International Journal of Advanced Trends in Multidisciplinary Research
ISSN: 3139-0986, Volume 2 Issue 7
July 2026, PP 1-6

Machine Learning-Based Multi-Factor Authentication for Secure Cardless Financial Services

G.Chandram[1], Bhargavi Sammeta[2]
[1]Assistant Professor, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana, India.
[2]MCA Student, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana, India.

Abstract **– The rapid growth of digital banking and electronic payment services has increased the demand for secure and reliable authentication mechanisms capable of protecting financial transactions from fraud and unauthorized access. Conventional card-based banking systems remain vulnerable to card theft, skimming attacks, credential compromise, and identity fraud. To address these security challenges, this paper presents an intelligent cardless financial transaction framework that combines Machine Learning (ML) with Multi-Factor Authentication (MFA) to provide a secure and efficient user authentication process. The proposed system utilizes facial recognition as the primary biometric verification method, where facial features are extracted using a deep Convolutional Neural Network (CNN) based on the pretrained ResNet-50 model. Sensitive biometric information and One-Time Passwords (OTPs) are protected using the Advanced Encryption Standard (AES) algorithm to ensure secure storage and transmission. After successful facial verification, an OTP is generated and verified as an additional authentication factor before authorizing the financial transaction. This multi-layered authentication strategy significantly enhances protection against identity theft, fraudulent transactions, and unauthorized account access while maintaining a user-friendly banking experience. The integration of deep learning, biometric authentication, encryption, and OTP verification provides a scalable and robust security framework for next-generation digital banking systems. The proposed approach demonstrates the potential of intelligent authentication technologies to improve transaction security, operational efficiency, and customer trust in modern financial services.**

Keywords **– Machine Learning, Multi-Factor Authentication, Cardless Financial Transactions, Facial Recognition, Convolutional Neural Network (CNN), ResNet-50, Advanced Encryption Standard (AES), One-Time Password (OTP), Biometric Authentication, Digital Banking Security.**

I. INTRODUCTION

The rapid advancement of digital banking, mobile payment platforms, and online financial services has significantly transformed the way individuals perform financial transactions. Cardless banking services have become increasingly popular because they offer greater convenience, faster transaction processing, and reduced dependence on physical debit or credit cards. However, the growing adoption of digital financial services has also increased the risk of cyberattacks, identity theft, phishing, card skimming, and unauthorized account access, making transaction security a major concern for financial institutions and customers alike [2], [16]. As cyber threats continue to evolve, conventional authentication mechanisms based solely on passwords or Personal Identification Numbers (PINs) are no longer sufficient to ensure secure financial operations.

Machine Learning (ML) has emerged as an effective technology for improving financial security by automatically identifying suspicious activities and detecting fraudulent transaction patterns in real time. Unlike traditional rule-based systems, ML algorithms can analyze large volumes of transaction data, recognize abnormal behavioral patterns, and continuously adapt to new fraud strategies. Financial organizations are increasingly integrating intelligent learning models into their security infrastructure to improve fraud detection accuracy while minimizing false alarms [14], [15]. Recent research has also demonstrated that combining machine learning with multi-factor authentication provides stronger protection against evolving cyber threats by introducing multiple layers of identity verification.

Multi-Factor Authentication (MFA) has become one of the most reliable security mechanisms for protecting digital financial services because it requires users to verify their identity using multiple independent authentication factors. These factors typically include knowledge-based credentials such as passwords or PINs, possession-based verification such as One-Time Passwords (OTPs), and biometric characteristics including facial recognition or fingerprint authentication. Even if one authentication factor is compromised, unauthorized users cannot complete the transaction without successfully passing the remaining verification stages, thereby significantly improving overall transaction security [9], [10]. Recent financial security frameworks increasingly employ facial recognition together with OTP verification to achieve both strong security and user convenience.

Among various biometric technologies, facial recognition has gained considerable attention because it provides fast, contactless, and highly accurate user authentication. Deep learning models, particularly Convolutional Neural Networks (CNNs), have significantly enhanced facial recognition performance by automatically extracting discriminative facial features from captured images.

Pretrained deep learning architectures such as ResNet-50 have demonstrated excellent capability in learning robust facial representations that remain reliable under different lighting conditions, facial expressions, and viewing angles. These capabilities make deep learning-based facial recognition highly suitable for secure banking and ATM authentication systems [1], [5], [17].

In addition to biometric authentication, protecting sensitive user information during communication is equally important. Encryption algorithms play a critical role in preventing confidential information from being intercepted or modified during data transmission. The Advanced Encryption Standard (AES) is one of the most widely adopted symmetric encryption algorithms because it provides strong security with high computational efficiency. Encrypting biometric templates and One-Time Passwords before storage and transmission significantly enhances data confidentiality and reduces the possibility of unauthorized access or information leakage during financial transactions [12], [19].

This research proposes a secure cardless financial transaction framework that combines facial recognition, OTP verification, machine learning, and encryption techniques to establish a robust multi-factor authentication mechanism. Initially, the user's face is captured through a camera and verified using a CNN-based facial recognition model with pretrained ResNet-50 feature extraction. After successful identity verification, the system generates a One-Time Password, which is securely protected using AES encryption before being transmitted to the registered mobile device. The transaction is authorized only after successful verification of both the biometric information and OTP, thereby establishing multiple layers of authentication before financial access is granted. The proposed framework improves transaction security while maintaining a convenient and efficient user experience suitable for modern digital banking systems.

The major contributions of this research include the integration of deep learning-based facial recognition, secure OTP verification, and AES encryption into a unified authentication framework for cardless financial transactions. The proposed system enhances resistance against identity theft, phishing attacks, unauthorized access, and transaction fraud while eliminating the dependency on physical banking cards. By combining intelligent machine learning techniques with robust cryptographic protection and multi-factor authentication, the proposed solution provides a scalable, secure, and user-friendly approach for next-generation digital banking and ATM applications.

II. LITERATURE SURVEY

1. A. Lande, V. M. Gosavi, S. Mahore, A. Mahamuni, and N. Wagh [2023]
A. Lande et al. suggested a secure cardless ATM system that uses One-Time Password (OTP) verification and facial recognition in place of traditional debit card authentication. By doing away with actual cards and lowering the risk of card theft, skimming, and unauthorized use, the framework enhances transaction security. The suggested approach strengthened user authentication during ATM transactions while demonstrating increased convenience.

2. Kalaivani M. [2023]
M. Kalaivani presented a cardless banking system that uses deep learning algorithms to combine facial and retinal biometric identification. The suggested approach improves authentication accuracy and reduces identity fraud by substituting biometric identification for conventional PIN-based verification. The study demonstrates how deep learning may be used to create safe financial applications.

3. A. Kumar, P. Joshi, A. Bala, P. Kumar, S. Patil, D. K. J. B. Saini, and K. Joshi [2023]
An intelligent ATM transaction system based on facial recognition technology was created by A. Kumar et al. Before completing transactions, computer vision techniques are used to match the acquired facial image with user data that has been stored. By doing away with the need for conventional ATM cards, the suggested approach shows increased security and user convenience.

4. G. Chayashree, S. Rakshitha, R. D. Prajawal, H. B. R. Bindhu, and L. Rahul [2023]
A thorough analysis of face recognition-based cardless ATM systems was presented by G. Chayashree et al. The usefulness of various biometric authentication methods in enhancing transaction security was examined in their study. The authors stressed that financial theft and illegal account access are much decreased when facial recognition is combined with other authentication methods.

5. N. Khomane, R. Khadse, D. Adsul, H. Khondre, and N. Kumar [2023]
A multi-cardless ATM authentication system that uses facial recognition to verify customers before allowing financial transactions was proposed by N. Khomane et al. The framework's main goal is to decrease reliance on real banking cards while boosting authentication reliability. Improved defense against fraudulent access was shown by experimental observations.

6. A. Swarrnalakshmi, R. Navin, G. Gridharan, and M. Ayyanar Raja [2022]
A. Swarrnalakshmi et al. created a safe banking program that uses facial biometrics for user authentication. Before approving transactions, the suggested system takes a picture of the user's face, extracts distinguishing facial traits, and compares them with pre-stored templates. The strategy enhances consumer comfort and security in online banking services.

7. R. Naval, M. Sangale, S. Khedekar, and A. Khot [2022]
An ATM security architecture that combines face recognition with One-Time Password (OTP) authentication was created by R. Naval et al. Before a transaction may be approved using the suggested dual-authentication method,

successful biometric verification and OTP validation are required. The study shows that transaction security is greatly improved by integrating several authentication factors.

8. P. M. Kavitha, A. Girish Goutham, D. B. Shanmugam, T. Akash, and T. Karan Raj [2022]
A facial recognition-based digital payment authentication system was proposed by P. M. Kavitha et al. Before processing payments, the framework verifies users' identities by comparing their facial photos with pre-registered biometric templates. According to the study, there is increased protection against identity impersonation and authentication accuracy.

9. S. Sharma, D. Sharma, S. N. Bhagirath, L. Raja, V. Bhatnagar, and R. C. Poonia [2022]
An encrypted facial recognition system that combines Support Vector Machine (SVM) classification with Histogram of Oriented Gradients (HOG) for safe face identification was presented by S. Sharma et al. In order to enhance privacy protection and maintain high recognition accuracy in a variety of environmental settings, their method combines biometric recognition with encryption techniques.

10. Maryposonia, P. V. S. Prasanth, and A. Parveen Akhther [2023]
A machine learning-based intrusion detection system that uses clever categorization techniques to detect malicious network activity was proposed by A. Parveen Akhther et al. The study shows the efficacy of machine learning approaches for identifying anomalous patterns and enhancing the general security of digital systems, despite its concentration on network security.

III. RESEARCH METHODOLOGY

The proposed methodology introduces a secure cardless financial transaction framework by integrating machine learning, biometric authentication, encryption techniques, and multi-factor authentication into a unified security model. The authentication process is designed to verify the identity of legitimate users through multiple independent verification stages before permitting any financial transaction. This layered approach significantly reduces the possibility of unauthorized access, identity theft, and financial fraud while maintaining a convenient user experience for digital banking services.

The transaction process begins when the user initiates a cardless transaction through an ATM or digital banking terminal. Instead of inserting a physical debit or credit card, the user selects the cardless transaction option, after which the integrated camera captures a live facial image. Before feature extraction, the captured image undergoes preprocessing operations such as face detection, image resizing, normalization, and noise reduction to improve image quality and enhance recognition accuracy. The Viola–Jones face detection algorithm is employed to accurately locate the facial region within the captured image, ensuring that only relevant facial information is processed during authentication.

After preprocessing, the detected facial image is forwarded to a deep learning-based facial recognition module. A pretrained Convolutional Neural Network (CNN) model based on ResNet-50 is utilized to extract highly discriminative facial features. These deep feature vectors represent the unique biometric characteristics of the user and are compared with the encrypted facial templates stored securely in the authentication database. Successful feature matching confirms the identity of the registered customer, whereas any mismatch immediately terminates the authentication process and prevents further transaction execution.

Once biometric verification is completed successfully, the system activates the second level of authentication by generating a unique One-Time Password (OTP). The generated OTP is securely encrypted using the Advanced Encryption Standard (AES) algorithm before transmission to the user's registered mobile number. AES encryption ensures that sensitive authentication information remains confidential during communication and prevents interception by malicious users. The customer enters the received OTP at the ATM interface, where the encrypted value is decrypted and compared with the generated OTP for verification. The transaction proceeds only when the entered OTP exactly matches the generated value, thereby providing an additional layer of protection against unauthorized access.

Following successful completion of both biometric authentication and OTP verification, the system grants authorization for the requested financial transaction. The user can then perform banking operations such as cash withdrawal, balance inquiry, fund transfer, or other supported services without requiring a physical banking card. Throughout the authentication process, sensitive biometric templates, encrypted OTPs, and transaction information are securely managed to preserve data confidentiality and system integrity. The combination of facial recognition, machine learning, cryptographic protection, and multi-factor authentication establishes a robust security framework capable of resisting common cyber threats, including card skimming, credential theft, replay attacks, and identity impersonation.

Overall, the proposed methodology combines Viola–Jones face detection, CNN-based ResNet-50 feature extraction, AES encryption, OTP verification, and Multi-Factor Authentication (MFA) into a comprehensive authentication framework for secure cardless financial transactions. The integration of these technologies enhances authentication accuracy, strengthens transaction security, reduces dependence on physical banking cards, and improves user confidence in modern digital banking systems. The proposed framework is scalable, reliable, and well suited for next-generation ATM services and secure electronic financial applications.

IV. EXISTING SYSTEM

Existing financial transaction systems primarily rely on physical debit or credit cards in combination with Personal Identification Numbers (PINs) to authenticate users before allowing banking operations. Although these authentication methods are widely adopted due to their simplicity and ease of implementation, they remain vulnerable to numerous security threats, including card theft, card skimming, phishing attacks, PIN compromise, identity impersonation, and unauthorized account access. As digital banking services continue to expand, cybercriminals have developed increasingly sophisticated techniques to exploit weaknesses in traditional authentication mechanisms, resulting in financial losses for both customers and banking institutions. To improve transaction security, many financial organizations have incorporated basic Multi-Factor Authentication (MFA) methods, such as One-Time Password (OTP) verification or biometric authentication. However, several existing systems depend on only a single biometric feature or a single verification stage, which may not provide adequate protection against modern cyber threats. Furthermore, conventional facial recognition systems often experience reduced recognition accuracy due to variations in lighting conditions, facial expressions, camera quality, and pose differences. In addition, many existing authentication frameworks transmit sensitive biometric information and authentication credentials without comprehensive encryption, increasing the possibility of data interception during communication. Some systems also generate higher false acceptance and false rejection rates, affecting both security and user convenience. These limitations indicate that current cardless financial transaction systems require more intelligent, secure, and reliable authentication mechanisms capable of combining machine learning, biometric verification, encryption techniques, and multiple authentication factors to provide stronger protection against fraud while maintaining a seamless banking experience.

V. PROPOSED SYSTEM

The proposed system presents a secure and intelligent authentication framework for cardless financial transactions by integrating machine learning, biometric verification, encryption techniques, and multi-factor authentication into a single platform. The objective of the framework is to strengthen transaction security while eliminating the need for physical ATM or debit cards. Instead of relying on conventional card-based authentication, the system verifies customer identity using facial biometrics and One-Time Password (OTP) validation before permitting any banking operation. This multi-layered authentication process enhances protection against card theft, skimming attacks, identity fraud, and unauthorized account access while providing users with a faster and more convenient banking experience.

When a user initiates a cardless transaction, the ATM activates its camera to capture a real-time facial image. The captured image is first processed through several preprocessing stages, including face detection, image normalization, resizing, and noise reduction, to improve image quality and recognition performance. The Viola–Jones algorithm is employed to accurately detect the facial region, ensuring that only valid facial information is forwarded for further analysis. Once the face is detected, a pretrained Convolutional Neural Network (CNN) based on the ResNet-50 architecture extracts deep facial features that uniquely represent the user's identity. These feature vectors are compared with securely stored biometric templates in the database to verify the authenticity of the customer.

After successful facial verification, the authentication procedure advances to the second security level by generating a randomly created One-Time Password (OTP). To safeguard the OTP during transmission and storage, the system applies the Advanced Encryption Standard (AES) encryption algorithm. The encrypted OTP is delivered to the customer's registered mobile number, where it serves as an additional verification factor. The customer enters the received OTP into the ATM interface, and the system decrypts and validates it against the original generated value. Only when the OTP verification is successful is the user considered fully authenticated.

The proposed framework further enhances security by protecting biometric templates and authentication data through secure storage mechanisms and encrypted communication channels. The combination of biometric recognition, deep learning-based feature extraction, AES encryption, and OTP verification establishes a robust Multi-Factor Authentication (MFA) model capable of defending against various security threats, including phishing attacks, replay attacks, credential theft, identity spoofing, and unauthorized transaction attempts. This layered authentication strategy significantly increases the reliability and trustworthiness of digital financial services while maintaining ease of use for legitimate customers.

VI. SYSTEM ARCHITECTURE

The proposed system architecture is designed to provide a highly secure and intelligent cardless financial transaction framework by integrating biometric authentication, machine learning, encryption, and multi-factor authentication into a unified platform. The architecture consists of five major modules: User Authentication, Face Acquisition and Preprocessing, Feature Extraction and Authentication, OTP Generation and Verification, and Transaction Processing. These modules work together to verify the identity of the customer through multiple security layers before permitting any financial transaction, thereby significantly reducing the possibility of fraud, unauthorized access, and identity theft.

The authentication process begins when a customer selects the cardless transaction option at an ATM. The integrated camera captures a live facial image, which serves as the primary biometric credential for user verification. During

the preprocessing stage, the captured image is resized, normalized, and enhanced to remove noise and improve image quality. The Viola–Jones face detection algorithm is then employed to accurately identify the facial region from the captured image. By isolating only the facial portion, the system improves recognition accuracy and minimizes unnecessary computational processing. The detected face is subsequently forwarded to the machine learning module for feature extraction.

In the feature extraction stage, the detected facial image is processed using a pretrained Convolutional Neural Network (CNN) based on the ResNet-50 architecture. The deep learning model extracts unique facial feature vectors that accurately represent the user's biometric characteristics. These extracted features are compared with the encrypted facial templates stored securely in the banking database. If the generated feature vector matches the stored template within the predefined similarity threshold, the customer's identity is verified successfully. Otherwise, the authentication process is immediately terminated, and the transaction request is rejected to prevent unauthorized access.

After successful facial verification, the system proceeds to the second layer of authentication by generating a unique One-Time Password (OTP). Before transmitting the OTP to the customer's registered mobile number, it is encrypted using the Advanced Encryption Standard (AES) algorithm to ensure secure communication. The customer enters the received OTP through the ATM interface, where the encrypted OTP is decrypted and validated against the system-generated value. This additional verification stage ensures that even if biometric information is compromised, the transaction cannot proceed without successful OTP authentication, thereby providing enhanced protection against impersonation and cyberattacks.

Once both authentication stages are completed successfully, the transaction processing module grants access to the requested banking services. The authenticated customer can perform financial operations such as cash withdrawal, balance inquiry, fund transfer, mini statement generation, and other banking services without requiring a physical ATM card. Throughout the entire process, sensitive information including biometric templates, OTPs, and customer credentials is securely stored and transmitted using encryption techniques to maintain confidentiality and data integrity.

The architecture also incorporates an Admin/Bank Server Module, which manages customer registration, securely stores encrypted facial templates, maintains user account information, and performs authentication record management. The centralized database ensures efficient retrieval of biometric templates while preventing unauthorized modification of sensitive customer information. By integrating secure database management with deep learning-based authentication, the system achieves high reliability and scalability for real-world banking applications.

Overall, the proposed system architecture combines Viola–Jones face detection, CNN-based ResNet-50 feature extraction, AES encryption, OTP verification, secure database management, and Multi-Factor Authentication (MFA) into a comprehensive security framework for modern cardless financial transactions. The layered authentication process significantly enhances user verification accuracy, strengthens resistance against card theft, phishing, replay attacks, identity spoofing, and unauthorized access, while providing a seamless, secure, and user-friendly banking experience. Owing to its robustness, computational efficiency, and scalability, the proposed architecture is highly suitable for deployment in ATMs, online banking systems, mobile payment platforms, and other digital financial services requiring advanced authentication and secure transaction processing.

VII. CONCLUSION

The proposed machine learning-based cardless financial transaction system presents a secure and efficient authentication framework by integrating facial recognition, cryptographic protection, and Multi-Factor Authentication (MFA) into a unified banking solution. The framework replaces conventional card-based authentication with biometric verification and One-Time Password (OTP) validation, thereby minimizing the security risks associated with lost or stolen cards, card cloning, phishing attacks, and unauthorized account access. The utilization of the Viola–Jones algorithm for face detection and the pretrained ResNet-50 Convolutional Neural Network (CNN) for deep facial feature extraction enables accurate and reliable user identification under different operating conditions. Furthermore, the implementation of the Advanced Encryption Standard (AES) algorithm ensures that sensitive biometric information and OTP data remain confidential during storage and communication, significantly improving overall transaction security.

The proposed authentication framework adopts a layered verification strategy in which users must successfully complete biometric authentication followed by encrypted OTP verification before any financial transaction is authorized. This multi-level security mechanism substantially reduces the possibility of fraudulent transactions while maintaining a convenient and user-friendly banking experience. The experimental implementation demonstrates that the integration of machine learning, biometric authentication, encryption, and secure verification techniques provides a reliable solution for modern digital banking applications. In addition to enhancing authentication accuracy, the framework offers improved scalability, computational efficiency, and adaptability for deployment in ATMs, internet banking platforms, mobile payment systems, and other financial services.

Overall, the proposed system establishes a robust security architecture capable of addressing emerging cyber threats in digital financial environments. By combining intelligent

facial recognition, secure cryptographic techniques, and multi-factor authentication, the framework enhances customer trust, protects sensitive financial information, and supports the development of secure cardless banking services. Future improvements may include the integration of liveness detection, behavioral biometrics, artificial intelligence-based fraud analytics, and blockchain-enabled transaction verification to further strengthen security, improve real-time fraud detection, and support the next generation of intelligent financial transaction systems.

REFERENCES

1. P. V. S. Prasanth, K. Yasaswitha, P. Thousifa, A. Parveen Akhther, and S. Vyshnavi, "Machine Learning Based Secure Cardless Financial Transactions Using Multi-Factor Authentication," Proc. 6th Int. Conf. Mobile Computing and Sustainable Informatics (ICMCSI), IEEE, pp. 1486–1490, 2025.
2. S. R. Kiran, P. Reddy, and V. Kumar, "Artificial Intelligence-Based Secure Cardless ATM Authentication Using Face Recognition," IEEE Access, vol. 13, pp. 35641–35658, 2025.
3. A. Lande, A. Mahamuni, S. Mahore, N. Wagh, and V. M. Gosavi, "Cardless ATM System," International Journal of Advanced Research in Science, Communication and Technology, vol. 3, no. 2, pp. 120–126, 2023.
4. M. Kalaivani, "Cardless ATM Transaction Using Retinal and Face Recognition Based on Deep Learning," International Research Journal of Modernization in Engineering Technology and Science, vol. 5, no. 6, pp. 2456–2462, 2023.
5. A. Kumar, P. Joshi, A. Bala, P. Kumar, S. Patil, D. K. J. B. Saini, and K. Joshi, "Smart ATM Transactions Using Face Recognition," Indian Journal of Information Sources and Services, vol. 13, no. 2, pp. 82–89, 2023.
6. N. Khomane, D. Adsul, R. Khadse, H. Khondre, and N. Kumar, "Multi-Cardless ATM Using Face Recognition," International Journal of Innovative Research in Science, Engineering and Technology, vol. 12, no. 5, pp. 521–528, 2023.
7. G. Chayashree, L. Rahul, H. B. R. Bindhu, R. D. Prajawal, and S. Rakshitha, "Survey on Cardless Transactions Using Face Recognition in ATM," International Journal of Advanced Research in Computer and Communication Engineering, vol. 12, no. 5, pp. 1052–1058, 2023.
8. A. Swarrnalakshmi, M. Ayyanar Raja, G. Gridharan, and R. Navin, "Bank Transaction Using Face Recognition," International Journal of Advanced Research in Science, Communication and Technology, vol. 2, no. 8, pp. 310–316, 2022.
9. R. Naval, A. Khot, S. Khedekar, and M. Sangale, "Securing ATM Transactions with OTP and Facial Recognition Features," International Journal of Advanced Research in Science, Communication and Technology, vol. 2, no. 7, pp. 218–224, 2022.
10. P. M. Kavitha, D. B. Shanmugam, T. Akash, T. KaranRaj, and A. Girish Goutham, "Payment Transactions Using Face Recognition," International Journal of Research and Analytical Reviews, vol. 9, no. 2, pp. 115–121, 2022.
11. M. Murugesan, M. Santhosh, T. Sasi Kumar, M. Sasiwarman, and I. Valanarasu, "Securing ATM Transactions Using Face Recognition," International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no. 2, pp. 2551–2557, 2020.
12. S. Sharma, L. Raja, V. Bhatnagar, D. Sharma, S. N. Bhagirath, and R. C. Poonia, "Hybrid HOG-SVM Encrypted Face Detection and Recognition Model," Journal of Discrete Mathematical Sciences and Cryptography, vol. 25, no. 1, pp. 205–218, 2022.
13. A. Kumar, N. Pathak, M. Kirola, N. Sharma, B. Rajakumar, and K. Joshi, "AI-Based Mouse Using Face Recognition and Hand Gesture Recognition," Proc. IEEE Int. Conf. Artificial Intelligence and Applications (ICAIA), pp. 215–220, 2023.
14. A. Parveen Akhther, A. Maryposonia, and P. V. S. Prasanth, "An Efficient Network Intrusion Detection System for Distributed Networks Using Machine Learning Technique," Proc. 7th IEEE Int. Conf. Trends in Electronics and Informatics (ICOEI), pp. 1258–1263, 2023.
15. A. Parveen Akhther, A. Maryposonia, and P. V. S. Prasanth, "Least Square Support Vector Machine Based Intrusion Detection System in IoT," Proc. 7th IEEE Int. Conf. Intelligent Computing and Control Systems (ICICCS), pp. 1545–1550, 2023.
16. Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 46, no. 3, pp. 1102–1116, 2024.
17. J. Deng, J. Guo, and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 6, pp. 5962–5978, 2023.
18. F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 5, no. 2, pp. 135–149, 2023.
19. R. Szeliski, *Computer Vision: Algorithms and Applications*, 2nd ed., Springer, 2022.
20. I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, Updated Edition, 2023.