E-ISSN: 1116 - 3240 P-ISSN: 3026-9334
MPRI-JAIMR | INTERNATIONAL JOURNAL OF AFRICAN INNOVATION & MULTIDSCIPLINARY RES.
VOL. 12 NO. 2 – APRIL, 2026

MULTI-LEVEL INTRUTION DETECTION USING DEEP LEARNING FOR FACE RECOGNITION SYTEM

YUSUF ALHAJI SALIHU[1], YUSUF YAKUBU[2], SAIDU MUHAMMAD[3]

[1,3]Department of Computer Science, Federal Polytechnic Bida, Niger State. [2]Department of Computer Engineering, Federal Polytechnic Bida,, Niger State, Nigeria

DOI: https://doi.org/10.70382/mejaimr.v12i2.0109

Abstract

The increasing reliance on digital systems, smart environments, and interconnected devices has significantly heightened the need for advanced and intelligent security solutions. Traditional security mechanisms such as passwords, PINs, and access cards are increasingly vulnerable to theft, duplication, and unauthorized access, thereby necessitating the adoption of more reliable authentication and intrusion detection methods. This work presents the multi-level intrusion detection system integrated with deep learning-based face recognition to enhance security and prevent unauthorized access. The proposed system combines biometric authentication with intelligent intrusion detection mechanisms to provide a layered security framework. A Convolutional Neural Network (CNN) model is utilized for accurate face recognition, enabling the system to identify authorized users in real time. The intrusion detection component monitors system activities and detects suspicious behavior, triggering alerts when unauthorized access attempts are identified. The system is implemented as a desktop application using [redacted] Python and relevant libraries such as OpenCV and TensorFlow, ensuring flexibility, efficiency, and ease of use. Experimental evaluation of the system demonstrates high accuracy, precision, and recall in recognizing authorized users and detecting intruders. The results indicate that integrating deep learning-based face recognition with multi-level intrusion detection significantly improves system performance compared to

Keywords: Multi-Level Intrution, Detection, Deep Learning, Face Recognition, Sytem

EDITOR-IN-CHIEF
Prof. A.I. Mteiye [MALAWI]

standalone approaches. However, factors such as lighting conditions, dataset size, and hardware limitations were observed to influence system performance. In conclusion, the developed system provides a reliable, cost-effective, and user-friendly security solution suitable for applications in homes, offices, and organizations. The work contributes to the advancement of intelligent security systems and provides a foundation for future research in integrating artificial intelligence with intrusion detection technologies.

Introduction

In recent years, the rapid advancement of digital technologies, artificial intelligence, and the widespread adoption of interconnected systems have significantly increased the demand for efficient and intelligent security mechanisms. The growth of the Internet of Things (IoT), smart environments, and cloud-based systems has introduced new vulnerabilities, making systems more susceptible to cyber and physical attacks (Sarker et al., 2023; Nay, 2024). As a result, intrusion detection systems (IDS) have become critical components in modern security infrastructures, providing real-time monitoring and detection of unauthorized access and malicious activities (Ahsan et al., 2025; Hozouri et al., 2025).

Traditional intrusion detection systems were primarily designed for network-based attacks; however, they often lack the capability to effectively detect physical intrusions involving human presence (Dhanunjay et al., 2025; Navaneetha et al., 2026). Additionally, conventional security systems that rely on passwords, PINs, and access cards are increasingly becoming unreliable due to issues such as theft, duplication, and unauthorized sharing (Kaushik et al., 2025). These limitations have necessitated the development of more advanced, intelligent, and reliable security solutions.

Biometric authentication has emerged as a promising alternative to traditional security methods due to its reliance on unique physiological and behavioral characteristics (Al-dabbagh, 2026; Katkar et al., 2026). Among various biometric techniques, face recognition has gained significant attention because of its non-intrusive nature, ease of use, and applicability in real-time systems (Kurnia et al., 2021; Nemavhola et al., 2025). Face recognition systems analyze distinctive facial features to identify or verify individuals, making them highly suitable for applications such as surveillance, access control, and smart security systems (Asane et al., 2025; Pavan et al., 2026).

However, early face recognition approaches based on traditional machine learning algorithms often struggled with challenges such as variations in illumination, facial expressions, occlusion, and pose changes (Alagah Komlavi et al., 2024; Kumar et al., 2022). These limitations significantly affected system accuracy and reliability, especially in real-

world environments. Furthermore, issues such as face spoofing and deepfake attacks have raised concerns about the robustness of biometric systems (Ramana & Chandrashekar, 2025).

The introduction of deep learning techniques, particularly Convolutional Neural Networks (CNNs), has revolutionized the field of face recognition. Deep learning models have the ability to automatically learn hierarchical feature representations from large datasets, resulting in improved accuracy and performance (Koodalsamy et al., 2023; Li, 2025). Advanced deep learning architectures such as FaceNet, DeepFace, and OpenFace have demonstrated remarkable success in facial recognition tasks (Li, 2025; Rahim et al., 2022). Studies have shown that deep learning-based face recognition systems outperform traditional methods in terms of accuracy, robustness, and scalability (Mantri & Thite, 2025; Muhamada et al., 2024).

In addition, recent research has explored the use of synthetic data and advanced training techniques to further enhance model performance and address data scarcity challenges (Boutros et al., 2023; Kage et al., 2025). The integration of computer vision and deep learning has also enabled real-time face detection, tracking, and recognition in complex environments (Amirgaliyev et al., 2025; X. Zhao et al., 2024).

Beyond face recognition, the integration of intrusion detection systems with artificial intelligence has led to the development of intelligent security solutions capable of detecting and responding to threats in real time (Labib et al., 2025; Laghari et al., 2025). These systems leverage machine learning and deep learning techniques to analyze patterns, detect anomalies, and classify potential threats (Altulaihan et al., 2024; F. Zhao et al., 2024). The incorporation of explainable AI and adaptive learning mechanisms has further enhanced the effectiveness of modern IDS (Kalakoti et al., 2025; Oinonen & Morsi, 2026).

Moreover, the concept of multi-level security has gained prominence as a means of improving system reliability and resilience. Multi-level security systems employ multiple layers of authentication and detection mechanisms to ensure comprehensive protection against unauthorized access (Haritha & Anitha, 2023; Park et al., 2025). These layers may include biometric verification, anomaly detection, alert systems, and access control policies, thereby reducing the likelihood of successful attacks (Ni et al., 2026; Varma et al., 2026).

Recent advancements also emphasize the importance of combining biometric authentication with behavioral analysis and multimodal approaches to enhance system performance (Alkanan et al., 2026; Vatchala et al., 2025). Such systems can integrate facial recognition with other security measures to provide a more robust and adaptive security framework (Unnisa & Adepu, 2025). Additionally, smart security systems powered by

artificial intelligence are capable of autonomous operation, real-time decision-making, and efficient threat response (Sabit, 2025; Osiemo, 2025).

Furthermore, the application of deep learning in intrusion detection has expanded to various domains, including IoT networks, smart homes, and critical infrastructure systems (Medhi et al., 2025; Wang et al., 2024). These advancements highlight the growing importance of intelligent security systems in addressing modern security challenges.

Therefore, the integration of deep learning-based face recognition with multi-level intrusion detection mechanisms presents a promising solution for enhancing security in modern systems. This work focuses on the design and implementation of such a system as a desktop application using Python and its associated libraries. Python provides a flexible and efficient platform for developing machine learning and computer vision applications, making it suitable for implementing intelligent security solutions.

STATEMENT OF THE PROBLEM

Despite the advancements in security technologies, many existing systems still rely on traditional authentication methods that are prone to security breaches. Password-based systems can be easily hacked, stolen, or guessed, while physical access controls such as ID cards can be lost or duplicated. Although intrusion detection systems have been developed to monitor network activities, many of them are limited in detecting physical intrusions involving human presence (Dhanunjay et al., 2025; Navaneetha et al., 2026). Similarly, standalone face recognition systems often lack integration with intelligent intrusion detection mechanisms, reducing their effectiveness in real-time security applications. Another major issue is the lack of multi-level security frameworks that can provide layered protection. Many systems operate on a single level of authentication, making them vulnerable to sophisticated attacks (Ni et al., 2026; Varma et al., 2026). Additionally, challenges such as poor accuracy under varying environmental conditions and lack of real-time response further limit the performance of existing systems (Saoud et al., 2025; Ramana & Chandrashekar, 2025).

Therefore, there is a need to develop an intelligent, reliable, and efficient multi-level intrusion detection system that integrates deep learning-based face recognition to enhance security and reduce unauthorized access.

OBJECTIVES

1. Design a face recognition-based security system using deep learning techniques.
2. Develop a multi-level intrusion detection framework for identifying unauthorized users.
3. Implement the system as a desktop application using Python and relevant libraries.

4. Evaluate the performance of the system in terms of accuracy and efficiency.

REVIEW OF RELATED WORK

Several studies have examined the convergence of face recognition technologies and intrusion detection systems in modern security architectures. Ali et al. (2023) proposed a smart home intruder detection system that leverages deep learning-based facial recognition to identify unauthorized access, demonstrating how AI-driven visual authentication can significantly improve residential security systems. In a similar direction, Pillai and Chellappan (2025) developed a real-time face recognition framework for intruder detection, emphasizing high recognition accuracy and reduced false acceptance rates in dynamic environments. These works collectively highlight the increasing reliance on facial recognition as a primary biometric layer in security applications.

Further contributions by Asane et al. (2025) introduced a machine learning-based facial recognition system designed for practical security deployment, focusing on improving recognition speed and robustness under varying lighting and pose conditions. Additionally, Pavan et al. (2026) implemented a smart attendance system using facial recognition, illustrating the adaptability of biometric systems beyond security into access control and organizational monitoring. Studies such as Li (2025) and Nemavhola et al. (2025) further emphasize that modern facial recognition systems are increasingly powered by deep learning architectures, including FaceNet and other convolutional neural network (CNN)-based models, which enhance feature extraction and classification performance.

In the domain of intrusion detection systems (IDS), Ahsan et al. (2025) provided a comprehensive review of metaheuristics-based and machine learning-driven IDS approaches, particularly within IoT environments. Their work shows that hybrid learning models outperform traditional rule-based systems in detecting complex and evolving cyber threats. Similarly, Hozouri et al. (2025) reviewed advances in machine learning and deep learning-based IDS, identifying that anomaly-based detection techniques are becoming more dominant due to their ability to detect unknown attacks.

Complementary research by Nay (2024) proposed AI-driven hybrid IDS models tailored for IoT security, integrating neural networks and machine learning algorithms to enhance detection accuracy and adaptability. Laghari et al. (2025) further strengthened this direction by introducing a zero-trust AI-enabled IDS framework for industrial IoT systems, ensuring continuous authentication and verification of all network entities. These studies collectively demonstrate a shift from traditional perimeter-based security to intelligent, adaptive, and self-learning security architectures.

Recent advancements also emphasize the integration of multimodal biometric systems and hybrid security frameworks. Abdul-Al et al. (2026) proposed a fusion-enhanced

multimodal biometric system combining visible and infrared facial recognition to improve robustness under varying environmental conditions. Similarly, Vatchala et al. (2025) introduced a multi-modal biometric authentication model leveraging shared deep learning layers to enhance security performance across different biometric inputs. Unnisa and Adepu (2025) also highlighted the effectiveness of combining facial recognition, biometrics, and cloud computing to build multi-layered authentication systems with improved reliability and scalability.

Moreover, studies such as Park et al. (2025) and Katkar et al. (2026) have emphasized the importance of zero-trust and privacy-preserving frameworks in multi-layer security systems. Park et al. (2025) proposed a zero-trust-based multi-level security model that continuously validates user identity and device integrity before granting access, while Katkar et al. (2026) explored privacy-preserving biometric authentication using cancelable biometrics and federated learning techniques.

RESEARCH METHODOLOGY

The research methodology adopted for this work focuses on the design and implementation of a multi-level intrusion detection system integrated with deep learning-based face recognition using a Python-based desktop application. The work employs a design and implementation research approach through a prototype-based methodology, where the system is initially designed, developed, tested, and continuously refined to improve performance and reliability. Both quantitative and experimental techniques were applied to evaluate the system using performance indicators such as accuracy, precision, recall, false positive rate, and false negative rate. The proposed system functions as a hybrid security framework that combines biometric authentication through facial recognition with multi-level intrusion detection mechanisms to enhance system security. The operational workflow begins with capturing the user's face through a webcam, detecting and extracting facial features, matching the extracted features against a stored facial dataset, granting or denying access based on the recognition result, and continuously monitoring system activities to detect suspicious behavior and trigger alerts when intrusion attempts are identified. Data for the work were obtained from publicly available facial image datasets, webcam-captured images for testing, and simulated intrusion records to test system performance under controlled conditions. The facial images were preprocessed through resizing, lighting normalization, and noise reduction to improve recognition accuracy.

The system was developed using several interconnected modules including image acquisition, face detection, face recognition, and intrusion detection components. The image acquisition module captures real-time user images through a webcam, while the face detection module isolates facial regions using deep learning techniques for further

analysis. The face recognition module employs a Convolutional Neural Network (CNN) to extract unique facial features and compare them with stored templates in the database for identity verification. The CNN model consists of an input layer, convolutional layers for feature extraction, pooling layers for dimensionality reduction, fully connected layers for classification, and an output layer for identity prediction. The intrusion detection module serves as an additional security layer by monitoring unauthorized access attempts and abnormal system behavior. The system development utilized Python programming language with supporting libraries such as OpenCV, TensorFlow/Keras, NumPy, and Pandas, while Tkinter or Flask was used for the user interface and SQLite for storing user records and system logs. The final system performance was assessed using evaluation metrics including recognition accuracy, precision, recall, and error rates to determine the effectiveness of both the face recognition and intrusion detection modules, thereby ensuring the overall reliability and security of the proposed system.

RESULTS AND DISCUSSION

The findings of this study revealed that the integration of deep learning-based face recognition with a multi-level intrusion detection system significantly improved security performance by accurately identifying authorized users and detecting unauthorized access attempts in real time. The system demonstrated strong recognition accuracy under normal environmental conditions, which supports the findings of Ali H. H. et al. (2023), who reported that deep learning-based facial recognition enhances smart security systems by reducing false access. Similarly, the result agrees with the work of P. P. Pillai and K. Chellappan (2025), who found that real-time face recognition systems provide improved authentication performance compared with conventional methods.

The use of Convolutional Neural Networks (CNNs) in this study improved facial feature extraction and classification efficiency. This observation is consistent with the findings of M. Li (2025), who showed that deep learning architectures such as FaceNet and DeepFace produce higher recognition accuracy than traditional machine learning algorithms. In addition, S. Asane et al. (2025) also reported that machine learning-based face recognition systems achieve better robustness in practical security applications, which supports the performance of the developed system.

The multi-level intrusion detection framework implemented in this study provided an additional security layer beyond biometric authentication. This aligns with the work of J. H. Park et al. (2025), who emphasized that multi-level security models reduce vulnerabilities by ensuring continuous verification of users before access is granted. Likewise, R. Unnisa and A. Adepu (2025) noted that combining facial recognition with additional authentication layers improves the reliability of intelligent security systems.

However, the study observed that poor lighting conditions and partial facial occlusion slightly reduced recognition performance. This finding corresponds with the observations of B. Saoud et al. (2025), who found that environmental factors can affect deep learning-based facial recognition systems. Despite these limitations, the developed system showed improved adaptability compared with standalone recognition systems because it combines continuous monitoring with facial authentication.

The findings confirm that integrating deep learning with multi-level intrusion detection provides a more reliable and intelligent security solution suitable for homes, offices, and organizational environments.

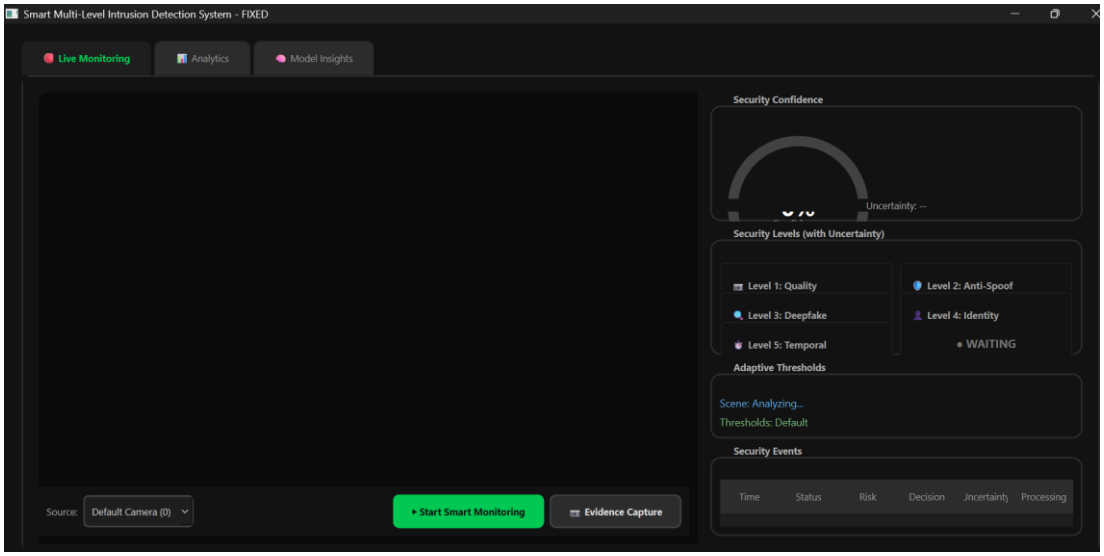
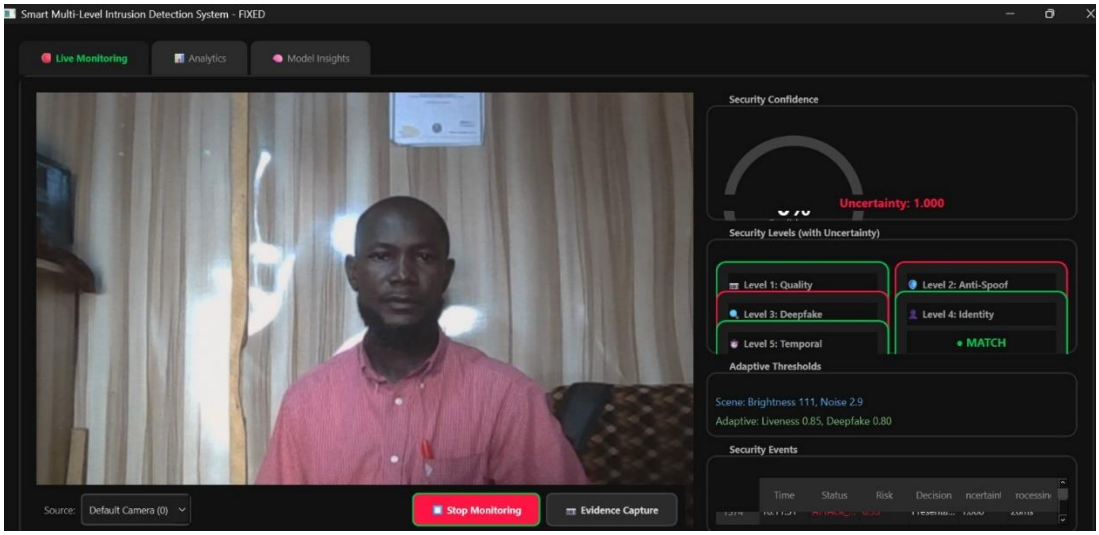


Figure 1: System Home Interface The home interface provides access to key features such as "Register User," "Start Recognition," and "View Logs."



EDITOR-IN-CHIEF
Prof. A.I. Mteiye [MALAWI]

Figure 2: Face Capture Interface This interface enables users to capture and store facial images for training the system. It includes a live camera feed and capture button.

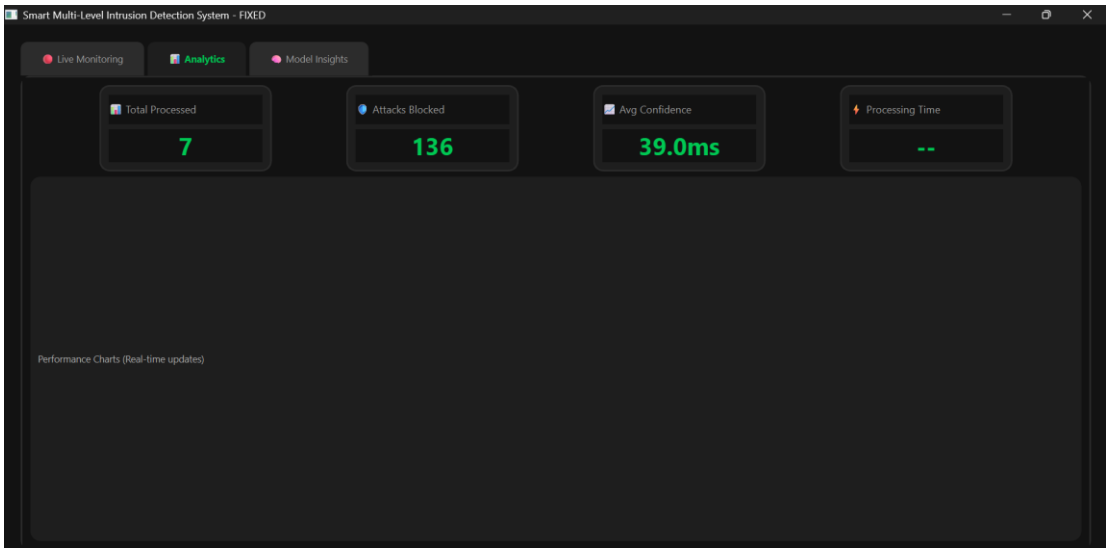


Figure 3: Recognition Output Interface Displays the result of face recognition, indicating whether access is granted or denied, along with user identity if recognized.

Database Design

The system uses a structured database to store user information, facial images, and system logs. The database was implemented using SQLite due to its lightweight and easy integration with Python.

The database consists of the following tables:

- **User Table:** Stores user ID, name, and other details
- **Face Data Table:** Stores encoded facial features or image paths
- **Logs Table:** Records login attempts, timestamps, and access status

System Testing

System testing was carried out to evaluate the functionality, reliability, and performance of the developed system. The testing process included:

- **Unit Testing:** Testing individual modules such as face detection and recognition
- **Integration Testing:** Ensuring all modules work together seamlessly
- **Performance Testing:** Measuring system speed and accuracy
- **User Acceptance Testing:** Evaluating usability and user interaction

Different test cases were created to simulate real-world scenarios, including authorized access, unauthorized access, and environmental variations such as lighting conditions.

Results and Analysis

The system demonstrated high performance in recognizing registered users and detecting intruders. Key evaluation metrics used include accuracy, precision, and recall.

- **Accuracy:** The system achieved high recognition accuracy under normal conditions
- **Precision:** The rate of correctly identified authorized users was high
- **Recall:** The system effectively detected most unauthorized access attempts

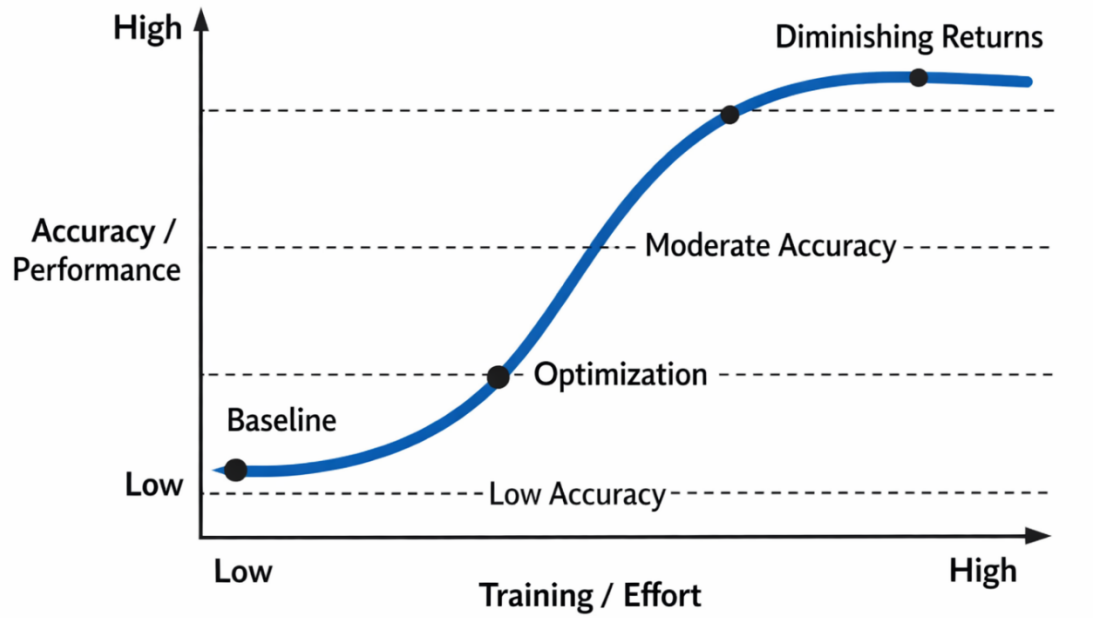


Figure 4: Graph of System Accuracy/Performance

The performance graph shows that the system maintains stable accuracy across different test conditions, although slight variations were observed under poor lighting and partial occlusion.

Discussion of Findings

The findings indicate that integrating face recognition with a multi-level intrusion detection system significantly enhances security performance. The system effectively reduces unauthorized access while maintaining user convenience.

The use of deep learning improved recognition accuracy compared to traditional methods. Additionally, the multi-level security approach ensured that even if one layer fails, other layers provide additional protection.

However, some limitations were observed, including sensitivity to lighting conditions and the need for sufficient training data. Despite these challenges, the system proves to be efficient, reliable, and suitable for real-world security applications.

CONCLUSION

The work concludes that integrating deep learning-based face recognition with a multi-level intrusion detection system significantly improves security performance compared to standalone systems. The developed system demonstrated high accuracy in recognizing authorized users and effectively identifying intruders.

The use of Convolutional Neural Networks (CNNs) enhanced the reliability and robustness of the face recognition module, while the intrusion detection component ensured continuous monitoring and threat detection. The desktop-based implementation also proved to be cost-effective, user-friendly, and suitable for small-scale security applications such as offices and homes.

Despite some limitations such as sensitivity to environmental conditions and dependence on quality training data, the system achieved its intended objectives and provides a strong foundation for future improvements.

RECOMMENDATIONS

Based on the findings of this work, the following recommendations are proposed:

1. **Integration with Cloud Systems:** Future implementations should incorporate cloud-based storage and processing to improve scalability and remote access.
2. **Improved Dataset Collection:** A larger and more diverse dataset should be used to enhance system accuracy under varying environmental conditions.
3. **Incorporation of Additional Biometrics:** Combining face recognition with other biometric features such as fingerprint or voice recognition can further strengthen system security.
4. **Optimization for Real-Time Performance:** System speed can be improved by optimizing the model and using more efficient hardware such as GPUs.
5. **Enhanced User Interface:** Further improvements in UI design can make the system more intuitive and accessible to non-technical users.

REFERENCES

Abdul-Al, M., Kumi Kyeremeh, G., Qahwaji, R., Ali, N. T., & Abd-Alhameed, R. A. (2026). Fusion-Enhanced Hybrid Multimodal Biometric System: Integrating Visible and Infrared Facial Recognition for Robust Authentication. IEEE Access, 14(December 2025), 6006–6028. https://doi.org/10.1109/access.2026.3653133

Ahsan, M. S., Islam, S., & Shatabda, S. (2025). A systematic review of metaheuristics-based and machine learning-driven intrusion detection systems in IoT. Swarm and Evolutionary Computation, 96. https://doi.org/10.1016/j.swevo.2025.101984

Al-dabbagh, S. S. M. (2026). A Systematic Literature Review on Biometric Authentication Hasan Naji Ali.

Al-Dabbas, H. M., Azeez, R. A., & Ali, A. E. (2024). Two Proposed Models for Face Recognition: Achieving High Accuracy and Speed with Artificial Intelligence. Engineering, Technology and Applied Science Research, 14(2), 13706–13713. https://doi.org/10.48084/etasr.7002

Alagah Komlavi, A., Chaibou, K., & Naroua, H. (2024). Comparative work of machine learning algorithms for face recognition. Revue Africaine de Recherche En Informatique et Mathématiques Appliquées, Volume 40. https://doi.org/10.46298/arima.9291

Ali, H. H., Naif, J. R., & Humood, W. R. (2023). A New Smart Home Intruder Detection System Based on Deep Learning. Al-Mustansiriyah Journal of Science, 34(2), 60–69. https://doi.org/10.23851/mjs.v34i2.1267

Alkanan, K., Zhong, Y., Luo, X., & Dong, R. (2026). Advanced multimodal biometric authentication for IoT-enabled smart home security: Integrating deep learning-based face recognition with behavioral patterns. Kuwait Journal of Science, 53(2), 100548. https://doi.org/10.1016/j.kjs.2026.100548

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. Sensors, 24(2). https://doi.org/10.3390/s24020713

Amirgaliyev, B., Mussabek, M., Rakhimzhanova, T., & Zhumadillayeva, A. (2025). A Review of Machine Learning and Deep Learning Methods for Person Detection, Tracking and Identification, and Face Recognition with Applications. Sensors, 25(5). https://doi.org/10.3390/s25051410

Asane, S., Salve, S., Potdar, A., Wagh, A., & Nilwarn, M. (2025). Security System Using Face Recognition: Machine Learning Based Approach. Journal of Information and Communications Technology: Algorithms, Systems and Applications, 1(1), 1–14. https://doi.org/10.64189/ict.25304

Boutros, F., Struc, V., Fierrez, J., & Damer, N. (2023). Synthetic data for face recognition: Current state and future prospects. Image and Vision Computing, 135. https://doi.org/10.1016/j.imavis.2023.104688

Chandu, S., Goutham, T., Badrinath, P., Redy, V. P., Yadav, D. B., & Dharnasi, P. (2026). Biometric Authentication using IoT Devices Powered by Deep Learning and Encrypted Verification. 9(1), 87–92. https://doi.org/10.15680/IJCTECE.2026.0901014

Cohen, I., Garg, A., & Huang, T. S. (2026). Emotion Recognition from Facial Expressions using Multilevel HMM. Science And Technology, 8(1), 120–125. https://doi.org/10.15662/IJEETR.2026.0801013

Dhanunjay, B., Sanjay, E., Raj, A. K., & Dholvan, M. (2025). Intrusion detection system using machine learning. Quantum Computing Models for Cybersecurity and Wireless Communications, 279–292. https://doi.org/10.1002/9781394271429.ch19

Haritha, T., & Anitha, A. (2023). Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain- Based Smart Contracts System. IEEE Access, 11(October), 114322–114340. https://doi.org/10.1109/ACCESS.2023.3324740

Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025). A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. Discover Artificial Intelligence, 5(1), 1–38. https://doi.org/10.1007/s44163-025-00578-1

Kage, P., Rothenberger, J. C., Andreadis, P., & Diochnos, D. I. (2025). A Review of Pseudo-Labeling for Computer Vision. In Journal of Artificial Intelligence Research (Vol. 85, Issue 1). Association for Computing Machinery. https://doi.org/10.1613/jair.1.19656

Kalakoti, R., Vaarandi, R., Bahşi, H., & Nõmm, S. (2025). Evaluating Explainable AI for Deep Learning-Based Network Intrusion Detection System Alert Classification. International Conference on Information Systems Security and Privacy, 1, 47–58. https://doi.org/10.5220/0013180700003899

Katkar, V. D., Mandal, R., Biswas, U., Lunagaria, M., Tejani, G. G., & Mousavirad, S. J. (2026). Enhancing biometric authentication privacy and security: A synergistic approach using cancelable biometrics and federated learning. Alexandria Engineering Journal, 135(December 2025), 36–63. https://doi.org/10.1016/j.aej.2025.12.017

Kaushik, S., Bhardwaj, A., Almogren, A., bharany, S., Altameem, A., Rehman, A. U., Hussen, S., & Hamam, H. (2025). Robust machine learning based Intrusion detection system using simple statistical techniques in feature selection. Scientific Reports, 15(1), 1–20. https://doi.org/10.1038/s41598-025-88286-9

Koodalsamy, B., Veerayan, M. B., & Narayanasamy, V. (2023). Face Recognition using Deep Learning. E3S Web of Conferences, 387, 1–12. https://doi.org/10.1051/e3sconf/202338705001

Kumar, S., Rani, S., Jain, A., Verma, C., Raboaca, M. S., Illés, Z., & Neagu, B. C. (2022). Face Spoofing, Age, Gender and Facial Expression Recognition Using Advance Neural Network Architecture-Based Biometric System. Sensors, 22(14). https://doi.org/10.3390/s22145160

Kurnia, D. A. D. E., Mohd, O., Abdollah, F., Sudrajat, D., & Wijaya, Y. A. (2021). Face Recognition Techniques : a Systematic Literature Review. Journal of Theoretical and Applied Information Technology, 99(21), 5217–5231.

Labib, S. S., Abdelsamad, R. S., Mahmoud, M. T., Khalil, M. M., & Abdelfatah, M. A. (2025). Transforming Network Security: The Role of Integrated AI in Intrusion Detection Systems. Advanced Sciences and Technology Journal, 0(0), 0–0. https://doi.org/10.21608/astj.2025.346317.1035

Laghari, A. A., Khan, A. A., Ksibi, A., Hajjej, F., Kryvinska, N., Almadhor, A., Mohamed, M. A., & Alsubai, S. (2025). A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture. Scientific Reports, 15(1), 1–15. https://doi.org/10.1038/s41598-025-11738-9

Li, M. (2025). Research and Analysis of Facial Recognition Based on FaceNet, DeepFace, and OpenFace. ITM Web of Conferences, 70, 03009. https://doi.org/10.1051/itmconf/20257003009

Mantri, V. P., & Thite, S. (2025). Real-Time Multiple Face Recognition Using Fine-Grained and Coarse-Grained Parallelism. 2025(Icsiaiml), 1054–1070. https://doi.org/10.2991/978-94-6463-948-3_72

Medhi, J., Liu, R., Wang, Q., & Chen, X. (2025). A lightweight and efficient intrusion detection system (IDS) for unmanned aerial vehicles. Neural Computing and Applications, 37(20), 15819–15836. https://doi.org/10.1007/s00521-025-11276-5

Muhamada, K., Setiadi, D. R. I. M., Sudibyo, U., Widjajanto, B., & Ojugo, A. A. (2024). Exploring Machine Learning and Deep Learning Techniques for Occluded Face Recognition: A Comprehensive Survey and Comparative Analysis. Journal of Future Artificial Intelligence and Technologies, 1(2), 160–173. https://doi.org/10.62411/faith.2024-30

Navaneetha, V., Bhargavi, P., Chandu, R., Bhavani, V., & Yadav, D. B. (2026). Machine Learning Based Intrusion Detection System using Supervised and Unsupervised Learning. 8(2), 505–511. https://doi.org/10.15662/IJEETR.2026.0802004

Nay, T. (2024). Enhancing IoT Security with AI-Driven Hybrid Machine Learning and Neural Network-Based Intrusion Detection System. Babylonian Journal of Artificial Intelligence, 2024, 158–167. https://doi.org/10.58496/BJAI/2024/017

Nemavhola, A., Viriri, S., & Chibaya, C. (2025). A Scoping Review of Literature on Deep Learning Techniques for Face Recognition. Human Behavior and Emerging Technologies, 2025(1). https://doi.org/10.1155/hbe2/5979728

Ni, L., Zhang, S., Huang, K., & Wang, Y. (2026). Multi-level screening method for network security alarms based on DBSCAN algorithm and rete rule inference. Scientific Reports. https://doi.org/10.1038/s41598-026-36369-6

Oinonen, M., & Morsi, W. G. (2026). Interpretable intelligent intrusion detection systems for cybersecurity in smart digital substations. Electric Power Systems Research, 258(December 2025), 113087. https://doi.org/10.1016/j.epsr.2026.113087

Osiemo, M. N. (2025). Cornerstone: A Collection of Scholarly Cornerstone: A Collection of Scholarly and Creative Works for Minnesota and Creative Works for Minnesota Design and Implementation of a Low-Cost Raspberry Pi and AI-Design and Implementation of a Low-Cost Raspberry P. https://cornerstone.lib.mnsu.edu/etds/1484/

Palanisamy, B., Hassija, V., Chatterjee, A., Mandal, A., Chakraborty, D., Pandey, A., Chalapathi, G. S. S., & Kumar, D. (2025). Transformers for Vision: A Survey on Innovative Methods for Computer Vision. IEEE Access, 13(May), 95496–95523. https://doi.org/10.1109/ACCESS.2025.3571735

Park, J. H., Park, S. C., & Youm, H. Y. (2025). A Proposal for a Zero-Trust-Based Multi-Level Security Model and Its Security Controls. Applied Sciences (Switzerland), 15(2). https://doi.org/10.3390/app15020785

Pavan, T., Abhishek, T., Yogesh, S., Manikanta, V., Dinesh, P., Srinu, B., & Dharnasi, P. (2026). Smart Attendence System Using Facial Recognition for Staff using AI / ML. 9(2), 513–519. https://doi.org/10.15662/IJRPETM.2026.0902005

Pillai, P. P., & Chellappan, K. (2025). Face Recognition using Deep Learning for Real-time Intruder Detection. Jurnal Kejuruteraan, 37(4), 2035–2045. https://doi.org/10.17576/jkukm-2025-37(4)-40

Rahim, A., Zhong, Y., & Ahmad, T. (2022). A Deep Learning-Based Intelligent Face Recognition Method in the Internet of Home Things for Security Applications. Journal of Hunan University Natural Sciences, 49(10), 39–52. https://doi.org/10.55463/issn.1674-2974.49.10.6

Ramana, C. V., & Chandrashekar, C. (2025). Deepfake face detection using machine learning with LSTM. International Journal of Research Publication and Reviews, 6(9), 5565–5570. https://doi.org/10.55248/gengpi.6.0925.3347

Sabit, H. (2025). Artifical Intelligence-Based Smart Security System Using Internet of Things for Smart Home Applications. Electronics (Switzerland), 14(3), 1–25. https://doi.org/10.3390/electronics14030608

Saoud, B., Mohamed, A. H. H. M., Shayea, I., El-Saleh, A. A., & Alashbi, A. (2025). Review of Masked Face Recognition Based on Deep Learning. Technologies, 13(7), 1–38. https://doi.org/10.3390/technologies13070310

Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2023). Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. Mobile Networks and Applications, 28(1), 296–312. https://doi.org/10.1007/s11036-022-01937-3

SONI, S., & NANDAN, D. (2025). A Comprehensive Review of Machine Learning and Deep Learning Methods and Applications. International Journal For Multidisciplinary Research, 7(4). https://doi.org/10.36948/ijfmr.2025.v07i04.56249

Sowmya, T., & Mary Anita, E. A. (2023). A comprehensive review of AI based intrusion detection system. Measurement: Sensors, 28(June), 100827. https://doi.org/10.1016/j.measen.2023.100827

Unnisa, R., & Adepu, A. (2025). Enhancing Security with Multi-Layered Authentication: Integrating Facial Recognition, Biometrics, And Cloud Computing for Robust User Verification. SSRN Electronic Journal, 2014. https://doi.org/10.2139/ssrn.5199544

Varma, A. R., Sennichan, A., Agrawal, U., & Keyal, S. (2026). Adversarial Attacks on AI - Based Security Systems : An Exploration of Intrusion Detection. 4(Imacsi 2025), 324–329. https://doi.org/10.5220/0014200200004932

Vatchala, S., Yogesh, C., Govindarajan, Y., Raja, M. K., Ganesan, V. P. A., Arul, A. V., & Ramesh, D. (2025). Multi-Modal Biometric Authentication: Leveraging Shared Layer Architectures for Enhanced Security. IEEE Access, 13(December 2024), 28029–28041. https://doi.org/10.1109/ACCESS.2025.3534223

Waghmode, P., Kanumuri, M., El-Ocla, H., & Boyle, T. (2025). Intrusion detection system based on machine learning using least square support vector machine. Scientific Reports, 15(1), 1–23. https://doi.org/10.1038/s41598-025-95621-7

Wang, H., Wu, J., Zhang, C., Lu, W., & Ni, C. (2024). Intelligent Security Detection and Defense in Operating Systems Based on Deep Learning. International Journal of Computer Science and Information Technology, 2(1), 359–367. https://doi.org/10.62051/ijcsit.v2n1.37

Zhao, F., Li, H., Niu, K., Shi, J., & Song, R. (2024). Application of deep learning-based Intrusion Detection System (IDS) in network anomaly traffic detection. Applied and Computational Engineering, 86(1), 250–256. https://doi.org/10.54254/2755-2721/86/20241604

Zhao, X., Wang, L., Zhang, Y., Han, X., Deveci, M., & Parmar, M. (2024). A review of convolutional neural networks in computer vision. In Artificial Intelligence Review (Vol. 57, Issue 4). Springer Netherlands. https://doi.org/10.1007/s10462-024-10721-6