Discover Engineering
An International Journal
OPEN ACCESS
ISSN 3117-566X
Original Research Article
Check for updates

IoT-Enabled Multi-Sensor Framework for Real Time ATM Physical Theft Detection

Akshata S Bhat*[1], Ankur Khare[1] and Praveen Kumar K[2]

[1]*Department of Computer Science and Information Technology, Rabindranath Tagore University, Raisen, M.P-464993, India*
[2]*Department of Computer Science, B S Channabasappa First Grade College, Davangere-577004, India*

Corresponding author: **Akshata S Bhat** | E-mail: **sweeksha@gmail.com**

Citation: Akshata S Bhat, Ankur Khare and Praveen Kumar K (2025). IoT-Enabled Multi-Sensor Framework for Real Time ATM Physical Theft Detection. *Discover Engineering: An International Journal.* **DOI: https://doi.org/10.51470/DE.2025.6.1.01**

Received 05 January 2025 | Revised 08 February 2025 | Accepted 10 March 2025 | Available Online 09 April 2025

Abstract

Automated Teller Machines (ATMs) are prime targets for physical theft attempts such as prying, drilling, hammering, tilting and towing. To address these threats, this paper proposes an IoT-based ATM Physical-Theft Detection System that integrates a suite of sensors, including magnetic, vibration, tilt/accelerometer. The system continuously monitors the ATM environment and classifies security events in real time based on severity levels. Magnetic sensors detect unauthorized panel displacement, vibration sensors capture drilling or hammering activities, and tilt sensors identify towing or lifting attempts when the ATM is tilted beyond 5° for over three seconds. A multi-sensor event correlation escalates alerts to critical, triggering immediate deterrent actions such as activating a siren, flashing lights, locking cash dispensers, capturing images or video, and sending encrypted alerts to a central monitoring server. Security staff are notified through SMS, email, or push notifications. This integrated approach enhances the resilience of ATMs against theft and tampering by combining real-time detection, automated deterrence, and centralized monitoring.

Keywords: *Magnetic, Vibration, Tilt Sensors, Physical.*

I. INTRODUCTION

Automated teller machines (ATMs) are a major component of the global financial system, by which they provide simple and easy access to cash and banking services. In general, the risks targeted at these machines have gone up proportionally with their use. Besides the issues that both consumers and banks are facing due to ATM crimes in the form of stealing and vandalizing, the security deployed to protect ATMs from criminals has to be more sophisticated to ensure that they continue to perform their functions safely as criminals become more complicated in their illegal activities[4]. Automated Teller Machines (ATMs) are vital to the whole banking ecosystem aside from regular bank operating hours, as they give clients access to the most basic financial services such as cash withdrawals, deposits, fund transfers, and balance inquiries. Moreover, their presence in cities, towns, as well as villages, has turned them into the most significant promoters of financial accessibility and ease of use. The flip side of the coin is that their comprehensive presence also renders them hot spots for bank robberies and thefts of different kinds. The below fig 1 shows that the Offenders use a variety of approaches starting with brute force prying, drilling, and cutting and going further to mixed techniques like tilting, towing, or trying to physically pull the ATM from its place. The attacks not only do banks lose money directly, but also there is a chain reaction with service downtime, the destruction of the infrastructure, and lack of customer trust.

Traditionally ATM security has relied on mechanical reinforcements, locks, vaults, closed-circuit video surveillance, and simple alarm systems. These methods are often seen as the lowest safety provision since they very often lack the capability for in-real-time detection and intervention. To give an example, take CCTV cameras as the most used means after the occurrence of an incident, only efficient in the cases of constant monitoring, which is not always possible. Additionally, even though strong locks and safes can provide some time for the security officers to respond, they are not capable of completely discouraging criminals who are armed with advanced tools. The latest technological advancements in IoT (Internet of Things) have significantly widened the possibilities for upgrading existing physical security systems. The term "internet of things" (IoT) refers to a network of linked devices with sophisticated capabilities that allow them to communicate with other devices, people, and the physical environment to carry out a range of functions [13]. In this regard, the incorporation of sensors into Internet of Things devices guarantees a smooth interaction between the gadgets and the real environment. In fact, a variety of sensors (such as an magnetic, vibration, tilt/accelerometer etc.) are included in contemporary IoT devices, allowing for more effective and user-friendly applications [14].

These sensors enable Internet of Things devices to detect changes in their environment and take appropriate action to enhance any ongoing task effectively [15]. IoT devices are now able to make decisions on their own due to their perception of changes in the real environment, while effective communication between the gadgets and the real world have led to the widespread use of IoT devices in a variety of applications [11]. IoT-based systems can more effectively scale, are more adaptable, and can better distinguish between a genuine threat and a minor environmental change through event classification and threshold calibration than the old-traditional ones.

The proposed ATM Anti-Theft Detection System using IOT being suggested the use of a multi-sensor method. The system implements tilt/accelerometer sensors for the detection of machine towing or lifting, vibration sensors for the detection of drilling, hammering, or cutting attempts, and magnetic sensors for the detection of the unauthorized displacement of ATM doors or panels. An ATM controller, which is linked to the sensor assembly, is always checking the inputs, classifying the seriousness of the events, and issuing the suitable responses.

Fig 1. Physical Attacks on ATM Machines

For instance, a tilt or door displacement occurrence could be elevated to medium priority with the audible alert, while a small vibration might only lead to the event's being recorded and a low-priority warning being issued. The most significant response is offered in the case of a critical event, which refers to a combination of tilt and vibration or displacement and vibration. The system goes on to perform various countermeasures when a critical warning is delivered. A siren and flashing lights, thus, are turned on locally to both deter the attacker and make the ATM area illuminated and hence, easily spotable by anyone approaching the place. At the same time, the mechanisms of the safe and cash dispenser are locked in order to prevent unauthorized access. On the communication end, a cellular or Ethernet connection is utilized to transmit encrypted alert messages to a central monitoring server. The server, if programmed, automatically escalates the alert and notifies via push notifications, email, or SMS. By significantly reducing the response time, this integrated workflow, is essentially, the killer of the thieves' chances. What essentially makes this method a novel automated response system and multi-sensor event fusion. The system determines the severity levels by looking at the data from several sensors rather than relying on a single tampering indicator only. This, in turn, reduces the number of false positives, at the same time assuring that, on the contrary, real threats are escalated. Besides protecting the physical assets, the multi-layered reaction also raises the ATM network's resistance to the continuous change of the attackers' modus operandi.

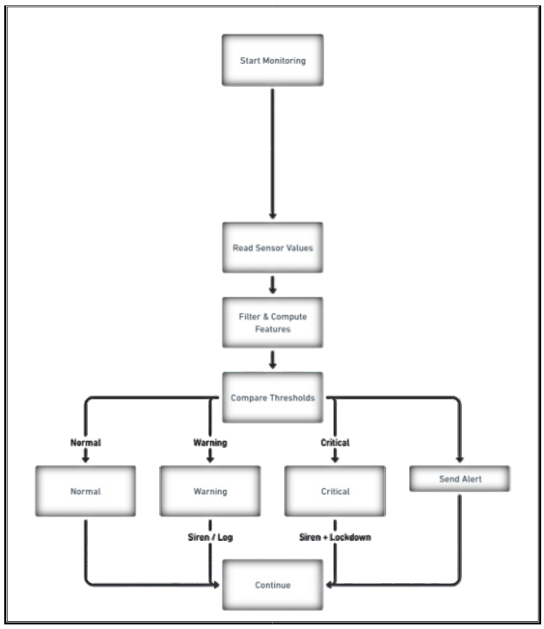

Fig 2. ATM Security Monitoring Flowchart

This flowchart fig 2. Shows that, depicts the monitoring process of an ATM security system. It begins with the system starting to monitor sensor values. These sensor readings are then filtered and computed to extract features. The system compares these features against predefined threshold values to determine the status. Based on the comparison, the system classifies the status into Normal, Warning, or Critical. If Normal, the system continues monitoring without action. If Warning, a siren or log is activated as a precaution. If Critical, both siren and lockdown actions are initiated to mitigate potential security breaches. An alert is sent accordingly, and the system continues its monitoring cycle to ensure ongoing protection.

This proposed system delivers a complete solution for the prevention and the detection of a robbery in real time by combining IoT-enabled monitoring and response devices with door, tilt, vibration, and magnetic sensors. The introduction serves as the conceptual basis for exploring the system design, functionalities, and the potential of the system to enhance ATM security.

II. LITERATURESURVEY

Degadwala, N. D. S et al,. The authors evaluates, ATM security and important concern because of the growing number of thefts and physical attacks. Many existing detection systems struggle with problems such as poor accuracy, delayed response, and false alarms. Recent research shows that machine learning (ML) and deep learning (DL) methods, especially object detection models like YOLO, can greatly improve movement and tampering detection in ATMs. These approaches offer faster and more reliable identification of suspicious activities compared to traditional methods. However, each system also has its strengths and weaknesses, such as differences in detection speed, hardware requirements, and adaptability to new attack methods. Overall, the use of advanced ML and DL techniques appears to be a promising direction for

making ATM security more accurate, real-time, and effective in the future.

M, J. K., Raman et al,. The authors presented an IoT based system using Raspberry Pi and sensors to detect ATM thefts, TMs are widely used by people for quick and secure cash withdrawals with the help of unique cards and PIN codes. However, they are also frequent targets of theft and vandalism, making crime prevention systems highly important. One proposed solution uses an embedded system with a Raspberry Pi to process real-time data collected from vibration sensors. In this system, robberies are detected when unusual vibrations or sounds are identified. Once detected, the sensor sends information to the bank's monitoring system and directly to a police station through the Internet of Things (IoT). At the same time, the ATM doors are locked automatically to prevent the thief from escaping. The IoTenabled system transmits data through a Wi-Fi module and displays alerts in real time on a cloud server for bank staff to monitor. Additionally, the system integrates cameras to capture images or video evidence, which helps in identifying suspects during theft attempts.

Thopate, K., Musale, P et al,. The authors presented an IoT-based ATM security system utilizing the IoT-based ATM security system built using the NodeMCU ESP8266 module, PIR sensor, LCD display, and the Telegram app. In this system, the NodeMCU acts as the main controller and communicates through Wi-Fi, while the PIR sensor detects human presence or suspicious motion near the ATM. The LCD display provides live updates such as “Motion Detected” or “No Motion,” helping staff monitor the ATM's status. Whenever unusual activity is sensed, the NodeMCU instantly sends a notification through Telegram to the ATM owner or security team, enabling them to take quick action. This real-time alert mechanism helps prevent unauthorized access and improves the overall safety of ATM operations.

Bolla, A The author proposed IoT-based ATM security systems that use microcontrollers and smart sensors to detect and prevent theft. In one such system, an Arduino Uno is used as the main controller to integrate different components. A MEMS sensor is placed on the ATM door to detect tilting, which may indicate forced access. When tampering is detected, a servo motor releases deterrent gases, while a buzzer sounds to alert people nearby. At the same time, an SMS notification is sent to security personnel or authorities for quick response. To strengthen surveillance, an IP camera provides real-time video streaming of the ATM area, allowing remote monitoring of threats. An LCD display gives live updates on the system's status, ensuring easy tracking of activities. This combination of sensors, alarms, and IoT communication offers a more active and responsive approach to preventing ATM theft and improving overall security.

In this paper Hossain, M. N et al,. authors presented an IoT-based systems using microcontrollers such as Raspberry Pi, NodeMCU, and Arduino have been developed to integrate sensors like vibration, PIR, and tilt sensors for detecting suspicious activities. Some studies focused on vibration sensors to identify physical attacks, while others used PIR sensors to detect human presence near the ATM and send real-time alerts via mobile applications such as Telegram. Advanced systems also introduced MEMS tilt sensors and cameras for monitoring unauthorized access and providing live video evidence. In addition, machine learning and deep learning techniques, particularly YOLO-based models, have been explored for anomaly detection and real-time monitoring. These methods highlight the progress made in ATM security, but also reveal challenges such as false alarms, high costs, and privacy concerns, which motivate the need for more efficient and reliable solutions.

Srilatha, M et al,.authors studies have proposed multilayered IoT-based security frameworks for ATMs that combine both transaction security and physical theft detection. One such system integrates an RFID-based smart card for user authentication, which, upon verification, triggers face capture for the bank's record-keeping and further monitoring. Transaction details are transmitted to the respective bank branch using IoT platforms such as the Blynk application, while GSM modules deliver real-time balance and transaction alerts to the user's mobile device. In terms of anti-theft measures, a vibration sensor attached to the ATM detects tampering or break-in attempts, activating an automatic door lock, buzzer alarm, and immediate notification to the bank's monitoring system. Complementary components such as USB cameras, IR sensors, DC motors, and LCD displays are controlled through a Raspberry Pi board, with all activities synchronized via Wi-Fi connectivity. By integrating transaction security, user feedback, and theft detection within a single architecture, this approach demonstrates a comprehensive solution to modern ATM challenges, ensuring both operational efficiency and enhanced safety.

M. M. E. Raj et al,. the authors presented the ATM security focuses on protecting machines from both physical and electronic theft through multiple protective measures such as anti-skimming devices, silent alarm systems, video surveillance, and monitoring solutions. A promising approach to enhance this is the use of Machine-to-Machine (M2M) communication, which supports real-time monitoring and control without human involvement, ensuring higher efficiency and wider coverage. To achieve this, the proposed work suggests implementing a low-cost Embedded Web Server (EWS) using an ARM11 processor and Linux-based Raspberry Pi. This setup provides a reliable, resourceefficient networking solution capable of serving web pages directly to browsers, making it suitable for ATM monitoring and other internet-enabled security applications.

Reddy, V. S et al,. the authors has proposed a focused on intelligent systems that combine multiple technologies to prevent ATM robberies and detect physical tampering. Wireless Sensor Networks (WSNs) are employed to monitor ATMs in real time and report suspicious activities to local authorities. USB cameras capture images or videos of users for verification and evidence, while tilt and vibration sensors detect abnormal behavior such as prying, drilling, or attempts to move the ATM.

By integrating these sensors, the system can quickly identify potential threats, enabling rapid response and reducing the likelihood of successful thefts.

Ajay, B et al,. the authors present an advanced IoT-based security system designed for Automated Teller Machines (ATMs) with a primary focus on theft prevention. The system uses an Arduino Uno microcontroller to seamlessly integrate various devices. A MEMS tilt sensor placed on the ATM door detects unusual tilting, signaling potential unauthorized access. Upon detection, the system immediately activates deterrent mechanisms such as a loud buzzer and flashing LED lights to alert nearby individuals, while simultaneously sending SMS notifications to predefined contacts and security personnel. To enhance surveillance, an IP camera provides real-time streaming of the ATM surroundings, allowing remote monitoring and assessment of potential threats. An LCD display offers an intuitive interface with real-time status updates and feedback on the system's functionality. By combining real-time monitoring, automated deterrents, and instant notifications, this IoT-based ATM security system provides a comprehensive and safe solution to deter theft, monitor suspicious activity, and ensure the security and integrity of ATM operations.

V. Ammisetty et al,. the authors presents the design and implementation of a Theft Detection System (TDS) to enhance the security and safety of Automated Teller Machines (ATMs), particularly in India where the number of ATM centers is rapidly increasing. In real-time scenarios, monitoring all activities at ATMs is practically challenging, and despite the presence of CCTV cameras, many ATM robberies still occur. The rising incidence of ATM-related scams poses a serious concern, highlighting the need for effective security solutions. The proposed system creates a secure environment that detects theft attempts and unauthorized access. When a break-in or suspicious activity is detected, the system automatically sends alerts through GSM connectivity to both the bank administrator and local police without notifying the thief. Additionally, the system leverages IoT technology to transmit alarms or video notifications via social media platforms such as Facebook, Twitter, or Gmail, and streams live CCTV footage to remote monitoring stations. By integrating real-time alerts, remote monitoring, and automated notification mechanisms, the proposed ATM theft detection model addresses the limitations of existing techniques and provides a highly secure and reliable solution for preventing ATM robberies.

III. PROPOSED SYSTEM

The working of the ATM physical-theft system relies on the integration of multiple sensors—magnetic, vibration, tilt/accelerometer sensors—each playing a critical role in identifying suspicious activities. These sensors are precalibrated and strategically installed on or inside the ATM to ensure maximum coverage. The ATM controller continuously monitors signals from these sensors and uses intelligent logic to distinguish between normal events such as maintenance or ambient vibrations and potentially dangerous activities such as prying, drilling, or towing.

A. Magnetic Sensor

A magnetic sensor is an electronic device that detects changes or disturbances in a magnetic field and converts this information into a measurable electrical signal. It works on the principle of magnetoresistance, Hall effect, or reed switch mechanisms depending on the design. These sensors are widely used for position detection, proximity sensing, and motion tracking because of their high sensitivity and reliability. In the context of ATM security, a magnetic sensor is typically installed on doors, panels, or critical locking points. It continuously measures the alignment of the metallic structures and detects any displacement, separation, or tampering. Even slight changes, such as prying open a panel or forcing a door, cause measurable variations in the magnetic field, which the sensor immediately registers. The noncontact nature of magnetic sensors makes them durable, tamper-resistant, and suitable for 24/7 monitoring. By acting as the first line of defense, magnetic sensors help identify unauthorized access attempts and feed real-time data to the ATM controller, ensuring rapid classification of events and triggering appropriate security responses.

B. Vibration Sensor

A vibration sensor is a device that detects mechanical oscillations, shocks, or movements from the surrounding environment and converts them into electrical signals. These sensors are typically based on piezoelectric materials, accelerometers, or micro-electromechanical systems (MEMS) that respond to changes in acceleration and pressure. Vibration sensors are widely used in industrial equipment monitoring, structural health assessment, and security systems, where abnormal vibration patterns may indicate malfunction or tampering.

In ATM security applications, the vibration sensor plays a vital role in identifying unauthorized mechanical impacts such as drilling, hammering, or cutting. By continuously monitoring vibration intensity and duration, the sensor helps differentiate between minor environmental disturbances and deliberate attempts to damage or access the ATM.

The vibration sensor operates by sensing variations in acceleration or pressure caused by mechanical forces acting on the ATM body. Under normal conditions, background vibrations are minimal, typically in the range of 0.02 g, and are classified as safe. When minor disturbances occur, such as a truck passing nearby, the vibration levels increase slightly (0.1–0.4 g) but are short-lived, allowing the system to log them as low-severity events without raising alarms. However, when tools like drills, hammers, or cutters are used against the ATM, the sensor detects sudden spikes in vibration, often exceeding 1.5 g for durations longer than three seconds. Such sustained abnormal activity is interpreted as a tampering attempt. Once this threshold is crossed, the ATM controller triggers immediate countermeasures such as activating a siren, logging the event, and notifying the operations staff.

C. Tilt Sensor

A tilt sensor, also referred to as an inclinometer or tilt switch, is a device used to measure the angular position or deviation of an object relative to the ground. It works by detecting changes in orientation and inclination, often using accelerometer or MEMS (Micro-Electro-Mechanical Systems) technology. Tilt sensors are widely applied in industrial safety systems, robotics, structural monitoring, and security applications where even small changes in angle can indicate abnormal activity. In the context of ATM security, tilt sensors play a critical role in detecting theft attempts where the machine is physically tilted, lifted, or towed away.

The tilt sensor operates by measuring angular displacement with respect to gravity. In most ATM anti-theft systems, MEMS-based accelerometers are used, which sense acceleration along multiple axes and calculate the tilt angle. Under normal conditions, the ATM remains almost upright, with tilt values less than 1°, which are considered stable. Small environmental movements, such as ground vibration or minor shifts, may cause negligible variations (under 2°) and are logged as harmless events. However, if the ATM is tilted beyond 5° and the condition persists for more than three seconds, the system interprets it as a potential towing or lifting attempt. When the angle exceeds 12° or shows sustained displacement, it strongly indicates that the ATM is being forcibly removed from its base. At this stage, the controller classifies the event as critical, triggering immediate countermeasures such as activating a siren, locking down the cash dispenser, sending encrypted alerts to the monitoring server.

In this way, the multi-sensor fusion approach enables the ATM physical-theft system to operate intelligently. Lowseverity events like minor vibrations are logged without triggering unnecessary alarms, while medium and highseverity incidents such as prying or drilling activate sirens and notify operators. Critical events, including towing or combined attacks, initiate full lockdown, continuous alarms, and immediate escalation to law enforcement. This layered, sensor-driven mechanism ensures real-time detection and response against a wide range of ATM theft and tampering attempts.

VI. METHODOLOGY

The proposed ATM Anti-Theft Detection System integrates multiple sensors to monitor any suspicious physical activities around the ATM. The sensors continuously collect real-time data such as vibration intensity, magnetic field changes, and tilt angles. The microcontroller processes this data to identify potential theft attempts like prying, drilling, hammering, or towing. Based on the detected event, the system triggers alarms and sends alerts to the control center.

A. Sensor Deployment

- Install the sensors on the ATM machine:
- Magnetic Sensor: detects any unauthorized door or panel displacement by monitoring magnetic field variations.
- Vibration Sensor: identifies drilling, cutting, or hammering by sensing unusual mechanical vibrations.
- Tilt Sensor (Accelerometer): detects abnormal changes in ATM orientation caused by lifting or towing attempts.
- Each sensor continuously sends signals to a microcontroller

B. Signal Acquisition and Preprocessing

The sensor readings are continuously collected at fixed time intervals. The raw sensor data is preprocessed by removing noise and applying filters such as a moving average filter for vibration signals and threshold normalization for tilt angles. The preprocessed data ensures that only meaningful fluctuations are analyzed for anomaly detection. Using mathematical formula for raw sensor data is read at a fixed sampling rate:

$$x_f(t) = x(t) * h(t) \quad (1)$$

Where,
$x(t)$: Raw sensor data $h(t)$: Low-pass filter kernel
$x_f(t)$: Filtered data

The equation(1) ensures only meaningful vibration or tilt events are captured.

C.Feature Extraction

Compute key parameters from each sensor, below equations used for calculate the event features:

Magnetic displacement:

$$\Delta M = |M_t - M_{ref} \quad (2)$$

Where,
M_t=current reading
M_{ref}=baseline magnetic field.

Vibration intensity (RMS value):

$$V_{RMS} = \sqrt{\frac{1}{N}\sum_{i=1}^{N} v_i^2} \quad (3)$$

The equation(3) indicates vibration strength.

Tilt angle (from accelerometer):

$$\theta = \tan^{-1}\left(\sqrt{\frac{a_x^2 + a_y^2}{a_z}}\right) \quad (4)$$

Where $a_{x,y}$,a_z are accelerations along each axis.

D. Threshold-based Event Classification

Each sensor has a predefined threshold value representing normal operating conditions. When the sensor output exceeds this threshold, it indicates a potential anomaly. Below table 1, shows that, each feature is compared to a predefined threshold values.

Table 1. ATM Security Sensors: Parameters, Alert Conditions, and Actions

Sensor Type	Parameter (threshold)	Condition	Action
Magnetic	$\Delta M > M_{th}$	Panel movement	Medium Alert
Vibration	$VRMS > Vth$	Drilling/Hammering	High Alert
Tilt	$\theta > \theta_{th}$	ATM Tilt/Towing	Critical Alert

E. Decision Model

The system applies a simple weighted scoring model:

$$S = w1.\ M\_\_\_\Delta Mth + w2.\ VVRMSth + w3.\ \theta\_\_\_t\theta h \quad (5)$$

- If $S \geq 1$, a theft alert is triggered.
- Where w_1, w_2, $w_3$are sensor importance weights (e.g., 0.3, 0.4, 0.3).

F. Alert and Response

If a threshold or score is exceeded:

- Local siren and alarm activate.
- Network message sent to central server.
- ATM locks down (cash dispenser disabled).
- Event is logged for analysis.

V. RESULT

To assess the effectiveness of the suggested ATM physical theft and tampering detection system, the different operational and attack scenarios were examined. Each of the scenarios provided a real-world simulation and was capable of detection theft attempts to include drilling, prying and towing. The system was able to assess the level of severity to be (NONE, LOW, MEDIUM, HIGH, CRITICAL) based on a pre-defined set of thresholds which determined the level of suspicious activities consisting a unique combination of magnetic displacement, vibration, and tilt/accelerometer.

Normal Idle State: During the idle state, the magnetic displacement was at Δ=0 mm, the vibration sensors picked background noise of 0.02 g, and the tilt angles remained small (roll = 0.4°, pitch = 0.2°) showing the door was closed. No alerts were generated, and the system sent regular messages to indicate normal functioning.

Authorized Maintenance: Authorized maintenance inspections encountered alerts from the magnetic sensor, as 1 to 3 mm displacements were noted, with an additional slight increase in the vibration levels between 0.05 and 0.1 g. The angles of the offsets were less than 2°, and the door was open during the inspections as confirmed by the door contact sensor. The maintenance inspectors logged the actions, which prompted the system to classify the events as low severity with no sirens or alarms activation.

Drilling/Hammering Attempts: The system was able to pick up simulated activity which consisted of drilling or hammering. The system recorded the prolonged periods of sustained vibrations which were greater than 1.5 g for over 3 seconds at a time and were accompanied by lower than 3° of tilt and magnetic displacements of 2 mm. The system was prompted to send an emergency notification to the operational team as the local sirens were activated.

Prying or Panel Displacement: There was a considerable amount of panel movement and magnetic sensor measurements were 4 to 25 mm with brief spurts of vibration 0.3 to 0.8 g. The door contact sensor was used to confirm unauthorized door openings, and the tilt measured below 5 degrees. The system responded by deploying a high severity alarm with sirens, locking the cash dispenser system and alerting the operational security personnel as well as the law enforcement agencies.

Tilt/Towing Attempts: Constant tilt angles above 5 degrees in excess of three seconds which increased to 12 degrees during towing simulations were observed with varying intensities of vibration (0.2 to 1 g) and low levels of magnetic movement. During these events the door was kept closed. Those readings were also registered as critical threats and led to constant siren activation, automatic lockdown of the cash dispenser, encrypted notification to the central monitoring server, and automatic notification to police authorities or operational team.

The below table2, shows that, all the cases with corresponding sensor activities and system responses:

Table 2. Sensor Thresholds and Corresponding ATM Security Responses

Case	Magnetic Displacement (mm)	Vibration (g)	Tilt Angle (°)	Door Contact	Severity Level	System Actions
Normal (Idle)	0	0.02 (background noise)	Roll: 0.4, Pitch: 0.2	Closed	None	Message only
Authorized Maintenance	1–3	0.05–0.1	< 2	Open (valid token)	Low	Log maintenance, no siren
Minor Ambient Vibration	0	0.1–0.4 (brief < 2s)	< 1	Closed	Low	Log only, no siren
Drilling / Hammering Attempt	0–2	> 1.5 (sustained > 3s)	< 3	Closed	High	Activate siren, log, notify operations
Prying / Panel Displacement	4–25	0.3–0.8 (short bursts)	< 5	Open (unauthorized)	High	Siren on, lock cash dispenser, notify operations team or police
Tilt / Towing Attempt	0–2	0.2–1 (variable)	> 5 for > 3s, > 12 towing	Closed	Critical	Continuous siren, lock dispenser, critical alert

A. Graph and Analysis

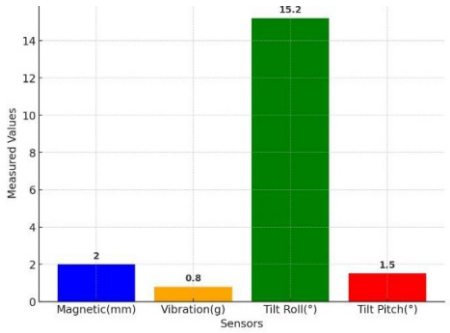

Fig 3. ATM Anti-Theft Sensor Analysis During Tilt Towing Detection

The graph fig 3, illustrates the sensor readings recorded during a Tilt Towing Detected event in the ATM Anti-Theft Detection System. It shows four key sensor parameters— Magnetic displacement, Vibration intensity, Tilt Roll, and Tilt Pitch. Among these, the Tilt Roll value is significantly higher at 15.2°, indicating that the ATM was physically tilted or moved, which confirms a towing attempt. The Magnetic sensor shows a small displacement of 2 mm, while the Vibration sensor recorded a mild impact of 0.8 g, suggesting some mechanical disturbance. The Tilt Pitch value of 1.5° further supports the evidence of movement.

Overall, the sensor data clearly indicates abnormal physical activity consistent with a theft attempt, triggering the system's critical alert actions such as activating the siren, locking the cash dispenser, and notifying the police.

VI. CONCLUSION

In conclusion, the current work is a successful effective of an ATM physical-theft and tampering detection device based on the implementation of Magnetic sensors, vibration and tilt sensors. This is because the multi-sensor combination and severity categorization allows the correct identification of various threat conditions and reduction of false alarms. A real-time response of the system such as siren activation, lockdown of the dispenser and alerts to the monitoring centers provide deterrence and quick response. Such a practice improves the security of the ATM by far as compared with the traditional systems by boosting the reliability of the detection and efficiency of its operation.

REFERENCES

1. Degadwala, N. D. S., &Bharatbhai, N. P. T. (2024). Advancements in ATM Security for Movement and Tampering Detection: A review. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 10(5), 79–89. https://doi.org/10.32628/cseit2410587.
2. Bolla, A. (2024). IoT-Enabled Automated Teller Machine (ATM) Theft Detection and Automatic Apprehension System. Indian Scientific Journal Of Research In Engineering And Management. https://doi.org/10.55041/ijsrem29616.
3. Ajay, B. (2024). IoT-Enabled Automated Teller Machine (ATM) Theft Detection and Automatic Apprehension System. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. https://doi.org/10.55041/ijsrem29616.
4. Degadwala, N. D. S., &Bharatbhai, N. P. T. (2024b). Advancements in ATM Security for Movement and Tampering Detection: A review. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 10(5), 79–89. https://doi.org/10.32628/cseit2410587.
5. M, J. K., Raman, R., Prabhakar, S., &Bernatin, T. (2023). IoT based Anti Theft Controlling and Security System for ATM Machine. 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), 1272–1277. https://doi.org/10.1109/icirca57980.2023.10220945.
6. Thopate, K., Musale, P., Dandavate, P., Jadhav, B., Cholke, P., Bhatlawande, S., &Shlaskar, S. (2023). Smart ATM Security and Alert System with Real-Time Monitoring. International Journal on Recent and Innovation Trends in Computing and Communication, 11(7), 32– 38. https://doi.org/10.17762/ijritcc.v11i7.7827.
7. V. Ammisetty, "Novel Based Hybrid Security Model For Bank Atm Theft Detector Using Internet Of Things," Mar. 2023, vol. 7, pp. 1–5. doi: 10.1109/aisp57993.2023.10134783.
8. Hossain, M. N., Sayeed, M. S., & Zaman, S. F. U. (2022). Utilizing the internet of things, monitoring and protecting system for automated teller machines. ASIAN JOURNAL OF CONVERGENCE IN TECHNOLOGY, 8(3). https://doi.org/10.33130/ajct.2022v08i03.004.
9. Srilatha, M., Meghamsh, G. S., Emmanuel, J. J., & Manohar, S. (2021). Safety and maintenance of ATM system using Internet of things. AIP Conference Proceedings, 2407, 020025. https://doi.org/10.1063/5.0074362.
10. Reddy, V. S., Kalli, S., Gebregziabher, H., & Babu, B. R. (2021). Smart door lock to avoid robberies in ATM. Journal of Physics Conference Series, 1964(4), 042032. https://doi.org/10.1088/17426596/1964/4/042032.
11. Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., &Uluagac, A. S. (2018). A survey on sensor-based threats to Internet-of-Things (IoT) devices and applications. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1802.02041.
12. M. M. E. Raj and A. Julian, "Design and implementation of anti-theft ATM machine using embedded systems," Mar. 2015, pp. 1–5. doi: 10.1109/iccpct.2015.7159316.
13. N. Bari, G. Mani, and S. Berkovich, "Internet of things as a methodological concept," in Fourth International Conference on Computing for Geospatial Research and Application (COM. Geo), 2013. IEEE, pp. 48–55.
14. N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," IEEE Communications magazine, vol. 48, no. 9, 2010.
15. Y. Yu, J. Wang, and G. Zhou, "The exploration in the education of professionals in applied internet of things engineering," in 4th International Conference on Distance Learning and Education (ICDLE), 2010. IEEE, pp. 74–77.