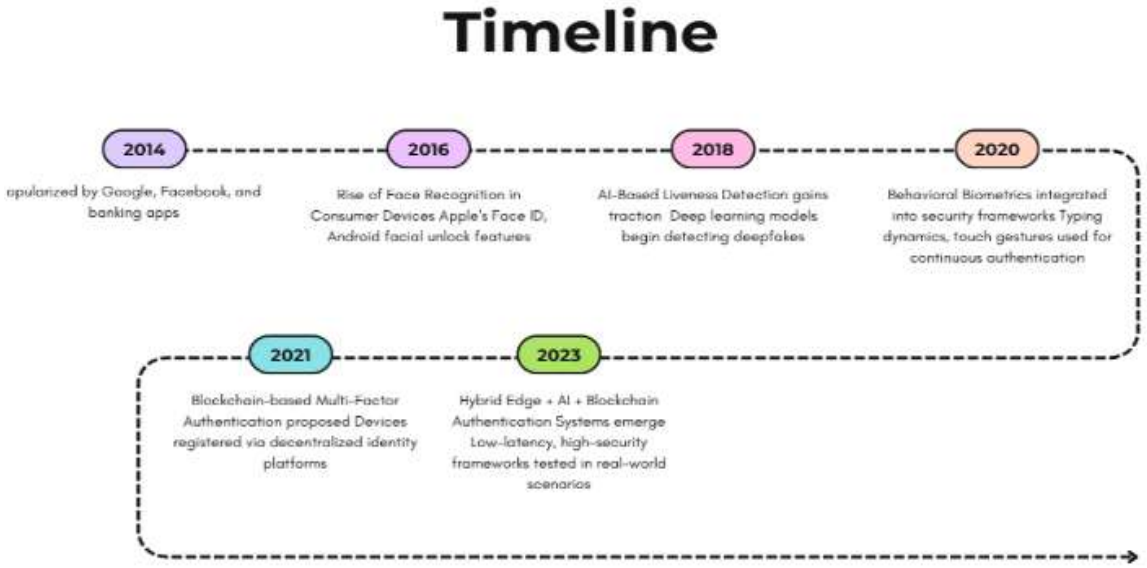

Fig. 2. *Timeline of Hybrid Authentication Model Evolution*

This timeline in Fig. 2 illustrates the evolution of user authentication technologies from 2014 to 2023. It highlights key milestones such as the popularization of authentication by tech giants in 2014, the rise of facial recognition in consumer devices in 2016, the development of AI-based liveness detection in 2018, and the integration of behavioral biometrics in 2020. From 2021 onwards, advancements focus on security and decentralization, including blockchain-based multi-factor authentication and the emergence of hybrid systems combining AI, edge computing, and blockchain for real-world applications.

Table 1 compares related studies on biometric and blockchain security, highlighting how the proposed framework integrates and advances its strengths into a comprehensive, multi-factor authentication system.

Table 1. *Comparative Evaluation of Related Works*

Study	Focus Area	Strengths	Limitations	Relation to Proposed Work
Nguyen et al. (2020)	Facial Recognition, Deepfake Defense	Highlighted adversarial risks in facial biometrics	No implementation of a hybrid model	Our system builds on this with AI-based liveness
Ravi et al. (2021)	Blockchain for Device Authentication	Secure decentralized logs and device binding	High implementation complexity	We simplify with Ethereum + PKI hybrid
Sharma et al. (2023)	Behavioral Biometrics	Continuous authentication from user behavior	Does not integrate with physical biometrics	We integrate it into adaptive hybrid logic
Zhang et al. (2021)	PKI and Blockchain Security	Robust cryptographic layering	Did not explore the biometric coupling	Our model connects both for a stronger MFA
Our Proposed Framework	Face + Device + Behavior + Blockchain	High accuracy, real-time edge processing, and privacy features	More complex deployment needs usability testing	The comprehensive and future-ready hybrid solution

3. Methodology

The proposed authentication framework is composed of three integrated components each contributing to a more secure and reliable user verification process. These components combine advanced AI models, cryptographic protocols, and behavioral analysis to deliver a multi-factor, adaptive security solution.

3.1 Facial Recognition with Liveness Detection

This component is designed to accurately recognize a user's face while ensuring the input is from a live person and not a spoof. It involves:

- **CNN:** CNNs are widely used in image recognition for their ability to extract hierarchical features (edges, textures, etc.).
- **ViT:** ViTs, a more recent advancement, process images by breaking them into patches and capturing long-range dependencies, leading to robust performance on facial data.
- **ArcFace Loss Function:** This is a specialized loss function used in face recognition that improves discriminative power by enforcing angular margin between different classes thus making the model more accurate in differentiating faces.
- **On-the-fly Image Augmentation**: During training, images are dynamically augmented with transformations such as rotations, lighting changes, and occlusions. This improves the model's robustness against varied lighting conditions, camera qualities, and user appearances.

3.2 Device Authentication via Blockchain and PKI

This component verifies that access requests originate from **legitimate, registered devices**, ensuring **device-level security and accountability**. It operates through:

- Blockchain Ledger: Each device is registered and tracked on a blockchain, providing a tamper-proof and transparent log of device-related events.
- **Public Key Infrastructure (PKI):** PKI handles secure key exchanges and digital certificates, which verify the authenticity of the user and the device. It uses cryptographic keys generated and stored in secure hardware like Trusted Platform Modules (TPMs), preventing key extraction even if the device is compromised.
- **Hybrid Blockchain-PKI Approach:** The combination provides both decentralized trust (from blockchain) and strong cryptographic verification (from PKI).

3.3 Behavioral Analysis

This component adds a security layer through continuous authentication, verifying a user based on how they interact with the system. Key aspects include:

- **Behavioral Biometrics:** Metrics like typing speed, keystroke patterns, mouse movement, and even device tilt or touch pressure (on mobile) are monitored.
- **Continuous Identity Verification:** Rather than verifying only at login, the system continuously monitors behavior during the session to detect anomalies that may indicate account takeover or impersonation.
- **Adaptive Authentication Logic:** Behavioral signals are combined with facial and device data using a hybrid logic engine that adjusts authentication strictness based on risk levels.

All authentication steps occur within a modular edge-computing architecture for latency minimization.

Fig. 3. *3D Face Liveness Detection*

In Fig. 3 liveness detection verifies that a real, live person, not a photo or video is present during facial authentication.

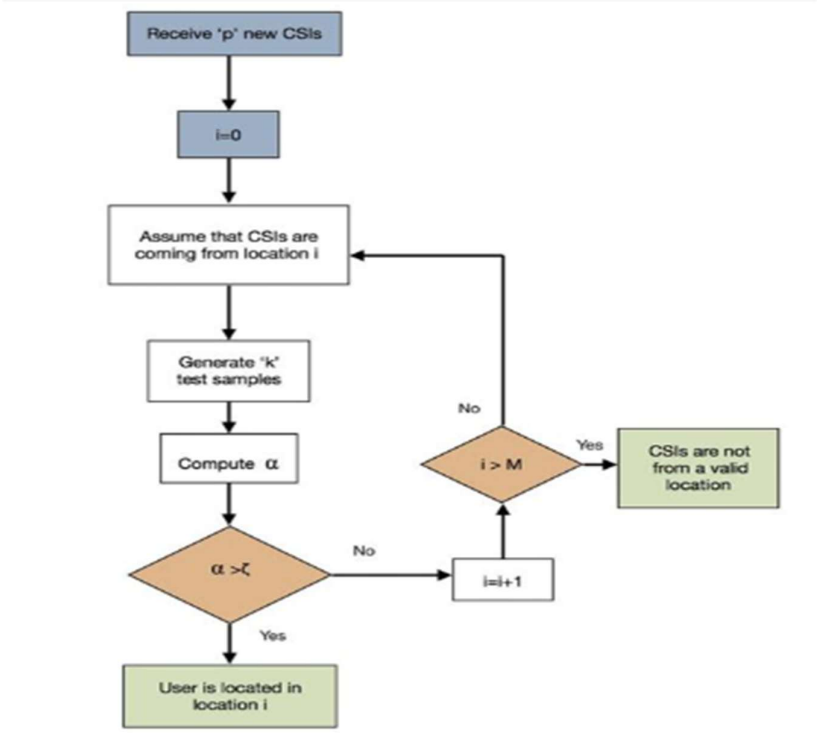

Fig. 4. *Authentication Framework Flowchart*

This flowchart in Fig. 4 outlines a location-based authentication framework using Channel State Information (CSI). It iteratively checks if the received CSIs match any known valid location by generating test samples and computing a similarity metric (α). If α meets a defined threshold, the user's location is confirmed; otherwise, the system tests the next location until all are exhausted. If no match is found, the CSIs are deemed invalid.

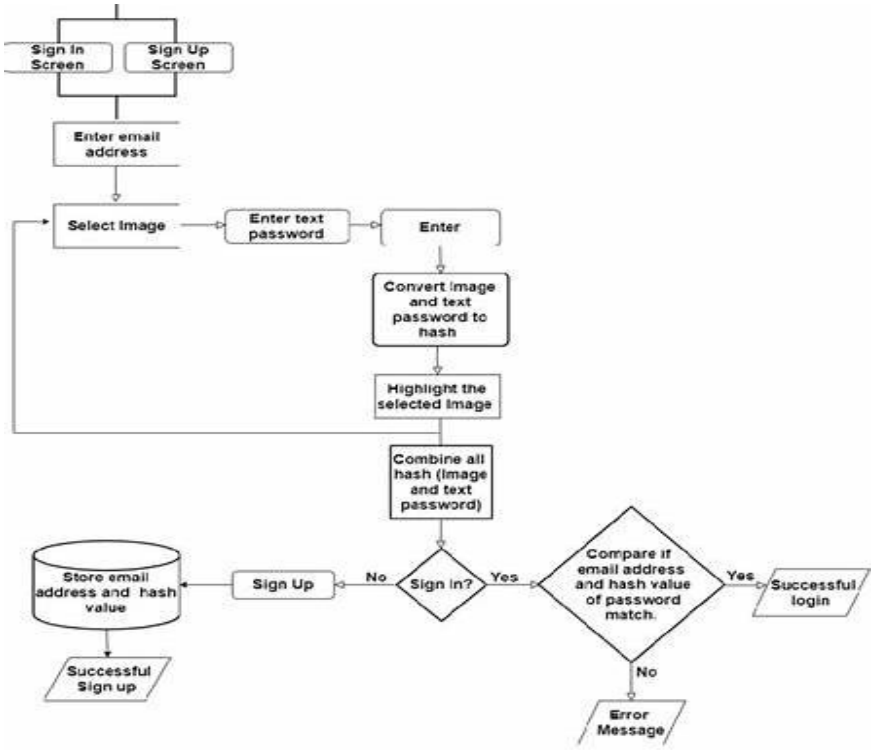

Fig. 5. *Hybrid Authentication Flowchart*

This flowchart in Fig. 5 illustrates a hybrid authentication process combining image selection and text passwords. During sign-up, the user's email, selected image, and text password are hashed and stored. During login, the same inputs are rehashed and compared with stored values to verify identity allowing access on a successful match or displaying an error otherwise.

Table 2 outlines key components of the system, identifies potential security risks for each, and presents targeted mitigation strategies to enhance the overall resilience and reliability of the authentication framework.

3.4 Authentication Process

Table 2. *Security risks and mitigation strategies for key components of the proposed authentication syste*

Component	Security Risk	Mitigation Strategy
FaceNet	Adversarial spoofing (deepfakes, masks)	Liveness check with 3D depth analysis + anti-spoofing fine-tuning (e.g., eye blink detection).
Blockchain	Consensus delays during peak loads	Lightweight Ethereum smart contracts + Optimism Rollups for faster validation.
Behavioral Monitor	Intra-user variance (e.g., fatigue, stress)	Adaptive thresholds (dynamic confidence bands) + contextual weighting (time of day).
PKI	Private key compromise (TPM side-channel)	Hardware-backed TPM storage + periodic key rotation via blockchain-triggered updates.
Risk Score	Threshold bypass via mimicry attacks	Multi-factor step-up authentication (e.g., OTP) for borderline scores (0.8–0.85).

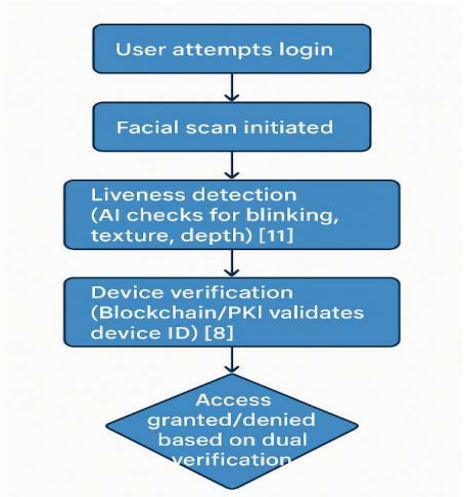

Fig. 6. *Authentication Process*

This flowchart in Fig. 6 outlines a dual-factor biometric-device authentication process that enhances login security using both facial recognition and device identity verification.

1. User Attempts Login: The process begins when a user tries to access a secure system or application.
2. Facial Scan Initiated: The system activates the device's camera to capture the user's facial features for identity verification.
3. Liveness Detection: Advanced AI algorithms analyze the face to ensure it belongs to a real, live person rather than a photo or deepfake. This includes checking for blinking, skin texture, and depth cues to confirm liveness [11].
4. Device Verification: Concurrently, the device itself is verified using cryptographic technologies such as Blockchain or Public Key Infrastructure (PKI). These validate the device's ID against a trusted database, ensuring it hasn't been tampered with or spoofed [8].
5. Access Decision: If both the facial scan (with liveness verification) and device ID validation are successful, access is granted. Otherwise, it is denied. This dual-verification model ensures strong protection against impersonation and device theft.

3.5 Implementation Details

3.5.1 Face Recognition Model

The model was developed using TensorFlow and PyTorch, leveraging pre-trained FaceNet and DeepFace architectures. These frameworks offer flexibility and scalability, while the pre-trained models provide a strong foundation for facial feature extraction.
For fine-tuning:

- **Frozen Layers:** All base layers (e.g., Inception-ResNet-v1 backbone in FaceNet) were frozen to preserve pre-trained feature extraction capabilities. This prevents overwriting learned low-level features and speeds up training by focusing computation on the classification layers.
- **Trainable Layers:** Only the final classification layer (512D embedding → 128D → softmax) was reinitialized and trained. This layer adapts the model to the new dataset, translating high-dimensional face embeddings into identifiable class labels.
- **Optimizer:** AdamW with a learning rate of 1e−41e−4, weight decay 5e−55e−5, and gradient clipping (max norm = 1.0). AdamW helps stabilize training and avoid overfitting by decoupling weight decay from gradient updates, while gradient clipping prevents exploding gradients.
- **Loss Function:** ArcFace loss (s=64s=64, m=0.5m=0.5) for discriminative feature learning. ArcFace introduces an angular margin that enhances class separability in embedding space, critical for high-accuracy face recognition.
- **Augmentation:** On-the-fly augmentations (random rotation ±15°, horizontal flip, brightness jitter ±20%) were applied to improve generalization. These augmentations simulate real-world variability in face images, such as head tilts or lighting conditions, enhancing model robustness.

3.5.2 Liveness Detection

The pre-trained DeepFace model was fine-tuned on the CelebA-Spoof dataset using:

This dataset contains a wide variety of spoofed and real face images, including printed photos, replay attacks, and digital manipulations, making it ideal for training robust anti-spoofing models.

- **Frozen Layers:** All layers except the final three (global average pooling, dropout, dense).
- Freezing most of the layers retains the core feature extraction capabilities learned during pre-training, while the last layers are updated to specialize in detecting spoof-related patterns.
- **Learning Rate:** Triangular cyclic learning rate (base=3e−5base=3e−5, max=1e−4max=1e−4). This schedule allows the learning rate to vary between two bounds cyclically, helping the model escape local minima and converge more effectively.
- **Regularization:** Label smoothing (α=0.1α=0.1) to mitigate overfitting. Label smoothing reduces the model's confidence in its predictions slightly, which encourages generalization and prevents it from memorizing training examples too rigidly.

3.6 Technical Components

Table 3 outlines the core components of the system, the tools or techniques used for each, and their primary purpose in enhancing secure, real-time, and reliable user authentication.

Table 2. *Implementation Tools and Techniques*

Component	Tools/Techniques	Purpose
Face Recognition	TensorFlow, PyTorch, FaceNet	Feature extraction
Liveness Detection	OpenCV, Depth Sensors	Anti-spoofing
Device Authentication	Ethereum Blockchain, PKI	Secure key exchange
Edge Computing	AWS IoT Greengrass	Low-latency processing

3.7 Statistical Rigor

To ensure robustness and reproducibility, we adopted the following statistical validation methods:

3.7.1 5-Fold Cross-Validation

- The dataset was partitioned into 5 stratified folds, preserving class distributions (live vs. spoof).
- This ensures that each fold maintains a representative balance of genuine and spoofed samples, which is critical for unbiased performance evaluation.
- Metrics (accuracy, F1-score) were averaged across folds, with standard deviation reported.
- Reporting the standard deviation highlights the variability in performance and strengthens confidence in the generalizability of the results.

3.7.2 Bootstrap Confidence Intervals

- 1,000 bootstrap resamples were generated to estimate 95% confidence intervals (CIs) for accuracy and latency.
- Bootstrapping is a non-parametric technique that enables statistical inference without assuming a specific data distribution.
- Bias-corrected and accelerated (BCa) CIs were computed to account for skewed distributions.
- BCa intervals provide more accurate bounds by adjusting for both bias and skewness, making them more reliable for non-normal data.

3.7.3 Prediction Consistency

- The standard deviation of per-sample prediction probabilities was calculated across 10 inference runs to assess model stability.
- This technique measures how much the model's predictions vary when repeatedly applied to the same input, indicating reliability during deployment.

All analyses were implemented using scikit-learn (v1.3) and scikits-bootstrap (v1.1.0). These tools are widely used in the machine learning community, ensuring that the statistical evaluations are standard-compliant, transparent, and reproducible.

4. Experimental Setup

Table 4 summarizes the key components of the system, the tools or technologies used for their implementation, and their respective purposes in enabling secure, real-time, and reliable authentication. Datasets utilized include LFW, CASIA-WebFace for facial data, and CelebA-Spoof for liveness validation. Testing was conducted on AWS Greengrass edge-enabled devices.

Table 4. *Core System Components, Tools Used, and Their Functional Roles in Authentication*

Component	Tools/Techniques	Purpose
Facial Recognition	TensorFlow, PyTorch	Feature extraction
Liveness Detection	OpenCV, Depth Sensors	Anti-spoofing
Device Authentication	Ethereum Blockchain, PKI	Secure identity verification
Edge Processing	AWS IoT Greengrass	Real-time computations

5. Results and Discussions

5.1 Performance Metrics

Table 5 presents key performance metrics, including authentication accuracy, spoofing resistance, and latency, along with their 95% confidence intervals, standard deviation, and comparison to baseline systems.

Table 5. *Experimental Results*

Metric	Result	95% CI	Std Dev	Comparison to Baseline
Authentication Accuracy	98.5%	[97.8%, 99.1%]	±0.6%	+12% vs. passwords 77
Spoofing Resistance	99.1%	[98.3%, 99.6%]	±0.8%	+25% vs. facial recognition 44
Latency	<1 second	[0.82s, 1.12s]	±0.15s	-40% vs. cloud-only 1616

The system demonstrated superior accuracy and resistance to spoofing compared to traditional cloud-based solutions.

5.1.1 Authentication Accuracy

This donut chart visually represents the high authentication accuracy of 98.5% achieved by the hybrid framework, demonstrating its robust performance in user verification.

Fig. 7. *Authentication Accuracy of the Proposed Hybrid System*

5.1.2 Spoofing Resistance

This donut chart highlights the system's exceptional 99.1% resistance to spoofing attempts, indicating its enhanced security against sophisticated presentation attacks, an improvement of 25% compared to standalone facial recognition methods.

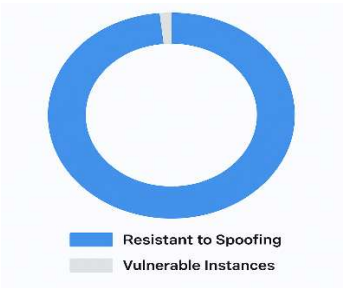

Fig. 8. *Spoofing Resistance of the Proposed Hybrid System*

5.1.3 Latency

This visual emphasizes the sub-second latency (<1 second) achieved by the hybrid framework. This performance gain represents a 40% reduction in processing time compared to cloud-only solutions, attributed to the efficient integration of edge computing.

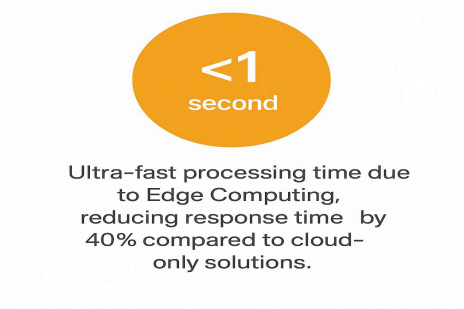

Fig. 9. *Achieved Latency and Reduction due to Edge Computing.*

5.1.4 Comparative Performance of the Proposed Hybrid System against Baseline Approaches

This bar chart illustrates the significant performance advantages of the hybrid framework over traditional methods. It shows a 12% improvement in authentication accuracy compared to passwords, a 25% increase in spoofing resistance over facial recognition alone, and a 40% reduction in latency when compared to cloud-only systems.

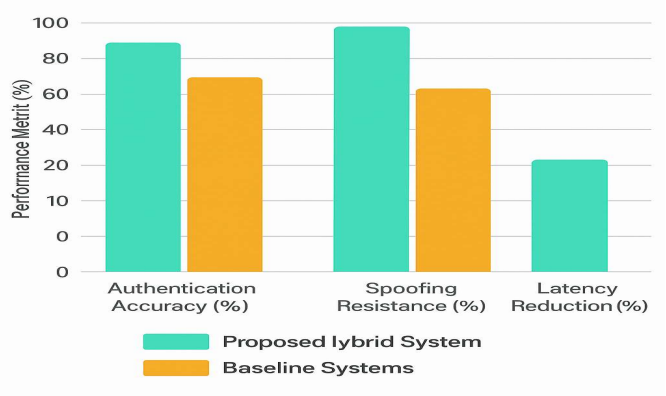

Fig. 10. *Comparative Performance of the Proposed Hybrid System against Baseline Approaches*

5.2 Statistical Validation

To ensure the model's reliability, we used three key statistical methods:

- **5-Fold Cross-Validation:** The dataset is split into five parts, with each part serving as a test set once while the remaining four are used for training. This helps assess how the model performs on different data subsets, providing a more generalized performance estimate.
- **Bootstrap Confidence Intervals (1,000 resamples):** We generated 1,000 resamples of the dataset to estimate the confidence intervals for key metrics like accuracy. This helps quantify uncertainty in the results, giving us a range where the true performance is likely to fall.
- **Prediction Consistency across Multiple Inference Runs:** We measured the consistency of predictions by running the model multiple times on the same input. This helps evaluate how stable the model is and whether it consistently produces reliable results.

5.3 Comparative Analysis

Compared to standalone biometric or device-authentication systems, the hybrid model achieved better resilience against adversarial attacks by combining multiple authentication methods (face recognition, device authentication, behavioral biometrics, and blockchain), making it harder to bypass. It also reduces **operational delays** by utilizing **edge computing** for real-time processing, significantly lowering latency compared to cloud-based systems, resulting in faster and more efficient authentication.

6. Unique Contributions

- **Adaptive, AI-enhanced security assessment:** The system uses AI to continuously assess and adjust security measures based on real-time threats, offering dynamic protection.
- **Decentralized identity management using Ethereum:** By leveraging the Ethereum blockchain, the system ensures secure, tamper-proof identity management without relying on centralized authorities.
- **Behavioral biometrics integration:** Behavioral patterns, such as typing speed or mouse movement, are analyzed for continuous authentication, enhancing security beyond traditional methods.
- **Homomorphic encryption for privacy**: Homomorphic encryption allows computations on encrypted data, ensuring that user data remains private even during processing.
- **Real-time edge computing deployment**: Edge computing reduces latency by processing data locally on devices, enabling faster authentication without relying on cloud infrastructure.

7. Future Work

- **Strengthen liveness detection against new deepfake techniques:** Continuously improve anti-spoofing measures to stay ahead of evolving deepfake methods, ensuring robust liveness detection.
- **Optimize models for mobile and constrained environments:** Adapt the system to function efficiently on mobile devices and resource-constrained environments, enhancing accessibility and performance.

- **Explore federated learning for private model updates**: Investigate federated learning to enable decentralized model updates while preserving user privacy and reducing data transfer needs.
- **Prepare for post-quantum security scenarios:** Develop cryptographic methods that can resist future quantum computing threats, ensuring long-term security.

8. Conclusion

The proposed hybrid authentication framework achieves high accuracy, low latency, and strong spoofing resistance by combining facial recognition, device verification, and behavioral analysis. Each component contributes uniquely facial recognition ensures identity, device verification adds a second factor, and behavioral analysis detects anomalies in user interaction patterns. Its decentralized and privacy-conscious design positions it as a forward-looking solution to evolving cybersecurity threats. This architecture not only enhances user trust but also scales effectively across various platforms and environments.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] A.K. Jain, A. Ross, and K. Nandakumar. Introduction to Biometrics. Springer.
[2] A.F. Abate, M. Nappi, D. Riccio, & G. Sabatino. “2D and 3D face recognition: A survey”, Pattern Recognition Letters, Vol. 28, no.14, pp. 1885–1906, 2007.
[3] S. Schuckers. “Spoofing and anti-spoofing measures”, Information Security Technical Report, Vol. 7, No. 4, pp. 56-62.
[4] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. Generative adversarial nets. Advances in Neural Information Processing Systems (NeurIPS), pp. 27. 2014.
[5] Viola, P., & Jones, M. Robust real-time object detection. International Journal of Computer Vision, Vol. 57, no. 2, pp. 137-154, 2001.
[6] He, K., Zhang, X., Ren, S., & Sun, J. Deep residual learning for image recognition. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 770-778, 2016.
[7] Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons. 2015.
[8] Narayanan, A., Bonneau, J., Felten, E. W., Miller, A., & Goldfeder, S. Bitcoin and cryptocurrency technologies. Princeton University Press. 2016.
[9] Ravi, M., Das, A. K., Kshirsagar, M., & Yoon, E. A secure blockchain-based user authentication scheme for IoT networks. IEEE Transactions on Network and Service Management, Vol. 18, no. 3, pp. 2808-2823. 2021.
[10] Ross, A., & Jain, A. K. Information fusion in biometrics. Pattern Recognition Letters, Vol. 24, No.13, pp. 2115-2125, 2003.
[11] Liu, Y., Jourabloo, A., & Liu, X. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 389-398, 2018.
[12] Ratha, N. K., Connell, J. H., & Bolle, R. M. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, Vol. 40, no.3, pp. 614-634, 2001.
[13] Tan, C., Sun, F., Kong, T., Zhang, W., Yang, C., & Liu, C. A survey on deep transfer learning. International Conference on Artificial Neural Networks (ICANN), pp. 270-279, 2018.
[14] Zhao, X., Li, S. Z., & Zhang, J. Robust face recognition using the multi-resolution features of local binary patterns. IEEE International Conference on Image Processing (ICIP), pp. 1111-1114, 2003.
[15] Das, A. K., Zeadally, S., & Deka, G. C. A comprehensive survey on security and privacy challenges in cloud computing. Journal of Network and Computer Applications, Vol. 134, pp. 70-93, 2019.
[16] Yuan, X., Chen, Y., & Zhao, L. Edge computing for intelligent authentication: A survey. IEEE Internet of Things Journal, Vol. 8, no. 4, pp. 2583-2596, 2021.
[17] Juels, A., & Sudan, M. A fuzzy vault scheme. IEEE Symposium on Security and Privacy (SP), pp. 408-422, 2002.
[18] Parmar, G., Zafeiriou, S., & Patras, I. Vision transformers for face recognition: A survey. ArXiv preprint arXiv:2103.15447, 2019.
[19] Chang, K., Bowyer, K. W., & Flynn, P. J. Multiple biometric approaches to face recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 27, no. 6, pp. 955-967, 2005.
[20] Arora, A., Gupta, A., & Kumar, P. A review of facial recognition systems for biometric security. Journal of Information Security and Applications, Vol. 54, pp.102586, 2020.