Attack Detection for Facial Recognization System

Rahul Bembade[1], Ranjeet Patil[2], Sumeet Hinge[3], Varad Virdhe[4]
[1]*Associate Professor,CSE-CSF. MITADT University Pune, India*
[2,3,4] *Student, CSE-CORE. MITADT University Pune, India*

Abstract— **This paper presents an enhanced facial recognition security system that integrates biometric authentication with real-time intrusion detection and multi- channel alert mechanisms. The system addresses critical security challenges in access control by combining powerful deep learning models, specifically Convolutional Neural Networks (CNNs), for accurate recognition with multi-modal anti-spoofing techniques to prevent fraudulent attempts [3, 13, 14]. A parallel Intrusion Detection System (IDS) monitors background processes, critical files, and network activity to identify and block cyberattacks, ensuring holistic security [4, 5]. The proposed solution provides comprehensive, real-time security monitoring with instant alerts delivered through multiple communication channels (email, sound, desktop notifications). This integrated system is specifically designed for deployment in high-security environments where both physical access control and digital system security are crucial for mitigating diverse security risks**

Index Terms—**Facial Recognition, Anti-Spoofing, Intrusion Detection System, Biometric Security, Computer Vision, Deep Learning, Cybersecurity, Multi-Factor Authentication**

I. INTRODUCTION

Conventional access control systems, relying on simple passwords, ID cards, or physical credentials, are inherently vulnerable to unauthorized access and manipulation. While facial recognition technology offers a superior, touchless, and convenient alternative for identity verification [2], even advanced biometric systems face dual threat vectors:
presentation attacks (spoofing) and system-level cyber intrusions [10]. Spoofing remains a persistent challenge, requiring sophisticated liveness detection, and the integrity of the underlying security system itself must be protected from external hacks or internal tampering.
This project proposes an innovative system that integrates three crucial security layers: accurate CNN-based facial recognition, real-time multi-modal anti-spoofing, and a system-wide Intrusion Detection System (IDS). The core objective is to establish a robust, multi-layered solution that not only ensures quick and accurate biometric authentication but also concurrently monitors for and responds to underlying system threats in real-time [17]. This holistic approach significantly improves the reliability and resilience of the security framework, making it ideal for sensitive operational and data environments. Recent advancements in Deep Learning, particularly CNNs and transformer-based models, have made such real-time, high-accuracy systems possible.

II. PROPOSED SYSTEM

The proposed system represents an architectural synthesis of multiple specialized security modules designed to operate within a unified, secure framework. It elevates security beyond basic authentication by incorporating concurrent system-level threat monitoring

2.1.System Modules

The core architecture is built upon five integrated modules that interact seamlessly:

- Facial Recognition Module: Responsible for real-time identification and verification of authorized individuals using deep learning models.
- Anti-Spoofing Detection Module: Dedicated to

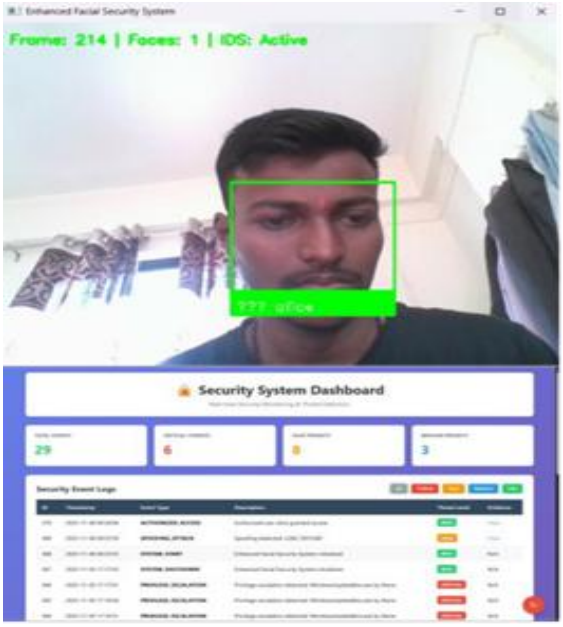
detecting presentation attacks (photos, videos, masks) using multi-modal analysis techniques [13].

- Intrusion Detection System (IDS): Operates in parallel to continuously monitor for cyber threats and suspicious host activity [4].
- Multi-Channel Alerting Module: Manages the instant generation and reliable delivery of security notifications.
- Secure Database Logging Module: Handles the encrypted storage of biometric data (encodings) and all security event logs.

2.2.Working Principle

The system's secure operation is initiated when the camera captures a live video feed. This process immediately splits into two parallel security streams:

1. Biometric Authentication and Liveness: The video feed is processed instantly by the Facial Recognition Module to verify the user's identity. Concurrently, the Anti-Spoofing Module executes its analysis, checking for presentation attacks by analyzing subtle features like texture, color, and motion [13, 18].
2. System Integrity Monitoring: The Intrusion Detection Module runs continuously in the background [4]. It monitors for malicious activity across background processes, critical files, and network connections [4].
3. Response Protocol: If the system detects any anomaly, a spoofing attempt, or unauthorized access, the Alert System instantly triggers notifications via email, sound, and desktop alerts. All incidents are simultaneously recorded and logged with forensic data in a secure database, ensuring accountability.



III. SYSTEM DESIGN

The system design adheres to principles of modularity, scalability, and robust data privacy. The

framework is constructed so that each major functional block
operates largely independently, which is crucial for flexibility and resilience.
Security is architecturally prioritized: high- dimensional face encodings are stored as encrypted numerical vectors rather than raw images, significantly enhancing privacy protection and compliance [19]. The system is engineered for real- time authentication performance, targeting a verification latency of under 500 milliseconds, enabling efficient, high-speed access control [7]. All
operational and security events are meticulously recorded in a secure local database to maintain a comprehensive and unalterable audit trail for post- incident forensic analysis [5].

IV. SYSTEM IMPLEMENTATION

The system is developed primarily in the Python programming language, leveraging its ecosystem for deep learning and system monitoring.
The implementation relies on established libraries such as OpenCV for fast video processing, dlib for facial feature correlation, psutil for low-level system monitoring, and the Flask framework for the secure system interface. The Facial Recognition Module utilizes pre-trained Deep Convolutional Neural Network (CNN) models to generate highly discriminative face embeddings, ensuring both reliable and accurate identification even in sub-optimal conditions [3, 16].

The Intrusion Detection System (IDS) module is implemented using real-time process and network analysis capabilities provided by system tools like psutil, which constantly tracks for predefined suspicious behaviors or unauthorized system changes. The Alert System is designed for high reliability, providing multi-channel notifications with customizable configurable severity levels. Finally, all security logs and access attempts are securely stored in an SQLite database, guaranteeing event traceability and accountability.

V. EXECUTION

The execution phase of the system involves the instantaneous and concurrent activation of its security layers. Upon launch, the system automatically activates the camera, bringing the biometric modules to the foreground for real-time authentication and anti- spoofing detection.
Simultaneously, the Intrusion Detection Module runs as a persistent, background process [4]. This dedicated process continuously screens the host system for any indicators of compromise, including suspicious process injections, privilege escalation attempts, or unauthorized network traffic indicative of a cyberattack [4]. This seamless, dual-layer operation ensures that both the physical access point and the underlying operating system are continuously monitored and secured. Any security event, whether a physical spoof or a digital threat, triggers instant alerts and logs the incident immediately for mitigation and review [5].

VI. CONCLUSION

The Enhanced Facial Recognition Security System successfully fulfills its objective by integrating a robust biometric authentication layer with critical cybersecurity monitoring, establishing a truly comprehensive and multi-layered security framework. By utilizing deep CNNs for recognition, multi-modal techniques for anti-spoofing, and a parallel IDS, the solution effectively mitigates a wide range of threats—from presentation attacks to cyber intrusions—all while maintaining the real-time performance essential for operational security [7, 10].

Future Scope

To further advance the system's robustness, accuracy, and operational reach, the following areas are planned for future development:

- 3D Spoofing Detection: Integrating advanced techniques, such as depth-map analysis, to detect sophisticated 3D-printed masks and other high-fidelity presentation attacks [13].
- ML-based Anomaly Detection: Implementing machine learning algorithms within the IDS to

establish baselines of normal user/system behavior and identify subtle, novel anomalies that may indicate emerging zero-day threats [20].

- Multi-Camera Support: Scaling the current architecture to natively support and manage multi-camera inputs for robust, distributed security across large-scale deployment environments [12].

REFERENCES

[1] Zhao, W., Chellappa, R., Phillips, P. J., and Rosenfeld, A. 'Face recognition: A literature survey,' ACM Computing Surveys, 35(4), 2003, 399-458.

[2] Turk, M. and Pentland, A. 'Eigenfaces for recognition,' Journal of Cognitive Neuroscience, 3(1), 1991, 71-86.

[3] Taigman, Y. et al. 'DeepFace: Closing the gap to human-level performance in face verification,' IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2014.

[4] Roesch, M. 'Snort: Lightweight intrusion detection for networks,' USENIX Conference on Systems Administration (LISA), 1999.

[5] Cichonski, P. et al. 'Computer security incident handling guide,' NIST Special Publication 800-61, Revision 2, 2012.

[6] Liu, X. et al. 'Learning deep models for face anti- spoofing: Binary or auxiliary supervision,' IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018, 1389-1398.

[7] Dlib Library. 'Dlib C++ Library: Face Recognition,' King, D. E., 2009.

[8] Siddiqui, T. et al. 'An advanced approach for facial liveness detection using texture and deep learning,' Journal of King Saud University - Computer and Information Sciences, 2024.

[9] Ranjan, R., Sankaranarayanan, S., & Chen, J. C. 'Deep learning approach for real-time face recognition on embedded devices,' IEEE Internet of Things Journal, 2023.

[10] Atoum, Y. et al. 'Face anti-spoofing using deep learning and rPPG detection,' IEEE International Joint Conference on Biometrics (IJCB), 2018.

[11] Simonyan, K., & Zisserman, A. 'Very deep convolutional networks for large-scale image recognition,' International Conference on Learning Representations (ICLR), 2015.

[12] Deng, J. et al. 'ArcFace: Additive angular margin for deep face recognition,' IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2019.

[13] Li, H., et al. 'Anti-spoofing with depth information for face recognition,' IEEE International Conference on Image Processing (ICIP), 2017.

[14] Feng, L. et al. 'A deep learning framework for detecting face spoofing in biometric authentication systems,' Journal of Computational Analysis and Applications (JoCAAA), 33(08), 2024, 4641–4651.

[15] Vaswani, A. et al. 'Attention Is All You Need,' Advances in Neural Information Processing Systems (NeurIPS), 2017.

[16] Zhang, Z., & Zhang, T. 'Real-time face detection and tracking using a cascade convolutional neural network,' IEEE Transactions on Cybernetics, 2022.

[17] Ching, S. Y. et al. 'Face liveness detection for biometric anti-spoofing applications using color texture and distortion analysis features,' Journal of Computer Science and Technology, 2024.

[18] Ghasemi, N. et al. 'Privacy-preserving face recognition using homomorphic encryption and deep learning,' International Conference on Information Security and Cryptology, 2023.

[19] Alippi, C. et al. 'Facial-based intrusion detection system with deep learning in embedded devices,' IEEE Transactions on Industrial Informatics, 2024.