Contextualized Facial Recognition and Anomaly Detection in High-Risk ATM Environments

[1] Mr . K. PremKumar, Assistant Professor
Computer Science and Engineering, St.Joseph College of Engineering, Chennai-602117, Tamil Nadu.

[2] Syed Uzair Ahmed.Q, UG Student
Computer Science and Engineering,St.Joseph College of Engineering,Chennai-602117,Tamil Nadu.

[3] Abishek.S, UG Student
Computer Science and Engineering, St.Joseph College of Engineering, Chennai-602117, Tamil Nadu.

[4] Arutchelvan.L, UG Student
Computer Science and Engineering, St.Joseph College of Engineering, Chennai-602117, Tamil Nadu

Abstract– Contextualized facial recognition and anomaly detection framework is implemented to enhance security in ATM transactions.By Using deep learning-based facial recognition, real-time behavioral analysis, and machine learning anomaly detection techniques, the system ensures user verification and threat identification. The proposed framework improves security by leveraging AI-driven monitoring and real-time alert mechanisms. Experimental evaluations demonstrate a high accuracy rate in detecting fraudulent activities, making ATMs safer and more secure.

I. INTRODUCTION

Automated Teller Machines, popularly referred to as ATMs, are one of the most useful advancements in the banking sector. ATMs allow banking customers to avail quick self-serviced transactions, such as cash withdrawal, deposit, and fund transfers. ATMs enable individuals to make banking transactions without the help of an actual teller. Also, customers can avail banking services without having to visit a bank branch. Most ATM transactions can be availed with the use of a debit or credit card. There are some transactions that need no debit or credit card.

In 1960, an American named Luther George Simjian invented the Bank graph, a machine that allowed customers to deposit cash and checks into it. The first ATM was set up in June 1967 on a street in Enfield, London at a branch of Barclays bank. A British inventor named John Shepherd-Barron is credited with its invention. The machine allowed customers to withdraw a maximum of GBP10 at a time.

The proposed framework continuously monitors ATM transactions, detects unauthorized users, and identifies unusual behavioral patterns that may indicate fraudulent activities. It leverages AI-driven monitoring, real-time alerts, and environmental context awareness to improve security while minimizing false positives.

II. BACKGROUND AND MOTIVATION

A. Overview

ATMs, being self-service financial access points, are prime targets for cybercriminals and fraudsters. Traditional security mechanisms rely on PIN-based authentication and card-based transactions, which can be easily compromised through techniques like shoulder surfing, card skimming, and phishing. The need for a more robust security framework has led to the adoption of biometric authentication methods.

Facial recognition has emerged as one of the most promising biometric solutions due to its non-intrusive nature and high accuracy. However, existing facial recognition systems lack contextual awareness, meaning they fail to analyze user behavior, transaction patterns, and environmental factors in real-time. This paper proposes an AI-driven security framework that not only authenticates users via facial recognition but also leverages machine learning-based anomaly detection to analyze transaction behaviors and detect security threats proactively

B. Motivation

The primary motivation behind this research is to develop an advanced security framework that enhances ATM security while maintaining user convenience. Several factors drive the need for such a system which includes

Escalating Financial Fraud: Banks worldwide face billions of dollars in losses annually due to ATM fraud. Current security measures have proven insufficient in mitigating these threats.

Limitations of PIN-Based Authentication: PINs are vulnerable to theft, social engineering, and brute-force attacks, making them an unreliable security measure.

Growing Adoption of Biometric Technologies: With the increasing acceptance of facial recognition in consumer electronics and public security systems, integrating biometric authentication into ATMs is a logical next step.

Advancements in Artificial Intelligence: AI-driven facial recognition and anomaly detection have significantly improved, making real-time fraud detection and prevention more feasible.

Regulatory and Compliance Requirements: Financial institutions are under increasing pressure to implement stringent security measures to comply with data protection and anti-fraud regulations.

User Convenience and Accessibility: A biometric authentication system enhances user experience by eliminating the need for PIN entry, reducing transaction time, and improving accessibility for users who may have difficulty remembering PINs.

By leveraging AI-powered contextual facial recognition and anomaly detection, our system enhances security, reduces fraud, and fosters a safer banking experience. Unlike traditional security measures, which reactively address fraud incidents, this approach proactively detects suspicious behavior, enabling banks to take preventive action in real time.

III. APPLICATIONS OF CONTEXTUALIZED FACIAL RECOGNITION AND ANOMALY DETECTION

The proposed system offers multiple applications that significantly enhance ATM security:

Biometric Authentication: Users are authenticated through facial recognition, eliminating the risks associated with PIN-based systems.

Fraud Prevention: The system detects and prevents fraudulent activities such as identity theft and card skimming by analyzing user behavior and ATM usage patterns.

Real-Time Surveillance: Integrated AI-driven surveillance continuously monitors ATM surroundings, flagging suspicious activities such as multiple failed authentication attempts or loitering.

Behavioral Anomaly Detection: Machine learning models analyze transaction history and user behavior to detect anomalies such as unusual withdrawal amounts or erratic transaction timings.

Emergency Alert System: In the event of unauthorized access or suspicious behavior, the system triggers real-time alerts to bank security teams and law enforcement.

IV. ROLE AND POTENTIAL OF SENSOR BASED HEART DISEASE DEDUCTION

i. Roles:

User Authentication: The primary role of the system is to authenticate users securely by verifying their facial features against stored biometric data. This reduces reliance on PIN-based authentication and mitigates risks such as stolen or duplicated cards.

Threat Detection: The system continuously scans for potential threats, including unauthorized users attempting access, multiple failed transactions, and suspicious ATM activity.

Enhanced Security Monitoring**:** The ATM environment is monitored in real time, identifying anomalies such as loitering individuals, multiple users at the same ATM, or extended transaction durations.

Automated Decision-Making: Using AI and machine learning, the system autonomously determines whether an ATM transaction is legitimate or if security intervention is required.

Fraud Prevention and Risk Mitigation: By detecting patterns associated with fraudulent activities such as withdrawing excessive amounts in quick succession, the system prevents unauthorized access and financial losses.

ii. **Potential:**

Reduction in Financial Fraud: The integration of facial recognition and anomaly detection significantly decreases fraud by eliminating loopholes exploited by criminals, such as stolen PINs or duplicated cards.

Enhanced Customer Trust**:** Secure ATM environments foster trust among users, encouraging them to continue using banking services with confidence.

Real-Time Security Alerts**:** The system immediately notifies banking authorities and law enforcement in the event of suspicious activities, enabling quick response times to mitigate threats.

Scalability and Adaptability: The framework is designed for easy scalability, allowing financial institutions to implement it across multiple ATM locations with minimal modifications.

Integration with Emerging Technologies: The system can be further enhanced with blockchain technology for secure transaction logging, edge computing for real-time data processing, and multi-modal biometric authentication for increased reliability.

Legal and Regulatory Compliance: Compliance with data protection regulations ensures user privacy and security, making the system a viable option for financial institutions globally.

V.CONCLUSION

Contextualized Facial Recognition and Anomaly Detection System designed to enhance security in high-risk ATM environments. By combining deep learning-based facial recognition with machine learning anomaly detection, the system effectively identifies unauthorized users and prevents fraudulent transactions. Our experimental evaluations demonstrate high accuracy in user authentication and anomaly detection, ensuring a secure and reliable banking experience.

Future work will focus on expanding the system’s capabilities by incorporating adaptive AI models, multi-modal biometric authentication, and integration with real-time financial fraud prevention networks. The deployment of this technology in real-world ATM infrastructures will revolutionize security measures, setting a new standard for fraud prevention in the financial sector.

VI.FUTURE RESEARCH DIRECTIONS FOR ENHANCED EDUCATION

Integration with Blockchain for Secure Transactions:

Blockchain technology can enhance ATM security by providing a decentralized and immutable ledger for transaction verification. Future research can focus on integrating blockchain to prevent unauthorized modifications, ensure transparency, and provide a tamper-proof transaction history.

Multi-Modal Biometric Authentication:

While facial recognition is a strong authentication method, integrating additional biometric modalities such as iris scanning, fingerprint recognition, and voice authentication can further enhance security. Future studies can explore the feasibility and effectiveness of multi-modal biometric authentication in ATMs.

Adaptive AI Models for Continuous Learning:

Current machine learning models require retraining to adapt to new fraud patterns. Future research should focus on **self-learning AI models** that continuously update themselves based on new threats, transaction behaviors, and fraud techniques, ensuring real-time adaptation to emerging security risks.

Edge Computing for Real-Time Processing:

To reduce latency in fraud detection and improve response times, edge computing can be integrated with the proposed system. Future work can focus on deploying AI-driven facial recognition and anomaly detection models directly on ATM hardware for real-time decision-making without relying on cloud-based processing.

Enhanced Behavioral Analysis with AI:

Future studies can develop more advanced behavioral analysis algorithms that consider gait recognition, emotional analysis, and micro-expressions to detect stress levels or coercion during ATM transactions, providing an additional security layer against forced withdrawals.

Privacy-Preserving Facial Recognition Techniques:

While facial recognition enhances security, privacy concerns remain a challenge. Future research should explore privacy-preserving techniques such as homomorphic encryption, differential privacy, and federated learning to ensure data security while maintaining high authentication accuracy.

Deployment in Real-World ATM Networks:

While the current system has been tested in a simulated ATM environment, future research should focus on deploying and testing the framework in real-world ATM networks. Studies should evaluate the system’s scalability, user acceptance, and performance in diverse banking infrastructures.

REFERENCES:

[1] A. J. Prakash, K. K. Patro, M. Hammad, R. Tadeusiewicz, and P. Pławiak, ‘‘BAED: A secured biometric authentication system using ECG signal based on deep learning techniques,’’ Biocybernetics Biomed. Eng., vol. 42, no. 4, pp. 1081–1093, Oct. 2022.
[2] S. H. Moi, P. Y. Yong, R. Hassan, H. Asmuni, R. Mohamad, F. C. Weng, and S. Kasim, ‘‘An improved approach of iris biometric authentication performance and security with cryptography and error correction codes,’’ JOIV Int. J. Informat. Visualizat., vol. 6, no. 2, p. 531, Aug. 2022.
[3] D. Jiang, G. Zhang, O. W. Samuel, F. Liu, and H. Xiao, ‘‘Dualfactor WBAN enhanced authentication system based on iris and ECG descriptors,’’IEEESensorsJ.,vol.22,no.19,pp. 19000–19009,Oct.2022.
[4] V. Esmaeili and M. M. Feghhi, ‘‘Real-time authentication for electronic serviceapplicantsusingamethodbasedontwo-stream3DdeepLearning,’’ Soft Comput. J. (SCJ), vol. 11, no. 2, pp. 38–49, Mar. 2023.
[5] D. K. Jain, S. Neelakandan, A. Vidyarthi, and D. Gupta, ‘‘Deep learningbased intelligent system for fingerprint identification using decision-based median filter,’’ Pattern Recognit. Lett., vol. 174, pp. 25–31, Oct. 2023.
[6] V. Esmaeili and S. O. Shahdi, ‘‘Automatic micro-expression apex spotting using cubic-LBP,’’ Multimedia Tools Appl., vol. 79, nos. 27–28, pp. 20221–20239, Apr. 2020.
[7] V. Esmaeili, M. M. Feghhi, and S. O. Shahdi, ‘‘Micro-expression recognition based on the multi-color ULBP and histogram of gradient direction from six intersection planes,’’ J. Iranian Assoc. Electr. Electron. Eng., vol. 19, no. 3, pp. 123–130, Jul. 2022.
[8] V. Esmaeili, M. M. Feghhi, and S. O. Shahdi, ‘‘Micro-expression recognition using histogram of image gradient orientation on diagonal planes,’’ in Proc. 5th Int. Conf. Pattern Recognit. Image Anal. (IPRIA), Apr. 2021, pp. 1–5.
[9] V. Esmaeili, M. M. Feghhi, and S. O. Shahdi, ‘‘Autonomous apex detection and Micro-expression recognition using proposed diagonal Planes,’’ Int. J. Nonlinear Anal. Appl., vol. 11, pp. 483–497, Aug. 2020.
[10] V. Esmaeili, M. Mohassel Feghhi, and S. O. Shahdi, ‘‘A comprehensive survey on facial micro-expression: Approaches and databases,’’ Multimedia Tools Appl., vol. 81, no. 28, pp. 40089–40134, May 2022.
[11] V.Esmaeili,M.M.Feghhi,andS.O.Shahdi,‘‘Automaticmicro-expression apex frame spotting using local binary pattern from six intersection planes,’’ 2021, arXiv:2104.02149.
[12] A. Krizhevsky, I. Sutskever, and G. E. Hinton, ‘‘ImageNet classification with deep convolutional neural networks,’’ in Proc. Adv. Neural Inf. Process. Syst., vol. 25, 2012, pp. 1–9.
[13] K. He, X. Zhang, S. Ren, and J. Sun, ‘‘Deep residual learning for image recognition,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), NV, NV, USA, Jun. 2016, pp. 770–778.

[14] K. Simonyan and A. Zisserman, ‘‘Very deep convolutional networks for large-scale image recognition,’’ 2014, arXiv:1409.1556.
[15] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, ‘‘Going deeper with convolutions,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Boston, MA, USA, Jun. 2015, pp. 1–9.
[16] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam, ‘‘MobileNets: Efficient convolutional neural networks for mobile vision applications,’’ 2017, arXiv:1704.04861.
[17] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, ‘‘Densely connected convolutional networks,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Honolulu, HI, USA, Jul. 2017, pp. 2261–2269. [18] J. Daugman, ‘‘How iris recognition works,’’ IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 21–30, Jan. 2004.
[19] L. Ma, Y. Wang, and T. Tan, ‘‘Iris recognition using circular symmetric filters,’’ inProc. ObjectRecognit. Supported UserInteract. Service Robots, vol. 2, 2002, pp. 414–417.
[20] S. Ajmi and P. Arun, ‘‘Performance analysis of iris recognition system using DWT, CT and HOG,’’ IOSR J. Electron. Commun. Eng. (IOSRJECE), vol. 11, no. 5, pp. 2278–2834, Oct. 2016.
[21] N. M. AL-Kardhi and A. M. Al-Juboori, ‘‘Iris recognition in cross-spectral based on histogram of oriented gradient and linear discriminant analysis,’’ J. Al-Qadisiyah Comput. Sci. Math., vol. 15, no. 3, pp. 83–97, Sep. 2023.
[22] N. Liu, M. Zhang, H. Li, Z. Sun, and T. Tan, ‘‘DeepIris: Learning pairwise filter bank for heterogeneous iris verification,’’ Pattern Recognit. Lett., vol. 82, pp. 154–161, Oct. 2016.
[23] A. Gangwar and A. Joshi, ‘‘DeepIrisNet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition,’’ in Proc. IEEE Int. Conf. Image Process. (ICIP), Phoenix, AZ, USA, Sep. 2016, pp. 2301–2305.
[24] Z. Zhao and A. Kumar, ‘‘Towards more accurate iris recognition using deeply learned spatially corresponding features,’’ in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Venice, Italy, Oct. 2017, pp. 3829–3838.
[25] K. Wang and A. Kumar, ‘‘Toward more accurate iris recognition using dilated residual features,’’ IEEE Trans. Inf. Forensics Security, vol. 14, no. 12, pp. 3233–3245, Dec. 2019.
[26] K. Nguyen, C. Fookes, A. Ross, and S. Sridharan, ‘‘Iris recognition with off-the-shelf CNN features: A deep learning perspective,’’ IEEE Access, vol. 6, pp. 18848–18855, 2018.
[27] T. Zhao, Y. Liu, G. Huo, and X. Zhu, ‘‘A deep learning iris recognition method based on capsule network architecture,’’ IEEE Access, vol. 7, pp. 49691–49701, 2019.
[28] J. E. Zambrano, D. P. Benalcazar, C. A. Perez, and K. W. Bowyer, ‘‘Iris recognition using low-level CNN layers without training and single matching,’’ IEEE Access, vol. 10, pp. 41276–41286, 2022.
[29] J. Sun, S. Zhao, S. Miao, X. Wang, and Y. Yu, ‘‘Openset Iris recognition based on deep learning,’’ IET Image Process., vol. 16, no. 9, pp. 2361–2372, Apr. 2022.

[30] H.-Y. Wu, M. Rubinstein, E. Shih, J. Guttag, F. Durand, and W. Freeman, ‘‘Eulerian video magnification for revealing subtle changes in the world,’’ ACM Trans. Graph., vol. 31, no. 4, pp. 1–8, Jul. 2012.

[31] A. Asthana, S. Zafeiriou, S. Cheng, and M. Pantic, ‘‘Robust discriminative response map fitting with constrained local models,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., Portland, OR, USA, Jun. 2013, pp. 3444–3451.

[32] Z. Zhang, T. Chen, H. Meng, G. Liu, and X. Fu, ‘‘SMEConvNet: A convolutional neural network for spotting spontaneous facial micro-expression from long videos,’’ IEEE Access, vol. 6, pp. 71143–71151, 2018.

[33] M. A. A. Kashani, M. M. Arani, and M. R. R. Fini, ‘‘Eye detection and tracking in images with using bag of pixels,’’ in Proc. IEEE 3rd Int. Conf. Commun. Softw. Netw., Xi’an, China, May 2011, pp. 64–68.

[34] X. Wang, L. Gao, J. Song, and H. Shen, ‘‘Beyond frame-level CNN: Saliency-aware 3-D CNN with LSTM for video action recognition,’’ IEEE Signal Process. Lett., vol. 24, no. 4, pp. 510–514, Apr. 2017.

[35] W.-J. Yan, Q. Wu, Y.-J. Liu, S.-J. Wang, and X. Fu, ‘‘CASME database: A dataset of spontaneous micro-expressions collected from neutralized faces,’’ in Proc. 10th IEEE Int. Conf. Workshops Autom. Face Gesture Recognit. (FG), Shanghai, China, Apr. 2013, pp. 1–7.

[36] W.-J. Yan, X. Li, S.-J. Wang, G. Zhao, Y.-J. Liu, Y.-H. Chen, and X. Fu, ‘‘CASME II: An improved spontaneous micro-expression database and the baseline evaluation,’’ PLoS ONE, vol. 9, no. 1, Jan. 2014, Art. no. e86041.

[37] P. J. Phillips, ‘‘Overview of the multiple biometrics grand challenge,’’ in Proc. 3rd ICB, Alghero, Italy, 2009, pp. 705–714.

[38] C. Nicholson. (2019). Evaluation Metrics for Machine LearningAccuracy, Precision, Recall, and F1 Defined. Accessed: Jul. 2022. [Online].
Available: http://pathmind.com/wiki/accuracyprecision-recall-f1

[39] Y. Lee, R. J. Micheals, J. J. Filliben, and P. J. Phillips, ‘‘VASIR: An opensource research platform for advanced iris recognition technologies,’’ J. Res. Nat. Inst. Standards Technol., vol. 118, p. 218, Apr. 2013.

[40] J. M. Colores-Vargas, M. Garca-Vzquez, A. Ramrez-Acosta, H. Prez-Meana, and M. Nakano-Miyatake, ‘‘Video images fusion to improve iris recognition accuracy in unconstrained environments,’’ in Proc. MCPR, 2013, pp. 114–125.