WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# PHYSICAL AND CYBER SECURITY OF ATM

***Prof. Rupali Patil[1], Mauli Harpude[2], Omkar Pande[3], Om Shende [4]***

Department of Electronics & Telecommunication Engineering, RMD Sinhgad College of Engineering, Pune

**ABSTRACT:**

Automated Teller Machines (ATMs) play a vital role in modern banking by offering convenient, round-the-clock access to financial services. However, they are increasingly targeted by both cyber and physical threats. This paper explores the dual dimensions of ATM security, examining how vulnerabilities in software, networks, and user interfaces expose systems to cyberattacks such as skimming, malware injection, and man-in-the-middle attacks. Simultaneously, physical threats including card trapping, cash trapping, and brute-force break-ins continue to pose serious risks. The study evaluates current security mechanisms, such as encryption protocols, biometric authentication, surveillance systems, and anti-tampering technologies. Furthermore, it highlights the importance of a layered defense strategy that integrates cybersecurity best practices with robust physical safeguards. By addressing these combined challenges, this research aims to guide the development of more resilient ATM infrastructures that can better protect financial assets and customer information.

**Keywords** - Rf id - EM18 , ACCELEROMETER - adxl345, Dash SENOER , keYpad 4X4, Raspberry= 3a (32gb memory), gsm800 , TRANFORMER 12V , regulator ,rectifier, I2c display (16-2), adapter 5 v.

## INTRODUCTION

Automated Teller Machines (ATMs) have become an essential part of the global banking infrastructure, offering customers quick and easy access to cash and other financial services. With the growing dependence on these machines, ensuring their security has become a major concern for banks, regulatory bodies, and technology providers. ATMs are exposed to a range of threats that fall into two main categories: cyber and physical attacks. Cyber threats target the internal systems and software of the ATM, often aiming to steal sensitive customer data or manipulate financial transactions. In contrast, physical threats involve direct tampering with the machine itself, such as forced entry, card skimming devices, or installation of hidden cameras.

As cybercriminals and physical attackers continue to develop more advanced techniques, the need for a comprehensive and integrated security approach becomes increasingly critical. This includes the deployment of secure software, real-time monitoring, user authentication methods, and physical deterrents like reinforced hardware and surveillance systems. This paper delves into the common vulnerabilities, recent attack trends, and the latest innovations in ATM security, aiming to provide a holistic understanding of how to protect these systems in an evolving threat landscape.

## Literature Review

The security of Automated Teller Machines (ATMs) has been a growing area of research due to the increasing number and complexity of attacks. Various studies have examined the evolving techniques used by attackerand the corresponding defense mechanisms.

Researchers have explored **cyber threats** such as malware-based attacks, where malicious code is introduced into ATM software to intercept card data or manipulate transactions. Studies have reported incidents where trojans like “Skimer” and “Tyupkin” enabled criminals to control ATMs remotely. These works emphasize the need for secure operating systems, regular software updates, and network isolation to reduce the attack surface.

In terms of **data protection**, literature suggests the adoption of strong encryption techniques and secure PIN entry mechanisms. Multi-factor authentication, including biometrics and mobile verification, is also being explored as an additional layer of defense. A number of papers highlight the weaknesses of magnetic stripe cards and recommend the widespread implementation of EMV (Europay, Mastercard, and Visa) chip technology for increased security.

On the **physical security** side, several studies have examined the effectiveness of anti-skimming devices and surveillance systems. Physical tampering techniques, such as card trapping, keypad overlays, and cash compartment breaches, remain common attack vectors. Research supports the integration of vibration sensors, GPS tracking, and reinforced ATM enclosures to deter these threats.

Recent literature also underlines the importance of **user awareness** and staff training as part of a comprehensive security approach. Some studies have proposed machine learning algorithms to detect suspicious transaction patterns or physical behavior around the ATM.

Overall, the literature reveals that while significant advancements have been made in both cyber and physical security, a combined and continuously adaptive strategy is necessary. Future research is shifting toward the integration of artificial intelligence, blockchain, and advanced biometrics to provide more proactive and resilient ATM security frameworks.

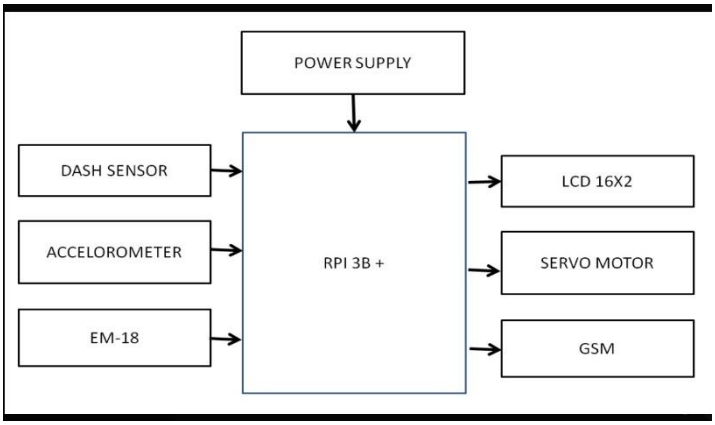


**Figure 1. Block Diagram of Cyber And Physical Security Of ATM**

## System Development

Developing a secure ATM system requires a multi-layered approach that addresses both digital and physical threats. The system architecture must integrate robust software security protocols, physical protection mechanisms, and intelligent monitoring tools to detect and prevent unauthorized access.

**1.Cybersecurity Measures:**
At the core of the system is secure software that operates on a hardened operating system with minimal services running to reduce vulnerabilities. The ATM software should include features such as encrypted communication between the machine and the bank's server, secure boot processes, and endpoint protection. Firewall configurations and intrusion detection systems (IDS) should be employed to monitor for suspicious network activity. User authentication should be enhanced using technologies like biometric verification (e.g., fingerprint or facial recognition) and One-Time Passwords (OTPs) sent via SMS or email.

**2. Physical Security Features:**
To defend against physical tampering, the system should incorporate tamper-proof hardware components, including reinforced ATM enclosures, anti-skimming card readers, and secure cash dispensers. Physical sensors, such as vibration detectors, thermal sensors, and door intrusion alarms, can alert authorities in real time if unauthorized access is attempted. In addition, high-definition surveillance cameras and GPS tracking systems can aid in monitoring and recovery efforts in case of theft.

**3. Real-Time Monitoring and Alerts:**
A centralized security dashboard should be developed to monitor all ATMs in real-time. This dashboard would collect data from cyber and physical sensors, process it using anomaly detection algorithms, and trigger alerts in case of suspicious activities. Integration with banking networks allows immediate freezing of ATM operations if an attack is detected.

**4. Regular Updates and Maintenance:**
An essential component of system development is the ability to perform remote updates and patches to the ATM software. This ensures that any newly discovered vulnerabilities can be quickly mitigated. Routine maintenance checks and audits of physical and software systems should be scheduled to ensure consistent protection.

**5.User Awareness and Interaction:**
The system interface should educate users about common fraud tactics (e.g., checking for skimming devices) and provide secure transaction prompts. Clear, user-friendly screens and secure PIN entry shields can reduce the risk of user-targeted attacks like shoulder surfing.
By combining these elements into a unified development plan, ATM systems can be made significantly more secure. The goal is not just to prevent attacks but to detect and respond to them efficiently, minimizing potential damage and maintaining customer trust.

**Figure 1. Assembled Hardware Kit of Physical And Cyber Security of ATM.**

## Conclusion

This paper presents ATMs continue to serve as a critical access point to banking services, ensuring their security remains a top priority. Both cyber and physical threats have evolved in complexity, targeting system vulnerabilities and customer data with increasing sophistication. This study highlights the need for a layered security approach that addresses these dual challenges. Implementing secure software, encryption, biometric authentication, and regular system updates is essential for defending against cyber threats. Simultaneously, reinforcing ATMs with anti-skimming devices, tamper-resistant hardware, and real-time monitoring can help deter and respond to physical attacks.

**REFERENCES**


1. European Central Bank. (2015). *Report on Card Fraud*. Retrieved from https://www.ecb.europa.eu
2. Kingpin, F. (2018). *Skimming and ATM Fraud: Understanding the Threat Landscape*. SANS Institute. Retrieved from https://www.sans.org
3. Kumar, P., & Sachdeva, M. (2020). Security issues in ATM systems: A review. *International Journal of Computer Applications*, 176(34), 12–16. https://doi.org/10.5120/ijca2020919883
4. Visa Security Team. (2021). *ATM Threat Intelligence Report*. Visa Inc. Retrieved from https://usa.visa.com
5. Bhargava, A., & Lal, A. (2019). A comprehensive survey on physical and cyber security of ATMs. *International Journal of Engineering Research and Technology*, 8(6), 1087–1092.
6. PCI Security Standards Council. (2023). *PCI PIN Security Requirements*. Retrieved from https://www.pcisecuritystandards.org
7. Symantec. (2017). *Financial Threats Report*. Norton by Symantec. Retrieved from https://www.symantec.com
8. Alzubaidi, L., & Kalita, J. (2016). Authentication of ATM users using facial recognition: A secure approach. *Procedia Computer Science*, 140, 602–609. https://doi.org/10.1016/j.procs.2018.10.369