https://doi.org/10.1051/itmconf/20257901001

# Design of Smart Security system for ATM

*Aska.* K S[1*], *Manjula.* T R[1], *Nandagoban.* M[1], *Anto* John Bosco. A[1], and *Moustapa* Daoud Narene[1]

[1]Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Jain (Deemed to be University), Bengaluru, India

**Abstract.** As technology rapidly evolves, it brings along fresh and innovative solutions aimed at enhancing security in the banking sector. In this spirit, this project proposes a Smart ATM Security System that harnesses Internet of Things technology and GPS tracking to help prevent unauthorized access and theft. This system is designed to continuously monitor the ATM environment in real- time using a combination of IoT sensors, GPS modules, and communication technologies. It can detect tampering or unusual activities, such as physical impacts, unauthorized access attempts, or any unauthorized movement of the ATM. When suspicious activity is detected, the system responds in multiple ways. It tracks the real-time GPS location of the ATM, activates an alarm, makes automatic calls to pre-set contacts, and sends notifications through SMS or mobile apps. To provide security personnel with valuable context, the system also features live video streaming, capturing visuals and recordings of any incidents. By leveraging IoT technology and cloud integration, this solution ensures continuous monitoring and allows for remote control of the ATM's operations during emergencies. Overall, this smart security system offers strong, scalable, and cost-effective way to protect ATMs. The paper presents the design and implementation of ATM security system by integration of microcontroller sensors and actuators. This automated system senses ATM machine and environment and take proactive actions like shutting doors and tracking real time location and automated alerts. The system is simulated and tested using ThinkSpeak App. The results demonstrate temperature and vibration sensor data status and remotely accessing latitude and longitude of the location. we create a proactive defense strategy that truly enhances security in the banking sector, keeping community's assets safe.

## 1 Introduction

Automated teller machines (ATMs) play a crucial role in providing convenient access to banking services for millions of people worldwide. ATM machines are vulnerable to physical attacks such as theft, vandalism, and fire, especially in Remote areas with limited surveillance. Moreover, fraudsters use a variety of deceptive tactics. ATM fraud not only affects banks but also poses a real threat to everyone involved. It calls for a united effort between banks, their customers, and law enforcement to tackle the issue effectively. The impact of ATM fraud can be damaging—not just financially, but also in terms of trust. When customers experience fraud, it can shake their confidence in using ATMs, leading them to hesitate in making transactions.

Existing security systems lack real-time location tracking, automated response, and instant alerts. There is a need for a smart ATM security system that uses GPS, GSM, and sensors to detect threats, send alerts, and lock the ATM automatically to prevent damage or theft [1].

Traditional ATM security measures often rely on physical barriers and surveillance cameras, but with the increasing sophistication of criminal tactics, there is a need for more robust security systems. The Smart ATM Security System combines multiple layers of security, including real-time monitoring, and remote management capabilities. Integrates advanced physical security technologies and measures to protect ATM infrastructure, components, and users from various physical threats, including vandalism, theft, and unauthorized access. Key components of the Smart ATM Physical Security System include tamper-resistant enclosures, alarm systems, surveillance cameras, biometric access control, remote monitoring and management capabilities, environmental sensors, and physical deterrents. These components work together to provide multi-layered protection for ATM assets and operations, ensuring the integrity, reliability, and safety of ATM transactions in diverse environments.

It offers several advantages, including enhanced protection against physical attacks, deterrence of criminal activities, real-time monitoring and detection of security incidents, proactive response to threats, and efficient management of ATM fleets. By deploying the Smart ATM Physical Security System, financial institutions can strengthen their ATM security posture, minimize operational risks, and enhance customer trust and confidence in ATM services.

This system is designed to continuously monitor the ATM environment in real-time using a combination of IoT sensors, GPS modules, and communication technologies. It can detect tampering or unusual

* Corresponding author: ks.asha@jainuniversity.ac.in

activities, such as physical impacts, unauthorized access attempts, or any unauthorized movement of the ATM. When suspicious activity is detected, the system responds in multiple ways. It tracks the real-time GPS location of the ATM, activates an alarm, makes automatic calls to pre-set contacts, and sends notifications through SMS or mobile apps.

The main goal of smart ATM physical security systems is to keep ATMs safe from physical attacks and other vulnerabilities, ensuring that they operate securely and reliably. The top priority is given to prevent physical attacks on ATMs, including vandalism. This includes taking steps to guard against theft, ram raids, and other forms of interference. By implementing these protective measures, we aim to create a secure environment for ATM infrastructure, components, and cash assets.

## 2 Literature survey

The literature surrounding smart ATM physical security systems presents a comprehensive overview of the challenges, advancements, and strategies in securing automated teller machines (ATMs) against physical threats and vulnerabilities. Researchers and industry experts have explored various technologies, measures, and methodologies to enhance the physical security of ATM infrastructure, components, and users. Here's a survey of some key findings and trends from recent studies.

The security system for ATM comprises NodeMCU ESP8266 with built in Wi-Fi, the passive infrared sensor, LCD display and telegram app. The security offered by the system is not robust as it only involves in detecting motion around which may give false alarms further lcd displays are not effective in alerting authorities over security breaches. The secured ATM transactions are facilitated by RFID tags rather than ATM cards as proposed in [2]. The RFID safer when inserted get the user details, the camera attached to machine captures the photo of the operator and matches with the extracted card data, access is granted to true users while in case of data not matching, extracted data is sent to user for authentication before beginning the transaction. [3] proposes theft prevention system for ATM using Raspberry pi, vibration sensor, cameras and GPS/GSM communication modules for information dissemination enabling surveillance, intrusion detection, alert and response system however vibration sensor alone may not suffice for effective detection. Similar work is proposed in [4] by using Arduino controller, vibration sensor and IR sensor to indicate entry and exit of transactions however lacks the robustness in real time monitoring. The security feature of ATMs are enhanced by embedding image recognition feature for safe access and unauthorised transaction detections with ATM physical security provided by sensor based real time monitoring as discussed in [5]. One of the distinct feature of ATM security system proposed in [6] is face recognition system and spraying of gas to bring in unconscious condition to one who is involved in looting ATM, in addition to real time monitoring and alert system. The three level security based ATM is proposed in [7] which uses RFID tag reading to get user details confirmation. The finger print authentication is the second level followed by OTP confirmation from the user to begin transaction. This system will address the theft of misplacement of ATM cards while physical security of ATM machines is unaddressed. [8] proposes security system with similar features except MQ2 sensor for fire alarm and continuous video streaming. [9] proposes IoT based real time monitoring of ATMs by detecting security breaches and automated door locking system in case of assault on machines. A distinct feature is RFID tag based deactivation of sensors for maintenance of ATM systems. [10] proposes skimming device detection in ATMs by using cameras, sensors and machine learning algorithms. The physical security of the ATM is addressed in [11] by processing the camera images captured in the vicinity of the ATM to detect face and other weapons of assault. The images are processed by dep learning algorithms like RCNN, LSTM and Face net. [12] proposes ATM security by continuously video streaming ATM inside activity and real time monitoring and controlling using blynk app. The Deep learning method enhance the security of ATM system is demonstrated in [13]. Employing machine learning in ATM surveillance involves processing captured image for object, weapons and emotion detection under limited conditions of ATM environment and auto triggering the action is demonstrated in [14]. Based on the literature survey, the conclusion that can be drawn is ATM security is offered in terms of physical security and transaction security as summarised in Table 1. The integration of IoT monitoring devices of ATM and blynk app to alert and upload all sensor data to user is proposed in [15]. To ensure security and safety in ATM machines, all features listed in Table 2.

**Table 1.** The summary of literature survey.

| Sl. No | Highlights | Strengths | Limitation |
|---|---|---|---|
| 1. | Sensor based security system | Buzzer alert, SMS alert, location status, automatic door close activation | Ensures only physical ATM security |
| 2. | Transaction security | Double authentication before allowing transactions | Lacks physical ATM security |
| 3. | Machine learning based security system | Face recognition based transactions | Delay in transactions |
| 4. | Camera based security system | To identify masked persons, weapons | Delayed response |

## 3 Methodology

Some innovative frameworks and prototypes have been developed to combine GPS, IoT, and other technologies for ATM security. The microcontroller the Arduino can be used to build affordable and efficient security systems for ATMs.

Multi-Sensor Integration: By integrating various sensors (vibration, temperature, gas and motion) into a single platform, enables real time data collection for effective threat detection. In addition, it facilitates remote Management which enables e remote-lock or remote-disable, which allow security teams to swiftly lock or disable ATMs through IoT systems.

Remote Maintenance is vital for keeping operations running smoothly. It allows us to manage ATM fleets and address security incidents from a centralized location, ensuring that we're always in control. Further that empower administrators to keep an eye on ATM operations from anywhere. They can receive real-time alerts and perform maintenance tasks without having to be on-site. This not only helps reduce downtime but also boosts overall operational efficiency.

Protecting Against Physical Attacks: The priority is to prevent physical attacks on ATMs, including vandalism. This includes taking steps to guard against theft, ram raids, and other forms of interference. By implementing these protective measures, we aim to create a secure environment for ATM infrastructure, components, and cash assets.

## 3.1 Implementation

To enhance ATM security, a smart embedded system is developed using vibration sensors, temperature sensors, GPS, and GSM modules motors, buzzers and so on as shown in the block diagram Figure 1. The Vibration sensor detects physical tampering, drilling, or shaking of the ATM. If vibrations exceed a certain threshold, it assumes a potential break-in attempt. Similarly temperature sensor monitors internal ATM temperature. If a fire or heating tool is used for assault (e.g., during gas-based attacks), the system detects it. The GPS Module tracks the ATM’s exact location in real-time. When a threat is detected, the module fetches the latitude and longitude for emergency response. The GSM Module sends SMS alerts and makes calls to pre-registered numbers (e.g., police, security staff, bank manager) along with the ATM's location and status (e.g., “Vibration Detected” or “High Temperature Detected”). Buzzer or Siren sounds a local alarm to alert people nearby and deter intruders.

Door Lock Mechanism (DC Motor + Relay) Automatically triggers to lock the ATM booth or cash vault when a threat is confirmed, preventing unauthorized access.

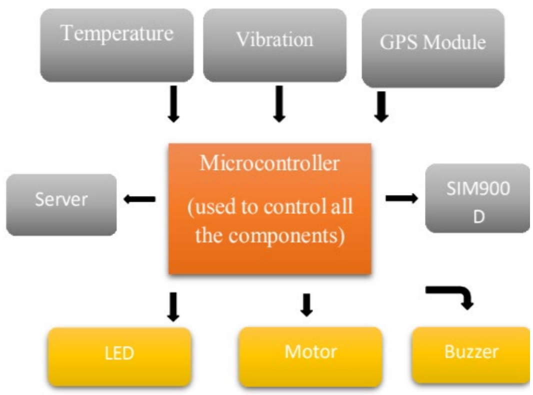


**Fig. 1.** Block diagram of the embedded smart ATM security system.

**Table 2.** The system components and specifications.

| Parameter | Specification |
|---|---|
| Microcontroller | Arduino UNO / NodeMCU |
| GSM Module | SIM800L (Quad-band 2G) |
| GPS Module | NEO-6M |
| Vibration Sensor | SW-420 |
| Temperature Sensor | LM35 / DHT11 |
| Motor Driver | L298N Dual H-Bridge |
| Door Lock Mechanism | 12V DC Motor with relay |
| Power Supply | 9V–12V Battery / Adapter with 5V regulator |
| Communication Method | GSM (SMS, Call) |
| Alert Types | SMS, Call, Buzzer Alarm |
| System Type | Real-Time Embedded Security System |

The IoT GPS and GSM technologies can significantly improve ATM security, especially when the traditional security measures have their limitations.

### *3.1.1 Real-Time monitoring using sensors*

IoT sensors—like those for vibration, temperature, and motion—can alert to tampering or unusual activity. For example, they can detect attempts at drilling, cutting, or using gas to break into an ATM.

### *3.1.2 GPS-based tracking*

GPS plays prominent role in ATM security by its ability to provide real-time location tracking. ATMs equipped with GPS can lead to quick detection of unauthorized movements or theft of the machines. The associated Geo fencing feature sends alerts if an ATM moves beyond specified geographic boundaries. While GPS is largely reliable, it can be affected by signal interference in busy urban areas or enclosed spaces. The NavIC -the Indian navigation system which provides regional coverage for India can be a prominent substitute for GPS.

### *3.1.3 Automated alarm systems*

Automated alert systems are essential for improving response times during security breaches. The Call and Notification Systems realized using GSM modules can automatically notify security personnel, local police, and bank managers through calls and SMS alerts. Moreover, the mobile Applications can provide real-time updates and enable remote control of ATM systems. The Table 2. Highlights the components comprising the ATM security system.

### **3.2 Work flow**

The work flow of the ATM security system is illustrated in the Figure 2.

### *3.2.1 Power ON*

The system is powered using a battery or main power. The Microcontroller (e.g., Arduino, Raspberry Pi, or any embedded system) boots up.

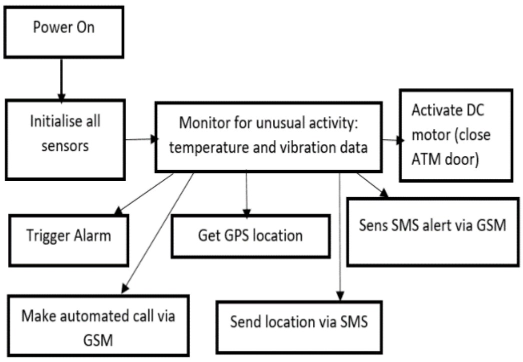


**Fig. 2.** Work flow diagram of the ATM security system.

### *3.2.2 Initialise all senosrs*

Detects any physical tampering like hammering or drilling. Temperature Sensor: detects unusual rises in temperature (e.g., due to gas cutting). The GPS Module continuously tracks the ATM location. The GSM Module enables SMS and calling functionality

### *3.2.3 Monitor for unusual activity*

The system continuously checks on the Vibration and tempetrature sensor, if tampering is detected, proceed to alert mode. And if a fire or heating tool is sensed, trigger alerts.

### *3.2.4 Any sensor triggered*

When either vibration or abnormal temperature is detected, alarm is triggered by a A buzzer or light can be activated to deter intruders. A sms alert is sent where GSM module sends an SMS to the bank authorities or security team with Message: "Intrusion detected at ATM location. Immediate action required."

### *3.2.5 Automated calls*

The GSM module initiates a voice call to a predefined emergency contact to draw urgent attention. The GPS module provides the real-time coordinates (latitude and longitude) of the ATM.and Send Location via SMS. Sends a Google Maps link with location.

### *3.2.6 Activate Dc motor*

The microcontroller signals a DC motor or solenoid to close or lock the ATM door automatically, preventing further intrusion. After taking action, the system resets or continues to monitor for additional events.

## **4 Results and discussion**

A website is created for Real time monitoring of the status of sensors as shown in the Figure 3.

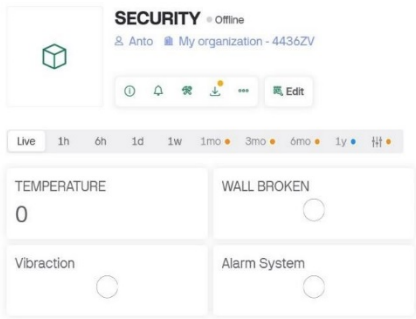


**Fig. 3.** Sample of website creation for sensor status monitoring.

The Blynk.Console web application enables users to configure connected devices, manage data, users organizations, and locations, and remotely monitor and control devices. Using ThingSpeak App, temperature and vibration sensor status is monitored as sample illustrated in the Figure 4 and Figure 5.


**Fig. 4.** Monitoring of temperature status sensor.


**Fig. 5.** Monitoring of ATM location by tracking GPS data in terms of latitude and longitude.

The circuit is simulated using Proteus simulation software as shown in the Figure 6 and tested for temperature readings as shown in the Figure 7.

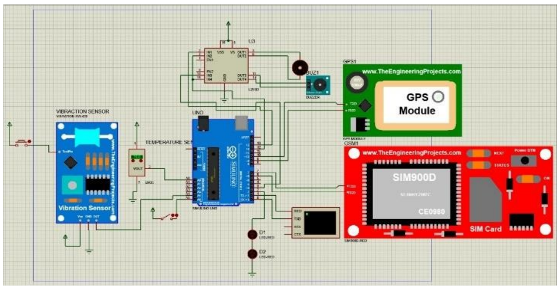


**Fig. 6.** The circuit simulation of the ATM security system.

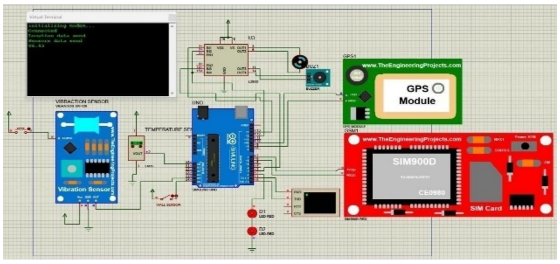


**Fig. 7.** The circuit simulation for temperature sensor triggering of the ATM security system.

## 5 Conclusion

The proposed ATM Security System, based on GSM communication, GPS tracking, and temperature and vibration sensors, is comprehensive and proactive about the growing security challenges of ATM machines. It greatly enhances the protection of ATMs from unauthorized access, physical tampering, and possible vandalism and theft threats through real-time monitoring and instant alerts. The integration of temperature and vibration sensors adds another layer of security by ensuring that any unusual activities are detected for signs of potential attacks. This is further backed by the presence of GPS tracking; hence, both the location and status of the ATM are well monitored, such that swift actions can be administered in case the ATM shows suspicious movement or tampering attempts. In general, the whole system features more reliability, efficiency, and responsiveness in the approach for ATM security while providing safety to these machines and protecting the financial information of users. With these enhanced security features, financial institutions can reduce fraud and theft risks, minimize downtime in operation, and enhance customer trust regarding the reliability and safety of banking services

## Acknowledgement

The authors and team would like to acknowledge the support and encouragement from Jain University management team and academic team in promoting research.

## References

1. K. Thopate, P. Musale, P. Dandavate, B. Jadhav, P. Cholke, S. Bhatlawande, S. Shlaskar, Smart ATM security and alert system with real-time monitoring. Int. J. Recent Innov. Trends Comput. Commun. **11**, 32-38 (2023). https://doi.org/10.17762/ijritcc.v11i7.7827
2. Martin Doe, E.G. Domanaanmwi, Y. Afriyie, A.A. Bayor, C.B. Baatuomu, J.J. Moyom, Enhanced Fingerprint-Based ATM Security Using Machine Learning Algorithms, in Proceedings of 2024 IEEE SmartBlock4Africa, IEEE, Accra, Ghana, December 12 (2024), 1-6
3. R. Raman, S. Prabhakar, T. Bernatin, IoT based anti theft controlling and security system for ATM machine, In 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), IEEE, Coimbatore, India, August 28 (2023), 1272-1277
4. D. Verma, K. Singh, A. Srivastav, V. Singh, IoT based smart framework for ATM security with electricity saver. Int. J. Comput. Sci. Eng. **10**, 12-15 (2022). https://doi.org/10.26438/ijcse/v10i7.1215
5. S. Arvind, A.K. Singh, B.S. Reddy, Enhancing ATM transaction security through face recognition. Int. J. Res. Anal. Rev. **10**, 461-467 (2023)
6. S. Ramyasri, M. Mahalakshmi, IOT Based Progressive Anti Theft ATM Security System, International Conference on Recent Advancements in Engineering and Management (ICRAEM-2020), IOP Publishing, Warangal, India, October 9-10 (2020), 042095
7. B. Sricharan, J.U. Sanjana, T.V. Vani, C.N. Sujatha, RFID Based ATM Security System Using IOT, 2022 International Conference on Intelligent Controller and Computing for Smart Power (ICICCSP), IEEE, Hyderabad, India, August 25 (2022), 1-6
8. G.C.K. Reddy, ATM security system. J. Eng. Sci. **15**, (2024)
9. S. Abhijith, K.N. Sreehari, An IOT based system for securing ATM machine, 8th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, Coimbatore, India, June 07 (2022), 1764-1768
10. G.M. Sujatha, F.A. Rahman, J.G. Dhanalaskhmi, S.K. Chandru, V. Srinivasan, ATM skimming device detection using IOT, In AIP Conference

Proceedings, AIP Publishing LLC, Chennai, India (2023), April 28-29 (2023), 030001

11. S. Dilshath, ATM fraud detection using deep learning. J. Tianjin Univ. Sci. Technol. **54**, (2021). https://doi.org/ 10.17605/osf.io/m3yth
12. K. Gavaskar, U.S. Ragupathy, S. Elango, M. Ramyadevi, S. Preethi, a novel design and implementation of IoT based real-time ATM surveillance and security system. Adv. Comput. Intell. **2**, 1 (2022). https://doi.org/10.1007/s43674-021-00007-7
13. A. Das, S. Modak, U. Biswas, Deep Learning for Intelligent Real-Time ATM Monitoring and Alert System to Enhance Security, 2025 8th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), IEEE, Kolkata, India, April 16 (2025), 1-6
14. S. Mandavilli, A. Pallayil, S. Evre, A. Mane, M. Parmar, ATM surveillance system using machine learning. Grenze Int. J. Eng. Technol. **9**, 369 (2023).
15. M. Nagabushanam, S. Jeevanandham, S. Ramalingam, K. Baskaran, A. Maheshwari, AI based E-ATM Security and Surveillance System using BLYNK-loT Server, 2022 3rd International Conference on Communication, Computing and Industry 4.0 (C2I4), IEEE, Bangalore, India, March 14 (2023), 1-5