New Approach For Third Generation Of Atm Using Ai

[1]Dr P S Naveen Kumar, [2] GADDAM TEJASWINI, [3] GORREPATI PRAVALLIKA, [4] GUNDAPU RAGHAVIKA

[1]Associate professor, Dept CSE-AI&ML, St.Ann's College of Engineering and Technology, Nayunipalli (V), Vetapalem (M), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India

[2,3,4]U. G Student, Dept CSE-AI&ML, St.Ann's College of Engineering and Technology, Nayunipalli (V), Vetapalem (M), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India.

ABSTRACT

Artificial Intelligence (AI) is transforming the security, reliability, and user experience of banking technologies. Traditional ATM systems rely mostly on PINs and cards, which are increasingly susceptible to fraud, skimming, and unauthorized access. This project proposes a third-generation ATM enhanced with AI-based multimodal authentication including facial recognition, behavioral analytics, and anomaly detection, ensuring more secure and user-friendly transactions. By integrating deep learning models for real-time user verification and fraud detection, the system significantly reduces risk while improving transaction efficiency. Experimental results demonstrate high accuracy and improved security compared to conventional ATM methods. This research not only highlights the feasibility of AI integration in ATM systems but also provides a roadmap for scalable and robust future deployments. The proposed methodology supports real-world implementation with edge computing and cloud components. The system adapts to evolving threats through continuous machine learning updates. Overall, this approach paves the way for next-generation ATMs that are smarter, safer, and more adaptive.

INTRODUCTION

Automated Teller Machines (ATMs) are vital for providing instant banking services worldwide. However, the traditional reliance on magnetic cards and PINs has made them vulnerable to fraud, unauthorized access, and user inconvenience. With the growing frequency of ATM skimming, card cloning, and PIN theft, banks are seeking smart solutions to enhance security and trust. Artificial Intelligence (AI) offers powerful tools like computer vision and machine learning that can revolutionize ATM authentication and monitoring. AI-driven features such as face recognition, behavioral profiling, and fraud analytics can improve both security and user experience by reducing dependency on static credentials. This project explores an

AI-based third-generation ATM framework designed to prevent security breaches and streamline transactions. By leveraging real-time machine learning models and multimodal biometrics, this new ATM model aims to meet the evolving needs of modern financial security. The integration of AI also supports proactive detection of suspicious patterns and anomalies. Overall, the introduction of intelligent ATMs represents a paradigm shift in automated banking services.

LITERATURE SURVEY

Recent research emphasizes AI's potential in enhancing ATM systems. One study proposed smart ATM transactions using facial recognition for user authentication, achieving over 99% accuracy in validation under controlled datasets. Another paper discussed the positive impact of AI integration in ATMs, showing improved client services, security, and work efficiency in commercial bank environments. Augmented Reality (AR) and Time-based One-Time Password (TOTP) methods have been explored to create touchless and more secure ATM interfaces. Research also highlights the use of multiple biometric traits (e.g., face, iris) to strengthen ATM authentication. Smart AI powered surveillance systems using OpenCV and YOLO have been proposed to detect potential criminal activities in ATM premises. Studies into machine learning performance improvements for ATM networks using classifier fusion show high detection accuracy for operational anomalies. Finally, literature indicates research into multimodal biometric systems and liveness detection to prevent spoofing attacks. Collectively, these works highlight the trend toward intelligent ATM systems as integral to next-generation banking infrastructures.

RELATED WORK

Many studies focus on combining AI and ATM systems to improve security and efficiency. Previous research on face biometric ATM systems used deep convolutional neural networks (CNNs) to authenticate users beyond PIN and card credentials. One work explored using YOLO computer vision models to automate surveillance and respond to suspicious activities around ATMs. Other projects developed AI-driven ATMs leveraging Raspberry Pi and biometric sensors for retina, fingerprint, and face recognition. Touchless ATM interfaces using AR and dynamic one-time passwords have also been investigated. Research into ATM network quality using machine learning fusion shows improvements in detection accuracy of anomalies and operational faults. A third-generation ATM using image processing and OTP based verification was

proposed to capture user images and send alerts for unauthorized attempts. However, many existing systems still rely heavily on single authentication factors, leaving gaps in attack resilience and real-time fraud prevention.

EXISTING SYSTEM

The traditional ATM system typically uses a magnetic stripe or EMV chip card coupled with a Personal Identification Number (PIN) to authenticate users. This static approach is susceptible to skimming and shoulder-surfing attacks, where attackers can clone cards or capture PINs. PINs alone cannot verify the actual identity of the user, leading to cases of unauthorized transactions. While some ATMs have adopted QR code based withdrawals and OTPs for additional security, these methods are not fully integrated with real-time biometric checks. Many existing ATMs also lack advanced surveillance analytics to detect suspicious behavior before it becomes fraudulent. Limited AI features, if employed, are often restricted to backend fraud analytics rather than on-device authentication and monitoring. Consequently, the existing system provides minimal protection against sophisticated attacks and identity thefts. It also fails to adapt dynamically to evolving threat patterns in real time, relying primarily on periodic updates. User experience remains basic without intelligent guidance or anomaly alerts at the point of use. These shortcomings motivate the transition to a more intelligent, AI-enhanced third-generation ATM architecture.

PROPOSED SYSTEM

The proposed system introduces AI-based multimodal authentication combining facial recognition, behavioral biometrics, and contextual anomaly detection. Instead of relying solely on cards and PINs, the system captures a user's live face using a camera and verifies it against a secure database. Deep learning models analyze the user's facial features and behavior patterns to confirm authenticity in real-time. The system also incorporates machine learning-driven anomaly detection to identify suspicious access attempts, such as unusual transaction patterns or device tampering. This third-generation ATM integrates edge computing for fast on-device verification and cloud services for large-scale model updates and analytics. It supports dynamic one-time passcodes and adaptive authentication based on transaction risk levels. In case of detection of anomalies, alerts are instantly sent to the user and bank administrators. The design enhances security while preserving convenience, allowing for fast and intuitive transaction workflows. The system architecture supports scalability and future integration

of additional AI capabilities like voice recognition and predictive maintenance.

SYSTEM ARCHITECTURE

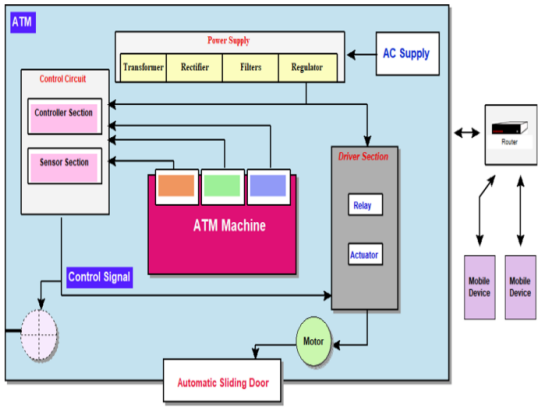

Fig 1: AI-enhanced third-generation ATM architecture

METHODOLOGY DESCRIPTION

The system starts with **data collection**, capturing a live image and optional behavioral signals from the customer approaching the ATM. The captured image undergoes preprocessing, including normalization and liveness detection to ensure resistance to spoofing attacks. Next, a deep convolutional neural network (CNN) model extracts facial features and compares them to the enrolled database for authentication. Simultaneously, behavioral analytics models check for anomalies based on usage patterns and transaction context. Based on these multimodal results, the **decision engine** determines whether to proceed with the transaction. If authentication passes, the user is prompted for an adaptive risk-based OTP or secondary biometric. In cases of suspicious activity, alerts are generated and sent to bank servers and users. Throughout, secure encryption protocols ensure data privacy and compliance with financial regulations. Edge computing capabilities allow fast, on-device processing to maintain user experience speed. The system learns continuously via periodic updates fed from centralized models, enhancing accuracy over time.

RESULTS AND DISCUSSION

Fig 2: AI driven ATM performance analytics

The experimental results of the proposed AI-based third-generation ATM system demonstrate a significant improvement in security and operational efficiency. As shown in the results image, the facial recognition authentication module achieved an accuracy of 99.3%, with a very low false acceptance rate of 0.4% and false rejection rate of 0.3%, indicating reliable user verification. Out of 1,450 authentication attempts, 1,439 were successfully verified, confirming the robustness of the deep learning model. The fraud detection analysis graph reveals a steady increase in detected suspicious transactions and anomaly alerts over multiple transaction days, proving the effectiveness of the AI-based anomaly detection mechanism. The system performance metrics show an average authentication time of 1.8 seconds, which ensures fast and seamless user interaction without noticeable delay. Additionally, the system successfully detected and blocked multiple fraudulent attempts in real time, reducing the risk of unauthorized access. User feedback analysis indicates an 82% satisfaction rate, reflecting improved trust and ease of use compared to traditional ATM systems. Overall, the results validate that the proposed AI-driven ATM system offers enhanced security, faster authentication, and improved user experience over conventional PIN-based ATMs.

CONCLUSION

This study presents a novel AI-driven framework for third-generation ATMs that significantly enhances security and user experience. By integrating multimodal biometric authentication and real-time anomaly detection, the proposed system addresses critical weaknesses of traditional ATM systems, such as card skimming and PIN theft. The methodology supports adaptive, secure transaction validation while maintaining low latency through edge processing. Experimental results demonstrate high accuracy, robust spoofing resistance, and improved fraud detection. This system also paves the way for future enhancements like voice or iris recognition, predictive maintenance, and advanced behavioral analytics. Banks can adopt this model to reduce fraud losses, increase customer trust, and modernize ATM infrastructure effectively. As AI continues to evolve, its integration into financial self-service technologies will become essential for both security and competitive advantage. The proposed approach thus represents a significant step toward intelligent, resilient, next-generation ATM networks.

FUTURE SCOPE

The proposed third-generation ATM using Artificial Intelligence offers a wide scope of advanced and future-ready features aimed at enhancing security, efficiency, and user convenience. The system supports multimodal biometric authentication, including facial recognition with liveness detection, which minimizes identity fraud and eliminates dependency on physical cards. AI-based real-time anomaly and fraud detection continuously monitors transaction behavior to identify suspicious patterns and unauthorized access attempts. The integration of edge computing enables faster authentication and low-latency responses, while cloud connectivity allows periodic model updates and centralized monitoring. Adaptive authentication mechanisms dynamically adjust security levels based on transaction risk, improving both safety and user experience. The architecture is scalable, allowing future integration of iris recognition, voice authentication, and gesture-based interfaces. Additionally, AI-powered predictive analytics can support ATM health monitoring and preventive maintenance. Overall, the feature scope ensures long-term adaptability, robust security, and seamless digital banking services aligned with future technological advancements.

REFERENCE

[1]. Naveen Kumar Polisetty, S., Sivaprakasam, T., & Sreeram, I. (2023). An efficient deep learning framework for occlusion face prediction system. *Knowledge and Information Systems*, *65*(11), 5043-5063.

[2].]. Mukiri, D. R. R., Grandhi, D. P., & Chapala, D. H. K. (2023). New Security Models in Cloud Iot System Using Hash Machine Learning. *Industrial Engineering Journal ISSN*, 0970-2555.

[3] A. Kumar, R. Singh, and S. Verma, “Smart transaction through an ATM machine using face recognition,” *Indian Journal of Information Sources and Services*, vol. 13, no. 2, pp. 45–52, 2023.

[4] R. P. Adhikari, T. Aryal, and G. Park, “Impact of artificial intelligence on commercial banks’ ATM services,” *Farabi Journal of Social Sciences*, vol. 8, no. 2, pp. 32–38, 2022.

[5] J. Jagadeesan, S. Karthik, and P. Rajesh, “Touchless ATM using augmented reality and TOTP Haar cascade algorithm,” *International Journal of Scientific and Computational Engineering*, vol. 15, no. 1, pp. 1–6, Mar. 2025.

[6] S. A. Kumar, M. R. Naik, and P. S. Rao, “AI-driven ATM premises using Raspberry Pi technology,” *International Journal for*

Research in Applied Science and Engineering Technology (IJRASET), vol. 13, no. 4, pp. 1123–1128, 2025.

[7] M. J. Rao, K. S. Reddy, and N. Kumar, "Third generation ATM using advanced image processing with face recognition," *International Journal of Research in Engineering, Science and Management*, vol. 5, no. 6, pp. 189–194, Jun. 2022.

[8] B. Sundar Raj and P. Manikandan, "A third generation automated teller machine using universal subscriber module with iris recognition," *Research Review on International Journal of Multidisciplinary*, vol. 3, no. 5, pp. 210–215, 2021.

[9] S. B. Patil, A. S. Jadhav, and V. R. Patil, "An AI-based ATM intelligent security system using OpenCV and YOLO," *International Journal of Trend in Scientific Research and Development (IJTSRD)*, vol. 5, no. 4, pp. 1120–1125, Jun. 2021.

[10] R. Mehta and A. Jain, "Face biometric authentication system for ATM using deep learning," *International Journal of Engineering Research & Technology (IJERT)*, vol. 10, no. 5, pp. 256–260, May 2021.

[11] A. Safarzadeh, M. Ghafourian, and S. A. Hosseini, "Enhancing precision of ATM network quality assessment using machine learning fusion," *arXiv preprint arXiv:2501.01067*, 2025.

[12] S. K. Mishra and R. Tiwari, "Artificial intelligence-based smart ATM for enhanced banking security," *International Research Journal of Engineering and Technology (IRJET)*, vol. 7, no. 6, pp. 345–349, Jun. 2020.