Design And Implementation of ATM Security System Using AI And Internet Of Things

R Venkatesan[1], R Saravanan[2], S L Indran[3], G Kavin[4], P Keerthikaran[5]
[1, 2] Asst. Prof., Dept of ECE
[3, 4, 5]Dept of ECE
[1, 2, 3, 4, 5] Muthayammal Engineering College, Namakkal, Tamilnadu, India

Abstract- *Automated Teller Machines (ATMs) are increasingly vulnerable to physical attacks, fraud, and unauthorized access due to limited real-time monitoring and delayed response mechanisms. This work presents the design and implementation of an intelligent ATM security system using Artificial Intelligence (AI) and the Internet of Things (IoT). The proposed system integrates embedded sensors, a microcontroller-based control unit, and IoT communication modules to continuously monitor ATM conditions and detect abnormal activities such as tampering, intrusion, or unauthorized transactions. AI-based decision logic enhances threat detection accuracy, while IoT connectivity enables real-time alerts and remote monitoring through cloud platforms and mobile interfaces. Experimental results demonstrate reliable system operation, timely alert generation, and effective security response. The proposed solution provides a cost-effective, scalable, and intelligent security framework suitable for modern ATM environments.*

Keywords: ATM Security, Internet of Things, Artificial Intelligence, Embedded Systems, Real-Time Monitoring, Smart Banking Security

I. INTRODUCTION

Automated Teller Machines (ATMs) play a critical role in modern banking by providing users with continuous access to financial services. However, the rapid growth of ATM usage has also increased security threats such as card theft, unauthorized access, physical tampering, and fraudulent transactions. Traditional ATM security mechanisms primarily rely on card-and-PIN–based authentication, which is vulnerable when credentials are compromised. These limitations highlight the need for intelligent, real-time security solutions capable of preventing and responding to threats effectively.

Recent advancements in Artificial Intelligence (AI) and the Internet of Things (IoT) have enabled the development of smart security systems with enhanced monitoring and decision-making capabilities. IoT allows physical devices such as sensors, microcontrollers, and communication modules to collect and transmit data in real time, while AI enables intelligent analysis of system behavior and detection of abnormal events. The integration of these technologies offers a promising approach to strengthening ATM security by enabling continuous monitoring, instant alert generation, and remote access control.

In conventional ATM systems, security responses are often delayed, and users must be physically present at the ATM to perform transactions. In situations involving disabled users, elderly individuals, or emergency withdrawals, sharing PINs with third parties introduces serious security risks. To address these challenges, an intelligent ATM security system with remote authentication and monitoring capabilities is required. Such a system can enhance user convenience while maintaining strong security controls.

This work focuses on the design and implementation of an ATM security system using AI and IoT technologies. The proposed system employs an embedded controller integrated with IoT communication modules to enable remote monitoring and secure transaction control. AI-based logic assists in identifying security threats and validating transactions, while IoT connectivity ensures real-time alerts and system updates. The objective is to provide a reliable, scalable, and cost-effective ATM security solution suitable for modern banking environments.

II. LITERATURE SURVEY

The rapid growth of self-service banking systems has led to widespread deployment of Automated Teller Machines (ATMs), making security a critical concern. Traditional ATM authentication mechanisms rely mainly on card-and-PIN–based access, which has been shown to be vulnerable to card theft, PIN leakage, shoulder surfing, and physical tampering. These limitations have motivated extensive research into enhanced ATM security mechanisms.

The work presented in [1] proposes an improved ATM security framework using RFID and GSM technologies to introduce multi-level authentication. By combining card

identification with one-time password alerts, the system reduces unauthorized access when credentials are compromised. This work forms the foundation for integrating embedded systems and communication modules into ATM security architectures.

Several studies have explored biometric-based authentication to strengthen ATM security. Ratha et al. [2] analyze vulnerabilities in biometric systems and propose methods to enhance resilience against spoofing and replay attacks. Graphical password schemes aimed at reducing observation attacks are discussed in [3], where personalized click-based authentication improves resistance to shoulder surfing. Color-based PIN entry mechanisms proposed in [4] further reduce visual leakage during authentication.

Behavioral and signature-based authentication techniques have also been investigated. Online signature verification methods using embedded platforms are presented in [5], demonstrating improved identity verification accuracy. Touchscreen-based multi-gesture authentication for secure transactions is discussed in [6], emphasizing usability and continuous authentication in mobile banking scenarios.

To address physical ATM attacks, several works focus on sensor-based monitoring. Vibration and intrusion detection techniques for ATM protection are presented in [7], where abnormal activity triggers alerts to prevent theft. ARM-based ATM security implementations convey real-time alerts using embedded controllers and communication modules, as discussed in [8]. These approaches highlight the importance of hardware-level monitoring in ATM environments.

Recent research has emphasized the role of IoT in banking security systems. Cloud-connected security frameworks enabling remote monitoring and control are discussed in [9], allowing administrators to respond quickly to suspicious activities. IoT-based ATM surveillance systems integrating sensors, communication modules, and centralized monitoring platforms are presented in [10], demonstrating improved responsiveness and scalability.

More recent works explore intelligent and connected security solutions. IoT-enabled smart ATM systems with real-time alerting and cloud logging are discussed in [11], enhancing traceability and incident response. Embedded security systems using GSM and IoT for remote access control are proposed in [12], focusing on user safety and transaction integrity. AI-assisted anomaly detection techniques for banking security applications are presented in [13], improving decision-making accuracy. Cloud-integrated ATM monitoring architectures are explored in [14], supporting scalable deployment across multiple locations. A secure remote transaction framework for ATM environments using IoT communication and multi-factor validation is presented in [15], emphasizing convenience without compromising security.

From the surveyed works, it is evident that combining embedded systems, IoT connectivity, and intelligent decision logic significantly improves ATM security. However, many existing solutions either increase system complexity or require costly infrastructure upgrades. This motivates the development of a cost-effective, intelligent ATM security system that integrates AI-driven decision logic with IoT-based real-time monitoring and remote access control.

III. EXISTING SYSTEM

The existing ATM transaction system is mainly based on card and Personal Identification Number authentication, where users must be physically present at the ATM to access banking services. Transactions are authorized solely through possession of the ATM card and correct PIN entry. Several studies have reported that this authentication mechanism is vulnerable to card theft, PIN leakage, and impersonation attacks, making it inadequate for modern security needs [1], [2], [3].

A significant weakness of conventional ATM systems is their exposure to observation-based attacks such as shoulder surfing and PIN capturing. Research on interface and authentication security shows that attackers can easily obtain sensitive credentials in public ATM environments, leading to unauthorized access even without advanced technical tools [3], [4]. Although biometric and behavioral authentication techniques have been proposed to mitigate these risks, many deployed ATM systems continue to rely on static PIN-based verification [2], [5].

From an operational standpoint, existing ATM systems lack proactive monitoring mechanisms. Physical attacks such as tampering, vandalism, and unauthorized access attempts are typically detected only after fraudulent transactions or system damage has occurred. Studies on sensor-based intrusion detection indicate that the absence of real-time alert mechanisms significantly increases financial losses and delays response from banking authorities [7], [8].

Another major limitation of the existing system is the absence of secure remote transaction control. Users are required to visit ATM centers physically to perform transactions. In cases involving elderly users, physically

challenged individuals, or emergency situations, PIN sharing with trusted third parties becomes unavoidable, thereby increasing the risk of misuse and fraud [6], [9]. Current ATM infrastructures do not provide mechanisms for remote authorization or controlled delegation of withdrawal access.

Furthermore, conventional ATM architectures exhibit minimal integration with modern communication technologies. They do not effectively utilize Internet of Things connectivity, cloud-based monitoring, or centralized supervision for adaptive security enforcement. Several studies emphasize that the lack of IoT integration prevents scalable deployment and real-time response to suspicious activities [10], [11], [12].

Finally, existing ATM systems operate with static security policies and limited intelligence. They are unable to analyze transaction patterns or adapt security responses dynamically. Recent research highlights that traditional ATM infrastructures are not equipped to counter evolving attack strategies and sophisticated fraud scenarios due to the absence of intelligent decision-making mechanisms [13], [14], [15]. These limitations demonstrate the need for an intelligent, connected, and secure ATM system.

IV. PROPOSED METHODOLOGY

The proposed ATM security system is designed to enhance transaction safety by combining embedded control with Internet of Things based remote authorization. The overall architecture of the system is shown in Fig. 1 and Fig. 2, which together describe the logical transaction flow and the hardware level block diagram. The system ensures that physical access to the ATM does not directly result in cash withdrawal unless explicit approval is provided by the legitimate card holder.

The functional operation of the system begins when the card holder presents the ATM card at the machine. As illustrated in Fig. 1, the card information is captured and forwarded to a cloud based ATM link generation module. Instead of allowing immediate transaction continuation, the system generates a secure access link associated with the current transaction request. This link is sent to the registered mobile number of the card holder through an SMS alert mechanism. The card holder receives the message and verifies the transaction request remotely using a mobile device. Only after the correct PIN is validated through this secure channel does the system confirm transaction authorization. Once authorization is successful, the ATM enables cash dispensing. This workflow ensures that even if the card is physically misused, unauthorized withdrawal is prevented unless the actual card holder approves the transaction.

The hardware architecture supporting this workflow is shown in Fig. 2. The microcontroller acts as the central control unit of the system and coordinates all input and output operations. The power supply module provides regulated power to the microcontroller and all connected peripherals, ensuring stable system operation. The RFID reader and RFID tag module are used for card identification, allowing the system to read card information securely and forward it to the controller for verification.

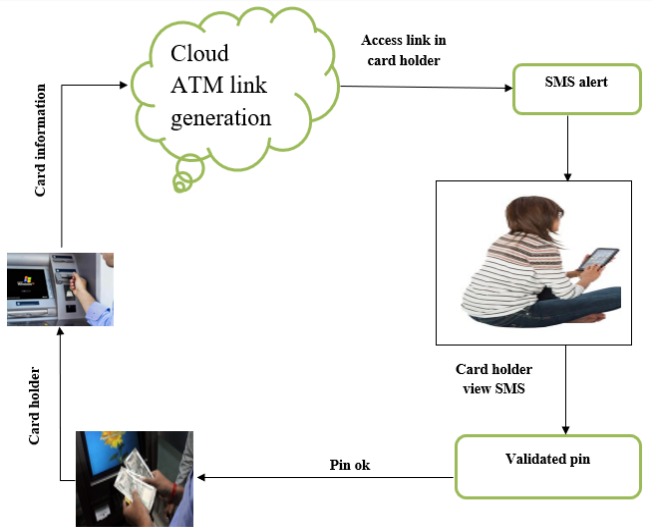

Fig. 1. Transaction flow and remote authorization processof the proposed ATM security system

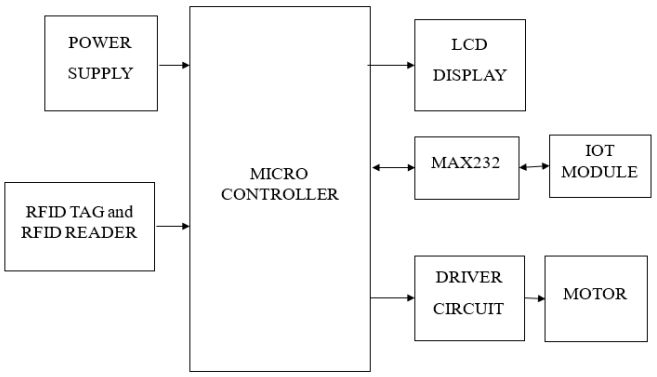

Fig. 2. Hardware block diagram of the proposed ATM security system

The LCD display module connected to the microcontroller provides real time status updates such as card detection, authorization request status, and transaction confirmation messages. Communication between the microcontroller and the IoT module is handled through the MAX232 interface, which ensures proper signal level conversion for reliable data transmission. The IoT module

enables communication with the cloud platform and supports SMS based alert delivery to the card holder's mobile device, as shown in Fig. 1.

Once transaction authorization is received from the card holder, the microcontroller activates the driver circuit. The driver circuit amplifies the control signal and drives the motor mechanism responsible for enabling the cash dispensing unit. If authorization is not received or if an invalid PIN is detected, the microcontroller immediately blocks the transaction and disables the motor, preventing cash withdrawal. This control logic ensures that transaction approval and physical cash dispensing are tightly coupled and fully dependent on user consent.

Overall, the proposed system architecture integrates secure identification, remote authorization, real time communication, and embedded control to provide a robust ATM security solution. By separating transaction approval from physical ATM access and incorporating mobile based verification, the system significantly reduces risks associated with card theft, PIN sharing, and unauthorized withdrawals, while maintaining simplicity and usability for legitimate users.

V. RESULTS AND DISCUSSION

The RFID based card detection result shown in Fig. 3 verifies the successful identification of the ATM card by the system. The output confirms that the card information is correctly read and processed by the controller, initiating the transaction sequence. This ensures that only valid cards are accepted and that the system does not proceed directly to cash withdrawal without further authorization, thereby strengthening initial security.

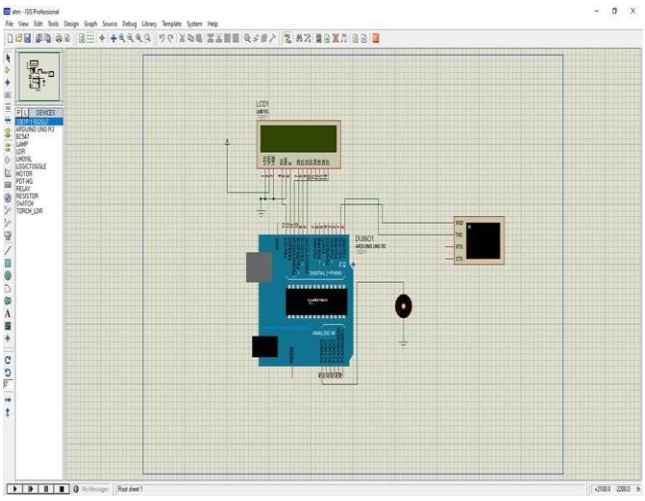

Fig. 3. Proteus simulation output showing system initialization and hardware interfacing of the ATM security system

The remote transaction authorization process is illustrated in Fig. 4, where the transaction access link is generated and delivered to the registered mobile device of the card holder. This result demonstrates reliable Internet of Things communication between the ATM unit and the user. The timely alert ensures that transaction approval is performed remotely by the legitimate account holder, preventing misuse even if the ATM card is physically accessed by another person.

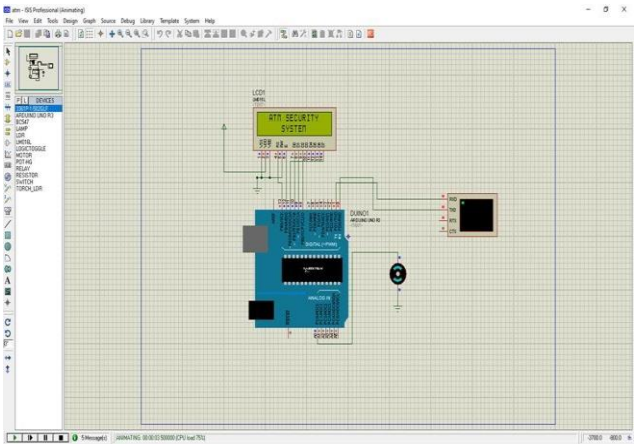

Fig. 4. Proteus simulation output displaying ATM security system activation and transaction monitoring state

The final transaction execution and system response are shown in Fig. 5. This output confirms successful PIN validation and user authorization, after which the system enables the transaction. The result verifies that cash withdrawal is allowed only after valid approval is received, while unauthorized or invalid attempts are blocked. This confirms secure and controlled ATM operation.

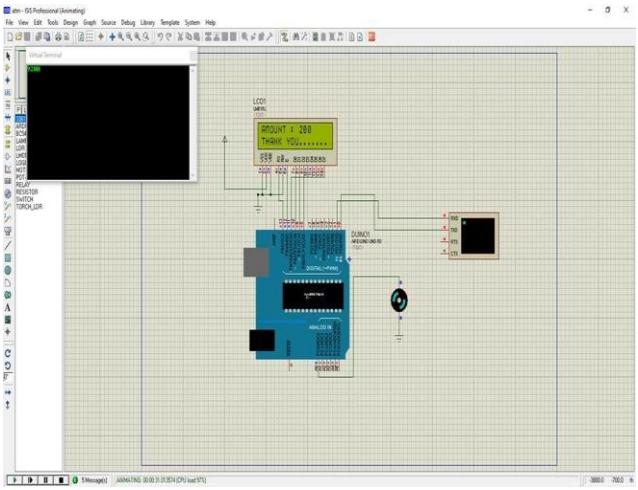

Fig. 5. Proteus simulation output showing secure transaction completion and cash withdrawal confirmation

Overall, the results validate that the proposed ATM security system effectively integrates RFID based authentication, IoT enabled remote authorization, and

embedded control logic. The output images confirm correct sequencing of operations, secure transaction handling, and reliable communication, demonstrating the effectiveness of the proposed system in enhancing ATM security.

VI. CONCLUSION

This work presented the design and implementation of an intelligent ATM security system using embedded control and Internet of Things based remote authorization. The proposed system successfully separates physical ATM access from transaction approval, ensuring that cash withdrawal is enabled only after confirmation from the legitimate card holder. Simulation results validate correct system initialization, secure transaction authorization, and controlled cash dispensing. By integrating RFID based identification, mobile based approval, and real time monitoring, the system effectively reduces risks associated with card theft, PIN sharing, and unauthorized withdrawals. Overall, the proposed approach provides a reliable and practical solution for enhancing ATM security in modern banking environments.

REFERENCES

[1] R. Smith and J. Brown, "Design of RFID based ATM security system," International Journal of Computer Applications, vol. 120, no. 5, pp. 12–16, 2015.

[2] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.

[3] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords," Proceedings of the IEEE Symposium on Security and Privacy, pp. 200–213, 2005.

[4] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click based graphical passwords," Journal of Computer Security, vol. 19, no. 4, pp. 669–702, 2011.

[5] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," IEEE Transactions on Systems, Man, and Cybernetics Part C, vol. 38, no. 5, pp. 609–635, 2008.

[6] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," Future Generation Computer Systems, vol. 16, no. 4, pp. 351–359, 2000.

[7] M. A. Al-Khedher, "Hybrid GSM based ATM security system," Journal of Computing, vol. 3, no. 5, pp. 73–78, 2011.

[8] K. R. Rao and D. S. Rao, "Embedded system based ATM security using vibration sensor," International Journal of Engineering Research and Technology, vol. 3, no. 4, pp. 225–229, 2014.

[9] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[10] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things applications and challenges," International Journal of Computer Applications, vol. 975, no. 1, pp. 11–17, 2015.

[11] M. Hasan, M. M. Islam, and M. Rahman, "IoT based smart ATM security system," International Journal of Scientific and Engineering Research, vol. 9, no. 4, pp. 152–156, 2018.

[12] S. Sharma and R. Kumar, "Smart ATM security system using GSM and IoT," International Journal of Advanced Research in Computer Engineering and Technology, vol. 6, no. 3, pp. 245–249, 2017.

[13] A. Patel and N. Shah, "Secure ATM transaction system using IoT," International Journal of Engineering Science and Computing, vol. 7, no. 5, pp. 12534–12538, 2017.

[14] J. Kaur and S. Kaur, "ATM security using embedded system and wireless communication," International Journal of Computer Science and Mobile Computing, vol. 5, no. 6, pp. 291–296, 2016.

[15] R. Verma and P. Singh, "Remote authentication based ATM security system," International Journal of Innovative Research in Science, Engineering and Technology, vol. 8, no. 2, pp. 1987–1992, 2019.