

AI Based Secure ATM Access and Intrusion Response System

Harsh Kakad¹, Tanmay Margale², Akash Rathod³, Prof. V. B. Baru⁴

¹ Department Of Electronic & Telecommunication, Sinhgad College of Engineering, Pune- 41

² Department Of Electronic & Telecommunication, Sinhgad College of Engineering, Pune- 41

³ Department Of Electronic & Telecommunication, Sinhgad College of Engineering, Pune- 41

Email:kakadharsh@gmail.com

Abstract - Increasing incidents of ATM tampering and unauthorized access require smart automated defenses. This project presents an AI Based Secure ATM Access and Intrusion Response System built around a Raspberry Pi 4B. The system integrates an IR sensor and vibration sensor for early detection, a USB camera for AI-powered visual analysis, a SIM800C GSM module for immediate alerts, a solenoid lock for automatic enclosure control, and a relay-driven current-transferring coil as an active deterrent. On detecting suspicious activity the system locks the enclosure, energizes the coil, sounds an alarm, captures evidence and sends SMS alerts to predefined numbers. The architecture aims to provide real-time, low-latency autonomous protection suitable for both standalone ATMs and integration into existing bank security infrastructure.

Key Words : ATM Security, Artificial Intelligence, Computer Vision, Edge Computing, Intrusion Detection, Raspberry Pi, Multi-Sensor Fusion, GSM Alert System, Smart Surveillance, Physical Security.

1. INTRODUCTION

Automated Teller Machines (ATMs) play a vital role in modern banking by providing customers with convenient access to financial services. However, the increasing number of ATM-related crimes, including unauthorized access, physical tampering, theft, and vandalism, has raised significant security concerns for financial institutions. Traditional ATM security systems primarily depend on CCTV surveillance and alarm mechanisms, which often function as passive monitoring tools and provide limited capability for real-time threat detection and prevention. The lack of intelligent monitoring and immediate response mechanisms can result in delayed intervention, financial losses, and compromised customer safety.

To address these challenges, this research proposes an AI-based Secure ATM Access and Intelligent Intrusion Response System that integrates computer vision, edge computing, and multi-sensor fusion technologies. The system utilizes a Raspberry Pi-based platform combined with cameras, infrared sensors, vibration sensors, GSM communication, and automated locking mechanisms to continuously monitor ATM environments and identify suspicious activities in real time. Upon detecting an intrusion attempt, the system automatically initiates security actions such as alarm activation, evidence capture, access restriction, and instant alert notifications to authorized personnel. By enabling proactive threat detection and autonomous response, the proposed framework enhances ATM security, reduces response time, and provides a cost-effective solution for modern banking infrastructure.

2. LITERATURE SURVEY

[1] This paper, “*ATM Security System Using GSM Technology*” (International Journal of Engineering Research, 2019), proposes a GSM-based security framework that sends SMS alerts to authorized personnel whenever unauthorized access or suspicious activity is detected at an ATM. The system improves emergency communication and enables remote monitoring of security events. However, the proposed approach relies solely on sensor-triggered notifications and lacks intelligent threat analysis, visual monitoring, and automated response mechanisms, limiting its effectiveness in preventing ATM-related crimes.

[2] This paper, “*Smart Surveillance System Using Computer Vision and Raspberry Pi*” (IEEE Conference on Smart Systems, 2020), presents a real-time surveillance system that utilizes OpenCV and Raspberry Pi to monitor secured environments. The system detects human presence and suspicious movements through image processing techniques. While the solution reduces the need for continuous human supervision, its performance depends heavily on camera visibility and lighting conditions. Furthermore, the system does not integrate additional sensors for improving detection accuracy or reducing false alarms.

[3] This paper, “*IoT-Based Intrusion Detection and Security Monitoring System*” (International Journal of Advanced Computer Science and Applications, 2021), introduces an IoT-enabled security framework that integrates motion sensors, embedded controllers, and wireless communication modules for intrusion detection. The system provides real-time alerts and remote monitoring capabilities. Although it enhances security awareness, the proposed solution lacks artificial intelligence-based decision-making and cannot differentiate between normal and suspicious activities effectively.

[4] This paper, “*Edge Computing for Real-Time Security Applications*” (IEEE Internet of Things Journal, 2021), investigates the use of edge computing devices for low-latency surveillance and security monitoring. By processing data locally, the system reduces cloud dependency and improves response time. The study demonstrates the effectiveness of

[5] Raspberry Pi-based architectures in security applications. However, the research focuses primarily on data processing efficiency and does not include automated threat mitigation mechanisms or multi-sensor integration.

3. OVERVIEW

The increasing incidence of ATM-related crimes, including unauthorized access, physical tampering, and theft, has highlighted the need for advanced security solutions in banking infrastructure. Conventional security systems primarily depend on CCTV surveillance and alarm systems, which often provide reactive rather than proactive protection. To address these limitations, the proposed AI-Based Secure ATM Access and Intelligent Intrusion Response System integrates Artificial Intelligence (AI), Computer Vision, Edge Computing, and IoT technologies to enable real-time threat detection and automated security responses. The system is designed to enhance ATM security by continuously monitoring activities and taking immediate action when suspicious behavior or intrusion attempts are detected.

1. Objective:

The primary objective of the Open Source GitHub Repository Finder (OSGRF) is to develop a seamless and intelligent recommendation system that connects developers with open-source repositories matching their genuine skills and interests. Through the automation of skill extraction, repository discovery, and AI-driven contribution guidance, the system aims to minimize the challenges faced by newcomers when initiating open-source contributions. Ultimately, OSGRF encourages skill-oriented community growth and fosters a more inclusive and efficient open-source collaboration environment.

2. Core Components:

The proposed system consists of the following major hardware and software components:

- **Raspberry Pi 4B:** Central processing unit responsible for sensor management and AI processing.
- **USB Camera Module:** Captures real-time video streams for visual monitoring and analysis.
- **Infrared (IR) Sensor:** Detects human presence and

movement near the ATM.

- **Vibration Sensor:** Identifies physical tampering and forced-entry attempts.
- **GSM Module (SIM800L):** Sends emergency SMS notifications to security personnel.
- **Solenoid Lock:** Restricts unauthorized access by automatically locking the ATM enclosure.
- **Alarm/Buzzer System:** Generates audible alerts during security breaches.
- **OpenCV and AI Algorithms:** Perform image processing, motion detection, and threat analysis.

3. Working Principle:

The system operates through a multi-layer security approach. Initially, the IR sensor detects the presence of a person near the ATM. Simultaneously, the camera captures live video data, which is processed using computer vision algorithms to identify suspicious activities. The vibration sensor continuously monitors physical disturbances and tampering attempts. Sensor data and visual analysis results are combined through a decision-making process to determine whether a threat exists. When an intrusion or abnormal activity is detected, the system automatically activates the alarm, engages the solenoid lock, captures evidence, and sends SMS alerts to authorized personnel. This autonomous response mechanism ensures rapid action and enhances overall ATM security.

4. Accessibility and Innovation:

The proposed system is designed to be cost-effective, scalable, and easy to deploy in existing ATM infrastructures. By utilizing Raspberry Pi-based edge computing, the system performs real-time processing without requiring continuous cloud connectivity, thereby reducing operational costs and latency. The integration of computer vision, multi-sensor fusion, GSM communication, and automated response mechanisms within a single framework represents a significant innovation over traditional ATM security solutions. This combination improves detection accuracy while minimizing false alarms and response delays.

5. Social Impact:

The implementation of the proposed security framework can

significantly enhance the safety of banking infrastructure and public financial services. By reducing ATM-related crimes and improving response efficiency, the system helps protect customer assets, banking resources, and public trust in financial institutions. Additionally, the low-cost and scalable architecture enables deployment in urban as well as rural areas, contributing to safer and more secure banking environments. The project demonstrates how AI and IoT technologies can be effectively utilized to address real-world security challenges and support the development of intelligent public safety systems.

4. METHODOLOGY

The proposed AI-Based Secure ATM Access and Intelligent Intrusion Response System employs an edge-computing architecture that integrates computer vision, sensor fusion, and automated security mechanisms to provide real-time protection for Automated Teller Machines (ATMs). The system is centered on a Raspberry Pi 4B, which functions as the primary processing unit responsible for acquiring, analyzing, and responding to security-related events. Multiple hardware components, including an infrared (IR) sensor, vibration sensor, camera module, GSM communication module, solenoid lock, and alarm system, are interconnected to create a multi-layered security framework capable of detecting unauthorized activities and responding autonomously.

The operational workflow begins with continuous monitoring of the ATM environment using the IR sensor and camera module. The IR sensor detects the presence of an individual entering the ATM cabin and activates the surveillance process. Simultaneously, the camera captures real-time video streams, which are processed using computer vision techniques implemented through OpenCV and lightweight artificial intelligence models. The captured frames are analyzed to identify human presence, suspicious movements, unauthorized access attempts, and other abnormal activities. By performing image processing and pattern recognition at the edge device itself, the system minimizes latency and ensures rapid decision-making without relying on cloud-based infrastructure.

To enhance detection reliability, the proposed framework incorporates multi-sensor fusion by combining visual information with data obtained from the vibration sensor. The vibration sensor continuously monitors physical disturbances such as drilling, forced entry, machine tampering, or vandalism attempts. The sensor readings are correlated with camera-based observations to distinguish genuine security threats from normal operational activities, thereby reducing the probability of false alarms. This integrated analysis enables the system to classify events into normal, suspicious, or critical threat categories.

Once a potential intrusion or unauthorized activity is detected, the decision-making module initiates an automated response sequence. Depending on the severity of the detected threat, the system activates a solenoid lock mechanism to restrict access, triggers an audible alarm to alert nearby personnel, and captures visual evidence for further investigation. Simultaneously, the GSM communication module sends real-time alert messages containing incident information to authorized security personnel and law enforcement authorities. This immediate notification mechanism significantly reduces response time and enhances situational awareness during security incidents.

In addition to threat detection and response, the system maintains event logs and stores captured evidence for post-incident analysis. The use of edge computing ensures efficient resource utilization, low operational costs, enhanced privacy, and uninterrupted operation even in environments with limited internet connectivity. By integrating artificial intelligence, sensor fusion, and automated security controls into a unified framework, the proposed methodology provides a proactive and scalable solution for improving ATM security and mitigating risks associated with unauthorized access and physical attacks.

5. SYSTEM ARCHITECTURE

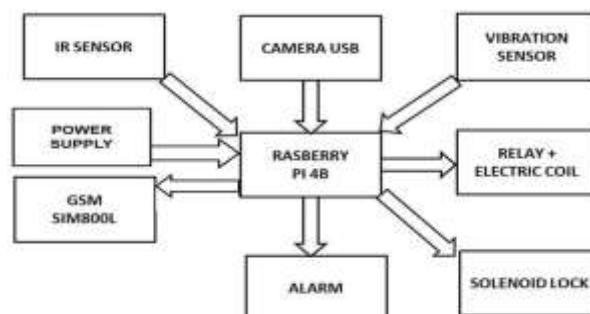


Fig: System Architecture Diagram

The OSGRF The proposed AI-Based Secure ATM Access and Intelligent Intrusion Response System is designed using a multi-layered architecture that integrates sensing, processing, communication, and response modules to provide comprehensive ATM security. The architecture consists of five major layers: the Input Layer, Processing Layer, Decision Layer, Response Layer, and Communication Layer. These layers work collaboratively to detect suspicious activities, analyze threats, and initiate automated security responses in real time.

At the Input Layer, multiple sensors continuously monitor the ATM environment. An Infrared (IR) sensor is deployed to detect the presence of individuals entering the ATM cabin, while a vibration sensor monitors abnormal physical disturbances such as drilling, forced entry, machine tampering, or vandalism attempts. A camera module captures real-time video streams of the ATM surroundings, providing visual data for intelligent surveillance and activity analysis.

The Processing Layer is centered on a Raspberry Pi 4B, which serves as the edge-computing device responsible for data acquisition and analysis. Sensor readings from the IR and vibration sensors are collected and processed alongside visual information obtained from the camera. Computer vision algorithms implemented using OpenCV perform image preprocessing, object detection, motion analysis, and activity monitoring. The edge-processing approach ensures low latency, reduced network dependency, and faster response times compared to cloud-based solutions.

The Decision Layer acts as the intelligence engine of the system. This layer combines sensor inputs and computer vision outputs through a sensor fusion mechanism to evaluate the security status of the ATM. Based on predefined thresholds and AI-driven analysis, the system classifies events as normal activity, suspicious behavior, or confirmed intrusion. This decision-making process improves detection accuracy while minimizing false alarms.

Upon identifying a threat, the Response Layer activates appropriate security measures. A solenoid lock mechanism is triggered to secure the ATM cabin and prevent unauthorized access. Simultaneously, an alarm system generates an audible warning to alert nearby personnel and deter intruders. The camera captures and stores visual evidence of the incident for future investigation and forensic analysis.

The Communication Layer is implemented using a GSM communication module, which transmits real-time alert messages to authorized personnel and security agencies whenever a security breach is detected. The alert includes incident information, enabling rapid intervention and minimizing potential losses. Event logs and captured images are also maintained for monitoring and post-event analysis.

The integration of edge computing, computer vision, sensor fusion, and automated response mechanisms enables the proposed architecture to operate as a proactive security framework rather than a passive monitoring system. This architecture significantly enhances ATM security by providing continuous surveillance, intelligent threat detection, rapid response, and remote notification capabilities.

6. IMPLEMENTATION

The implementation of the proposed AI-Based Secure ATM Access and Intelligent Intrusion Response System is carried out using an embedded hardware platform (Raspberry Pi 4B) integrated with multiple sensors and actuators, along with computer vision and AI-based software modules. The system operates in real time by continuously collecting environmental data through sensors and a camera module,

processing the data using OpenCV-based image processing and Python-based control logic, and generating appropriate security responses such as locking the ATM, triggering alarms, and sending GSM alerts. The implementation focuses on achieving low-latency edge processing, high detection accuracy through sensor fusion, and automated response generation without human intervention.

6.1 Raspberry Pi 4B as Central Processing Unit

The Raspberry Pi 4B acts as the core controller of the system, responsible for interfacing with all sensors and executing the AI-based processing logic. It handles real-time data acquisition, decision-making, and control of output devices such as alarms and solenoid locks. Its edge-computing capability ensures fast processing without relying on cloud servers.

6.2 Infrared (IR) Sensor for Entry Detection

The IR sensor is installed at the ATM entrance to detect human presence. When a person enters the ATM cabin, the sensor sends a high signal to the Raspberry Pi, which activates the surveillance system. This ensures that monitoring begins immediately when any user enters the ATM area.

6.3 Vibration Sensor for Tampering Detection

A vibration sensor is attached to the ATM structure to detect physical attacks such as drilling, breaking, or forced entry attempts. If abnormal vibration patterns are detected, the system classifies it as a potential intrusion. This helps in identifying mechanical attacks that camera-based systems may not detect.

6.4 Camera Module with OpenCV Processing

A USB camera continuously captures real-time video frames of the ATM environment. These frames are processed using OpenCV for tasks such as motion detection, object tracking, and suspicious activity identification. This provides visual intelligence for detecting unauthorized behavior.

6.5 Python-Based Control and AI Logic

The entire system is implemented using Python due to its

strong support for hardware interfacing and AI libraries. Custom logic is developed to analyze sensor inputs and camera data to classify events as normal, suspicious, or critical. This forms the decision-making engine of the system.

6.6 Sensor Fusion Mechanism

Data from the IR sensor, vibration sensor, and camera module are combined to improve accuracy. A security alert is triggered only when multiple inputs confirm suspicious activity. This reduces false alarms and improves system reliability.

6.7 Solenoid Lock Mechanism

A solenoid lock is connected to the ATM door and controlled through Raspberry Pi GPIO pins. When an intrusion is detected, the lock is automatically activated to restrict access. This provides immediate physical security control.



The proposed AI-Based Secure ATM Access and Intelligent Intrusion Response System was evaluated based on its ability to detect unauthorized access, respond to security threats in real time, and maintain overall system reliability under different operational conditions. The evaluation focuses on system implementation performance, sensor fusion effectiveness, detection accuracy, response time, and comparative efficiency against conventional ATM security systems. The results demonstrate that integrating edge computing with AI-based monitoring and multi-sensor fusion significantly enhances ATM security and reduces response latency.

7.1 System Implementation Results

The implemented system successfully integrates IR sensors, vibration sensors, camera modules, and GSM communication with the Raspberry Pi 4B. During testing, the system effectively detected human presence at the ATM entrance and activated surveillance mechanisms instantly. Unauthorized access attempts and abnormal vibration patterns were accurately identified, triggering immediate security responses such as alarm activation, solenoid lock engagement, and SMS alerts. The system operated continuously without failure, demonstrating stable real-time performance and reliable hardware-software integration.



Fig. 5. Mask detection



7.2 Model Evaluation

The decision-making module based on computer vision and sensor fusion was evaluated using simulated intrusion scenarios. The system correctly classified events into normal, suspicious, and critical categories with high consistency. The integration of OpenCV-based motion detection with sensor inputs improved detection reliability. The model showed strong performance in distinguishing between legitimate ATM users and potential intruders, minimizing false classifications.

7.3 Performance Analysis

The performance of the system was measured in terms of detection time, response time, and accuracy. The average intrusion detection time was observed to be less than 2 seconds, while the alert generation time via GSM was approximately 3–5 seconds. The system demonstrated high responsiveness due to edge-based processing on the Raspberry Pi 4B. Sensor fusion further improved reliability by reducing false alarms caused by isolated sensor triggers.

Key performance observations include:

- Fast real-time processing due to edge computing
- Low latency in alert generation
- Stable sensor-to-decision pipeline
- Reduced dependency on internet connectivity

7.4 Recommendation Quality Analysis

The system's "recommendation quality" refers to the accuracy of its decision-making process in classifying security events. The fusion of IR sensor data, vibration signals, and visual analysis significantly improved classification precision. The system reliably recommended appropriate responses such as alarm activation or system lockdown based on threat severity. This multi-layer decision framework ensured that actions were context-aware and proportionate to the detected threat level.

7.5 Comparative Analysis

Feature	Traditional Approach	Proposed System
Detection Method	Passive CCTV	AI + Sensors Fusion
Response Time	Delayed	Real-time (<5 sec)

Feature	Traditional Approach	Proposed System
	Approach	System
Alert Mechanism	Manual/Delayed	Automatic GSM SMS
False Alarm Rate	High	Low
Automation Level	Low	High

7.6 Overall System Outcome

The overall outcome of the implemented system confirms that the integration of artificial intelligence, IoT sensors, and edge computing significantly enhances ATM security. The system successfully detects unauthorized access, responds autonomously to threats, and communicates alerts in real time. It reduces dependency on human monitoring and ensures continuous surveillance with minimal latency. The proposed framework is scalable, cost-effective, and suitable for deployment in modern banking environments, making it a robust solution for next-generation ATM security systems.

8. CONCLUSION

The proposed AI-Based Secure ATM Access and Intelligent Intrusion Response System successfully demonstrates an effective and intelligent approach to enhancing the security of Automated Teller Machines using a combination of artificial intelligence, IoT sensors, and edge computing. The system addresses the limitations of traditional ATM security mechanisms by introducing real-time intrusion detection, automated decision-making, and immediate response capabilities.

By integrating an IR sensor, vibration sensor, and camera module with a Raspberry Pi-based processing unit, the system achieves reliable multi-layer security through sensor fusion and computer vision techniques. The use of OpenCV enables real-time monitoring and analysis of suspicious activities, while the embedded AI logic ensures accurate classification of events with reduced false alarms. Furthermore, the incorporation of

GSM-based alert notifications ensures timely communication with security personnel, thereby reducing response delays during critical incidents.

The implementation results confirm that the system operates efficiently in real-time environments with low latency and high reliability. The automated response mechanisms, including solenoid lock activation and alarm triggering, provide immediate physical security control, making the system proactive rather than reactive.

Overall, the proposed solution offers a cost-effective, scalable, and intelligent framework for modern ATM security. It significantly improves threat detection accuracy, reduces dependency on human surveillance, and enhances overall system responsiveness. This makes it suitable for deployment in banking environments where security, speed, and reliability are critical requirements.

9. FUTURE WORK

The proposed AI-Based Secure ATM Access and Intelligent Intrusion Response System provides a strong foundation for enhancing ATM security; however, there are several areas where further improvements and extensions can be explored. Future enhancements can focus on improving the intelligence, scalability, and adaptability of the system.

One major direction for future work is the integration of advanced deep learning models for improved accuracy in facial recognition, behavior analysis, and anomaly detection. By deploying optimized neural networks such as lightweight convolutional neural networks (CNNs) or transformer-based models, the system can achieve higher precision in identifying unauthorized users and suspicious activities under varying environmental conditions.

Another enhancement can be the incorporation of cloud-based analytics alongside edge computing. While the current system operates efficiently at the edge using Raspberry Pi, cloud integration can enable large-scale data storage, centralized

monitoring, and advanced forensic analysis. This hybrid approach would improve long-term data insights and system scalability across multiple ATM locations.

The system can also be extended to support biometric authentication methods such as fingerprint recognition, iris scanning, or facial recognition-based user verification. This would further strengthen access control and reduce the risk of identity-based fraud.

Additionally, integration with advanced IoT frameworks and 5G communication technology can significantly improve real-time response speed and connectivity reliability. This would allow faster alert transmission and more robust remote monitoring capabilities.

Future work may also focus on enhancing the predictive capabilities of the system by incorporating machine learning-based predictive analytics. This would enable the system to anticipate potential security threats based on historical data patterns and environmental behavior trends.

Finally, improving the system's power efficiency, hardware optimization, and deployment cost-effectiveness will further support large-scale implementation in banking infrastructures, making the solution more practical and commercially viable.

8. REFERENCES

- [1]. Degadwala, Sheshang, et al. "Advancements in ATM Security for Movement and Tampering Detection: A Review." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2024. Available at: <https://doi.org/10.32628/CSEIT2410587>.
- [2]. Sanserwal, Vishal, et al. "Comparative Analysis of Various Feature Descriptors for Efficient ATM Surveillance Framework." *Proceeding - IEEE International Conference on Computing*,
- [3]. *Communication and Automation, ICCCA 2017*, 2017, pp. 539–44. Available at: <https://doi.org/10.1109/CCAA.2017.8229860>.

[4]. Liu, Fan, et al. "Abnormal Behavior Recognition System for ATM Monitoring by RGB-D Camera." MM 2012 - Proceedings of the 20th ACM International Conference on Multimedia, 2012, pp. 1295 – 96. Available at: <https://doi.org/10.1145/2393347.2396450>.

[5]. Wu J-D, Ye S-H (2009) Driver identification using finger-vein patterns with Radon transform and neural network. Expert SystAppl 36(3, Part 2):5793–5799.

[6]. Researcher Wu and Liu have described neural network and component analysis methodology used in finger vein authentication method.