ATM Safety Alert

Prof. SHUSHMA PATWARDHAN[1], Prof. REENA ASATI[2], TEJASHREE DIXIT[3], ANIKET KOLI[4], SHUBHAM PATIL[5], SAMRUDDHI KOTKAR[6]

[1]Head of Department (ENTC), [2]Electronics and Telecommunication Engineering Department, [3]Genba Sopanrao Moze College of Engineering, Balewadi, Pune Maharashtra - 411045
[1,2,3]Student, Electronics And Telecommunication Engineering Department, Genba Sopanrao Moze College Of Engineering, Balewadi, Pune Maharashtra – 411045

ABSTRACT

This safety alert aims to raise public awareness regarding increasing incidents of ATM-related crimes, including card skimming, shoulder surfing, and physical theft. Criminals are employing advanced tactics such as hidden cameras, fake keypads, and remote data capture to steal personal banking information and commit fraud. Additionally, physical attacks near ATM machines, especially during nighttime or in poorly lit areas, have also been reported.

The alert emphasizes the importance of vigilance while using ATM machines and outlines safety measures such as covering the keypad during PIN entry, avoiding isolated machines, inspecting the ATM for suspicious devices, and being aware of surroundings. Financial institutions are advised to enhance surveillance, improve lighting, and educate customers on secure ATM practices.

Proactive measures by both users and institutions are crucial in mitigating risks and ensuring secure banking transactions.

The purpose of this project is to enhance the safety and security of Automated Teller Machine (ATM) users by identifying risks, raising awareness, and implementing preventative measures against ATM- related crimes. With the rise in fraudulent activities such as skimming, card trapping, PIN theft, and physical assaults, there is a critical need to educate the public and improve security infrastructure around ATM usage.

Keywords: *Survelience Camera, ATm Safety, Theif Protection, GPS location alert, Siren alert,*

INTRODUCTION

Automated Teller Machines (ATMs) have become an integral part of modern banking, offering convenient, round-the-clock access to financial services such as cash withdrawals, fund transfers, and balance inquiries. As the use of ATMs continues to grow worldwide, so too does the potential for criminal exploitation of this technology. ATM-related crimes—including card skimming, trapping, PIN theft, and even physical attacks—have increasingly become a serious threat to the safety and security of customers and their financial assets.Criminals have adopted sophisticated methods to compromise ATM transactions. These include the use of hidden cameras, fake keypads, card skimmers, and more recently, malware and cyber tools to access sensitive banking data.

Additionally, physical threats such as robbery or assault at or near ATMs—especially in secluded or poorly lit locations—pose a direct danger to users.

Despite security enhancements implemented by banks and financial institutions, ATM fraud and user- end negligence remain prevalent. A lack of awareness about potential risks, coupled with unsafe behaviors such as

DOI: 10.55041/IJSREM53787

not covering the PIN, using ATMs alone at night, or ignoring signs of tampering, can make individuals easy targets.

This project, ATM Safety Alert, is initiated in response to these growing concerns. It aims to analyze current ATM safety issues, educate the public on safe ATM usage practices, and recommend both technical and behavioral measures to prevent crimes. By identifying key risk areas and suggesting actionable solutions, the project seeks to minimize ATM-related incidents and foster a safer banking environment for all users.

LITERATURE REVIEW

The increasing use of Automated Teller Machines (ATMs) has attracted significant attention from researchers and security professionals due to the rise in ATM-related fraud and criminal activities.

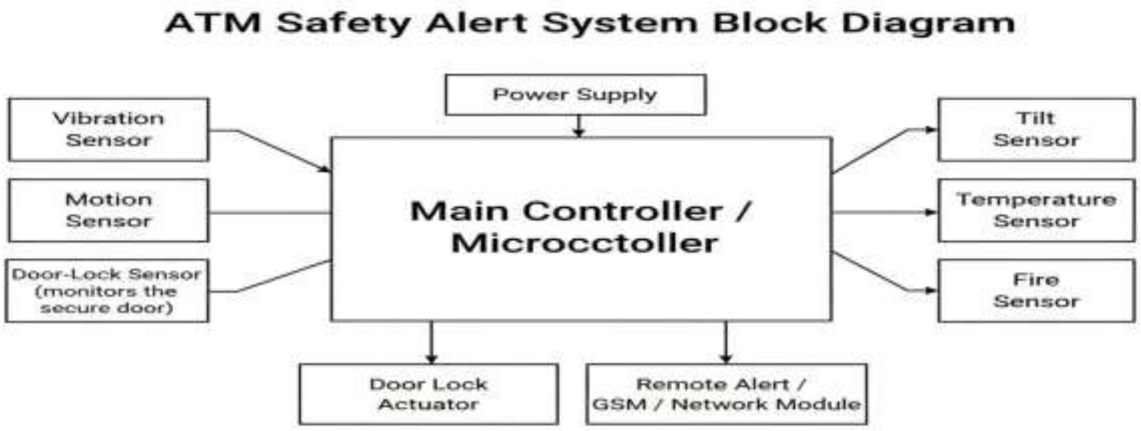
Several studies have explored the types of threats faced by ATM users and the corresponding security measures. According to Jain and Goyal (2019), card skimming and PIN theft are among the most common methods used by fraudsters, often involving hidden cameras and fake card readers installed on ATMs. Their study emphasizes the need for continuous technological updates to ATM systems.

A report by the Reserve Bank of India (2020) highlights the importance of user awareness and behavioral factors in preventing fraud, noting that a majority of successful attacks occur due to a lack of public knowledge about secure ATM practices. Further, research by Smith et al. (2021) discusses the effectiveness of installing surveillance cameras, anti-skimming devices, and biometric verification in reducing ATM-related crimes, particularly in urban areas.

SYSTEM ARCHITECTURE

Block Diagram

A typical Block Diagram of Project is shown in figure 1. Microcontroller The system includes components such as a Power Supply, vibration sensor, motion sensor, Door Lock actuator, Tilt Sensor, Temperature Sensor, Fire Sensor,Remote, alert / Gsm / Network module this are used in this


ATM Safety Alert System Block Diagram
Power Supply
Vibration Sensor
Motion Sensor
Door-Lock Sensor (monitors the secure door)
Main Controller / Microcctoller
Tilt Sensor
Temperature Sensor
Fire Sensor
Door Lock Actuator
Remote Alert / GSM / Network Module

aFigure 1

CIRCUIT DIAGRAM

A Circuit Diagram of Project is shown in figure 2. The Main Controller is the center. It uses a Power Supply. Sensors are inputs. The Vibration Sensor detects shocks. The Motion Sensor detects intruders. The Door-Lock Sensor monitors the door. The controller checks the Tilt Sensor for movement. It monitors the Temperature Sensor and Fire Sensor. If a threat is found, it uses the Door Lock Actuator. Most importantly, it sends a Remote Alert to security.

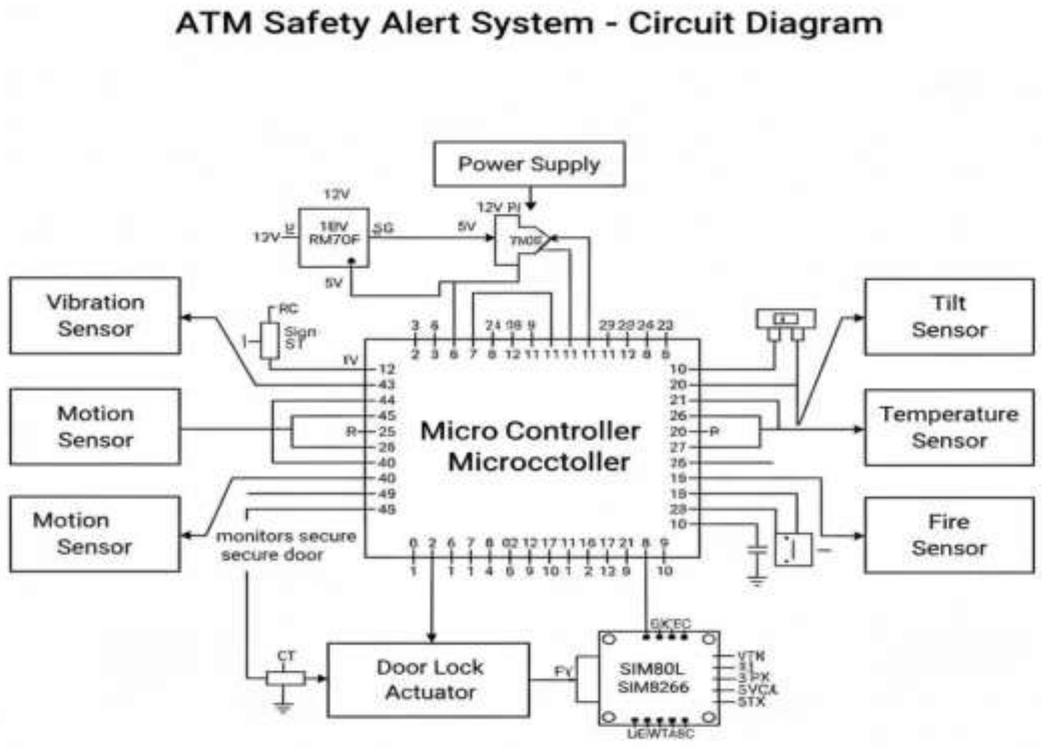


Figure 2

HARDWARE REQUIREMENTS AND SPECIFICATIONS

Main Controller / Microcontroller

Acts as the brain of the system — reads all sensor inputs, processes them, and triggers alerts or actuators.

1. **Power Supply**

Provides stable voltage to sensors, microcontroller, and modules.

2. **Vibration Sensor**

Detects shaking, drilling, or hammering on the ATM machine.

3. **Motion Sensor**

Detects human movement inside or around the ATM cabin.

4. **Door-Lock Sensor (Secure Door Monitor)**

Detects if the ATM cabin door or internal safe is opened.

5. **Tilt Sensor**

Detects if the ATM machine is tilted, lifted, or moved.

6. **Temperature Sensor**

Monitors the internal temperature of the ATM to detect overheating.

7. **Fire Sensor**

Detects presence of fire or smoke near the ATM enclosure.

8. **Door Lock Actuator**

Controls the physical lock mechanism of the ATM door or safe.

9. **Remote Alert / GSM / Network Module**

Sends SMS, call, or data alert to remote security center.

10. **Relay Module (for actuators)**

Switches higher current devices like locks or alarms.

11. **Optional Alarm / Buzzer**

Provides audible alarm when an event occurs.

Advantages

1. **Crime Deterrence:**

Visible cameras discourage criminals from attempting theft, vandalism, or fraud at ATMs because they know their actions are being recorded, increasing the risk of identification and arrest.

2. **Evidence Collection:**

High-quality video footage provides clear evidence for law enforcement investigations, helping to identify suspects and reconstruct the sequence of events during a security breach or fraud attempt.

3. **24/7 Surveillance:**

Cameras provide continuous monitoring, including during nighttime or low-light conditions thanks to infrared or night vision technology, ensuring the ATM area is always under watch.

4. **Remote Monitoring and Quick Response:**

Security teams can access live camera feeds remotely, enabling them to detect suspicious activity in real-time and coordinate prompt responses or alerts to authorities, minimizing damage.

5. **Enhanced User Safety and Confidence:**

Knowing that ATMs are monitored by cameras makes customers feel safer when withdrawing cash, encouraging more frequent use and improving overall trust in banking services.

Disadvantages

1. **High Installation and Maintenance Costs:** Setting up high-quality cameras, along with necessary storage and monitoring infrastructure, can be expensive, especially for multiple ATM locations.
2. **Vulnerability to Tampering:** Cameras themselves can be damaged, obstructed, or disabled by vandals or criminals, rendering the surveillance ineffective without immediate detection.
3. **Data Management Challenges:** Storing, processing, and managing large volumes of video footage require robust systems and can raise concerns over data security and retention policies.

RESULTS

The comparative study of various versions of ATM safety technologies shows a progressive improvement in both physical and digital security mechanisms.

Early ATMs (Version 1–2) focused mainly on basic physical protection like metal safes, PIN authentication, and CCTV monitoring.

Mid-level versions (Version 3–4) introduced tamper sensors, anti-skimming devices, and software- based security such as encrypted communication and endpoint protection.

While modern ATMs provide robust protection against both cyber and physical threats, upgrading old machines and integrating advanced technologies remain key challenges due to cost and compatibility factors.

CONCLUSION AND FUTURE SCOPE

The evolution of ATM safety technology shows a clear shift from basic physical protection to intelligent,networked,andAI-driven systems.

Early ATMs relied only on mechanical locks and PIN-based access, making them highly vulnerable to theft and skimming. With time, digital surveillance, tamper sensors, and software-based protection have significantly improved ATM security. Modern systems (Gen 4–Gen 5) now integrate secure operating systems, real-time monitoring, and machine learning algorithms to detect and prevent both physical and cyber threats. However, legacy ATMs still in use globally remain a major weakness. Upgrading them to newer standards is crucial for reducing fraud risk, complying with data security norms (like PCI DSS), and maintaining customer trust.

FUTURE SCOPE

1. AI and Machine Learning Integration
   - Wider use of AI for *real-time a.nomaly detection*, predictive maintenance, and fraud pattern
   - Self-learning systems that adapt to new attack methods.
2. IOT-Enabled ATMs
   - Smart sensors that monitor temperature, vibration, and tampering in real time.
   - Cloud-connected ATMs for instant alerts and automated shutdowns during attacks.

3. Biometric and Multi-Factor Authentication
   - Broader adoption of fingerprint, facial, and iris recognition for enhanced user verification.
   - Combining biometrics with tokens or mobile authentication for layered security.
4. Blockchain-Based Transaction Security
   - Using blockchain for *secure, transparent, and tamper-proof* ATM transaction records.
5. Enhanced Privacy and User Interface Security
   - Use of privacy screens, anti-shoulder-surfing technology, and voice-guided secure input.
6. Cloud and Edge Computing
   - Moving ATM software to secure cloud or edge platforms for faster updates and remote threat response.
7. Green & Energy-Efficient ATMs
   - Integration of eco-friendly designs and power-efficient components without compromising

REFERENCES

1. ATMeye.iQ. (2024). *Security Features of ATM Machines.* Retrieved from https://atmeye.com/blog/security-features-of-atm/
2. PonDiot Technologies. (2025). *ATM Security Trends for 2025: AI, RKL, and IoT-based Protection.* Retrieved from https://www.pondiot.com/blog/atm-security-trends-2025
3. Help Net Security. (2024). *Rain Technology Introduces Switchable Privacy for ATM Displays.* Retrieved from https://www.helpnetsecurity.com/2024/09/13/rain-technology- atm-switchable-privacy/
4. Cyttek Group. (2023). *Checker ATM Security® – Endpoint Protection for ATMs.* Retrieved from https://cyttek.com/prod-checker-eng.html
5. ATM Marketplace. (2023). *ATM Security: The Digital Difference.* Retrieved from https://www.atmmarketplace.com/articles/atm-security-the-digital-difference/
6. Wikipedia. (2024). *IBM 3624 ATM.* Retrieved from https://en.wikipedia.org/wiki/IBM_3624
7. Turkish Journal of Computer and Mathematics Education (TURCOMAT). (2021). *A Study on ATM Security: Electronic Theft and Physical Attacks.* Retrieved from https://turcomat.org/index.php/turkbilmat/article/download/8302/6478/14883
8. PCI Security Standards Council. (2024). *PCI DSS and PIN Security Standards for ATM Transactions.* Retrieved from https://www.pcisecuritystandards.org/