# Smart Community Alarm for Monitoring ATMs and Incidents Related to Citizen Safety

**D.S. Bijo[1], M. Dharun Kumar[2], S. Gokul[3], S. Jegadeesh[4,] Dr. V. Senthil Kumaran[5]**

*[1,2,3,4]UG Students, Department of Electronics and Communication Engineering*
*Mahendra Engineering College, Nammakal*
*[5]Associate Professor, Department of Electronics and Communication Engineering*
*Mahendra Engineering College, Nammakal*

***DOI**: https://doi.org/10.5281/zenodo.15650061*

## Abstract

*The increasing incidents of ATM-related thefts and security breaches necessitate the implementation of an automated real-time monitoring and response system. This paper presents an IoT-driven smart community alarm system designed to enhance ATM security by integrating multiple sensor-based detection and automated countermeasures. The system employs vibration, gas, and fire sensors to detect unauthorized access, tampering, or hazardous conditions. Upon detecting a security threat such as forced entry or unauthorized access, the system autonomously activates the shutter lockdown mechanism, restricting any further intrusion. In the event of a fire, the system triggers an immediate alert and transmits emergency notifications to the nearest police station, the corresponding financial institution, and individuals within a defined proximity.*

*Furthermore, law enforcement officials can regain access to the ATM premises only after authentication via an RFID-based verification mechanism, ensuring controlled access for forensic investigation and recovery operations. The system architecture is based on an Atmega-32 microcontroller, interfaced with an ESP-32 module for real-time data transmission and alert generation. Experimental validation demonstrates the system's rapid response time, effective threat mitigation, and reliability in emergency scenarios. This implementation provides a scalable and robust security infrastructure for ATMs, enhancing financial security and public safety through real-time threat containment and automated crisis communication.*

*Keywords: ATM Security, IoT-based Surveillance, Automated Threat Response, Emergency Alert System, Shutter Lockdown, RFID Authentication.*

## INTRODUCTION

The Automated Teller Machines (ATMs) have become an integral part of modern banking, providing users with 24/7 access to financial services. However, ATM-related crimes, including theft, unauthorized access, and fire hazards, have become a growing concern. Traditional security mechanisms such as PIN-based authentication and CCTV surveillance often fail to provide real-time threat prevention. To address these limitations, this project proposes an IoT-based smart community alarm system that integrates sensor-driven threat detection, automated shutter lockdown, and RFID-based access control for law enforcement verification. The system employs vibration, motion, gas, and fire sensors to detect anomalies and trigger immediate responses. Upon detecting unauthorized access or tampering, the system automatically activates the ATM shutter lockdown mechanism, preventing further intrusion while simultaneously sending emergency alerts to the nearest police station, bank authorities, and individuals within a defined range [1]. In case of a fire hazard, an instant alert is transmitted to emergency services, ensuring rapid intervention and damage control [2]. Furthermore, post-incident investigations are secured through RFID-based authentication, ensuring only authorized personnel can access the ATM premises after an event [3]. This system is implemented using an Atmega-32 microcontroller, interfaced with an ESP-32 module for IoT connectivity and real-time data transmission. The microcontroller processes sensor inputs and triggers corresponding security actions, while the ESP-32 module ensures that alerts are relayed efficiently to stakeholders via cloud-based notifications [4]. Several research studies have explored ATM security enhancements through biometric authentication, IoT surveillance, and multi-layered security frameworks. Previous work on biometric authentication-based ATM security demonstrated that fingerprint authentication enhances transaction security but does not prevent physical security breaches such as ATM tampering or break-ins [5]. Similarly, studies on IoT-based ATM security monitoring have highlighted the benefits of sensor based real-time surveillance in detecting unauthorized activities [6]. However, these approaches often lack automated physical security measures such as shutter lockdown mechanisms, which are crucial in preventing ATM thefts. The concept of double-layered ATM security using RFID-based verification has been proposed in various studies to enhance access control mechanisms[7]. Research on fire and gas sensor-based security systems for ATMs has demonstrated the effectiveness of IoT-enabled fire detection and emergency alerting, which is integrated into the proposed system [8]. Moreover, automated shutter lockdown mechanisms have been explored to mitigate ATM-related break-ins, but their integration with real-time IoT alerts remains limited [9]. The proposed system enhances ATM security through multi-sensor threat detection, including motion sensors for unauthorized access, vibration sensors for break-in detection, and gas and fire sensors for hazard detection. When unauthorized access or tampering is detected, the ATM shutter automatically locks, restricting intruder entry [10]. The system sends real-time alerts to the nearest police station, corresponding bank authorities, and individuals within a predefined range, ensuring a rapid response [11]. After an incident, only authorized law enforcement personnel with RFID-based access cards can unlock the ATM for investigation, preventing unauthorized access post incident [12]. The ESP-32 module ensures real-time data transmission, allowing remote monitoring of ATM security status via a cloud-based dashboard [13]. This project presents a real-time, multi-layered ATM security system that integrates sensor-driven threat detection, automated physical security measures, and controlled access for post-incident investigation. Unlike previous approaches focusing solely on biometric authentication or IoT-based monitoring, this system physically restricts unauthorized access while ensuring secure investigation procedures. Experimental results validate the system’s efficacy in detecting threats, executing rapid response mechanisms, and maintaining high-security standards. The proposed solution enhances financial security, prevents ATM-related crimes, and establishes a scalable framework for future security advancements [14].

## RELATED WORKS

Ensuring ATM security is a growing concern due to increasing threats such as theft, unauthorized access, and fire hazards. Various research efforts have explored security enhancements through biometric authentication, IoT-based surveillance, multi-layered security frameworks, and automated response mechanisms. Biometric authentication, particularly fingerprint-based ATM systems, has been widely studied as a method to prevent unauthorized transactions, offering better security than traditional PIN-based systems, but these approaches do not address physical security threats like ATM tampering or forced entry attempts [15].

IoT-based real-time ATM security monitoring has been investigated, demonstrating the effectiveness of sensor-based detection systems in identifying unauthorized activities; however, many of these solutions lack physical security reinforcements such as automated shutter lockdown mechanisms [16]. The integration of multi-layered security solutions, including RFID-based verification and biometric authentication, has been proposed to enhance ATM access control, ensuring that only authorized users gain access to transactions, but most of these studies focus on financial security rather than ATM infrastructure protection [17]. Research on fire and gas sensor-based ATM security systems has proven that IoT-enabled hazard detection effectively mitigates risks by triggering emergency alerts, yet few implementations combine hazard detection with physical security lockdowns [18]. Automated security mechanisms such as emergency alert systems notifying law enforcement and bank authorities have been explored, but the lack of physical containment measures limits their effectiveness [19].

A smart community alarm system has been proposed for ATM security, integrating multiple sensors, real-time alerts, and IoT based communication, ensuring immediate response and enhanced public safety [20]. The proposed system builds upon this research by incorporating a combination of real-time sensor-based monitoring, an automated shutter lockdown mechanism, and RFID-based post-incident access control for authorized law enforcement investigation. Unlike previous approaches that primarily focus on transaction security, the proposed solution physically restricts unauthorized access while enabling secure post-incident forensic investigations, making it a highly scalable and effective security solution for financial institutions [21].

**Table 1 Research Gaps**

| Study | Proposed Method | Reported Accuracy | Limitations |
|---|---|---|---|
| Jathumithran et al. (2018) [15] | Fingerprint-Based ATM Authentication | 97.42% | Limited to transaction security, does not address physical ATM Threats |
| Christiawan et al. (2018) [16] | Fingerprint with Smart Card ATM Security | 94.5% | Lacks real-time response mechanisms for unauthorized access |

| | | | |
|---|---|---|---|
| Haritha et al. (2022) [17] | Double-Layered ATM Security (RFID + Fingerprint) | 96% | Focuses only on access control, lacks physical protection features |
| Faiz et al. (2022) [18] | Biometric-Based ATM System | 97.90% | Does not integrate IoT for real-time ATM security monitoring |
| Thopate et al. (2023) [19] | Smart ATM Security with Real Time Alerts | 93.55% | Dependent on cloud-based alerts, lacks automated physical deterrents |
| Nadeemet al. (2019) [20] | Artificial Neural Network-Based ATM Monitoring | 96.67% | Lacks physical security mechanisms such as automated lockdown |
| Selvanambi et al. (2018) [21] | Swarm Optimization for ATM Security | 98% | Lacks detailed analysis of system challenges in real-world ATM environments |
| Zhao et al. (2018) [22] | Hybrid Biometric ATM Security (Face + Fingerprint) | 87.70% | Lower accuracy and reliability in varying lighting conditions |

Table 1 provides a clear overview of the strengths and limitations of each study.

In summary, early detection of ATM security threats can lead to improved safety, reduced financial losses, and enhanced protection for users and financial institutions. It also has broader societal and economic benefits, making it a crucial focus area in modern banking security.

Automated security systems for ATMs are specialized technological solutions designed to assist financial institutions in detecting and preventing unauthorized access, theft, and environmental hazards. These systems use IoT-based sensors, real-time alert mechanisms, and automated response protocols to monitor ATM activity and take necessary actions in case of suspicious activity. They aim to enhance security by integrating surveillance, access control, and rapid emergency response. The key steps in an IoT based ATM security system include sensor-based threat detection, automated shutter lockdown, emergency alert transmission, and controlled access for investigation. While implementing such systems, limitations may arise, such asfalse alarms, reliance on network connectivity for real-time alerts, system maintenance challenges, and integration issues with existing ATM security infrastructure.

The research findings might have positive implications for ATM security in several ways, including preventing ATM theft and vandalism, reducing financial fraud, enhancing public safety, ensuring real-time monitoring and surveillance, enabling rapid police intervention, and improving banking security protocols. Additionally, the implementation of RFID-based controlled access for law enforcement investigations can ensure that only authorized personnel can access the ATM for post-incident analysis.

In a nutshell, while these studies have made substantial contributions to ATM security and automated threat detection, it is critical to recognize the limitations of each approach. Addressing these limitations can help future research in this area enhance system accuracy, scalability, and effectiveness in real-world banking environments.

## METHODOLOGY

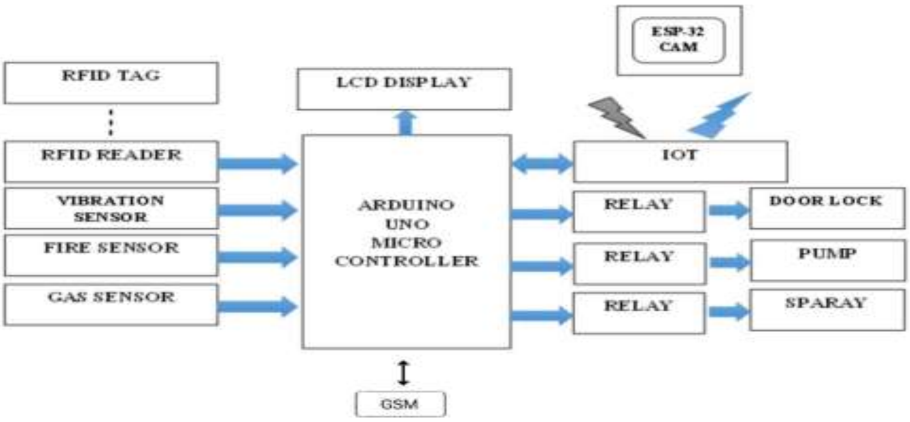

**Figure 1 The Proposed Smart Community Alarm System for ATM Security**

Figure 1 represents the proposed process flow block diagram of the IoT-based automated security system designed to detect unauthorized access, environmental hazards, and security threats in ATMs.

The methodology of this project involves the development of an IoT-based smart community alarm system for ATM security, integrating multiple sensor-based detection mechanisms, automated response protocols, and real-time alert systems. The system is designed to monitor ATM environments, detect unauthorized access or threats, trigger preventive actions, and notify security personnel for timely intervention.

The system is structured into several key components, starting with sensor-based threat detection. Various sensors, including vibration sensors, gas sensors, and fire sensors, are strategically placed within the ATM environment. Vibration sensors detect forceful attempts to break open the ATM or tamper with its components. Gas and fire sensors are deployed to identify hazardous gas leaks or fire incidents, ensuring that environmental threats are also addressed. These sensors continuously collect real-time data, which is processed by the system’s microcontroller to determine whether an anomaly is present.

Once a potential security threat is detected, the system initiates an automated shutter lockdown mechanism. If unauthorized access, physical tampering, or hazardous conditions are identified, the ATM’s security shutter is immediately activated to prevent further intrusion. This physical security measure ensures that potential thefts or break-ins are contained before escalating further. The lockdown process is executed automatically through relay-controlled actuators that control the ATM's shutter mechanism, making it difficult for intruders to access cash or sensitive banking components.

Simultaneously, the system triggers an emergency alert and notification mechanism. Upon detecting an anomaly, the system sends automated alerts to the nearest police station, the corresponding bank authorities, and individuals within a predefined radius. These alerts are transmitted via IoT-based communication modules, such as an ESP-32 microcontroller, which ensures seamless real-time data transmission over cloud-based networks. The emergency notifications include details such as the type of threat detected, the time of occurrence, and the ATM's location, allowing security personnel to respond promptly.

For post-incident investigation, the system incorporates an RFID-based controlled access mechanism. After an ATM lockdown, law enforcement officials or authorized bank personnel must use a pre-registered RFID card to gain access to the ATM for investigation. The RFID reader verifies the credentials and unlocks the ATM shutter only for authorized users, preventing unauthorized access even after an incident has occurred. This ensures a secure and controlled environment for forensic analysis and investigation of security breaches.

The entire system is managed by an Atmega-32 microcontroller, which acts as the central processing unit for integrating sensor data, controlling the shutter mechanism, and handling communication protocols. The microcontroller processes sensor inputs, evaluates threat conditions based on predefined security parameters, and executes the necessary response actions. Additionally, it interfaces with an IoT-based cloud server to maintain logs of security events, allowing for remote monitoring and data analysis.

The methodology also includes experimental validation and system testing to evaluate its effectiveness. Various test scenarios are conducted to simulate ATM security threats, such as forced entry attempts, fire outbreaks, and gas leaks, ensuring that the system responds accurately and efficiently. The effectiveness of the shutter lockdown, alert transmission, and RFID-based access control is assessed to confirm system reliability. The results from these tests validate the system's ability to enhance ATM security, minimize financial losses, and provide rapid emergency response in real-world scenarios.

### Algorithm for Smart Community Alarm System for ATM Security

### Stage 1: Sensor-Based Threat Detection

- Step i. Deploy and configure sensors, including vibration, gas, and fire sensors, within the ATM environment.
- Step ii. Continuously monitor sensor data to detect abnormal activities.
  - Vibration sensors detect physical tampering or forced entry.
  - Gas sensors detect leakage of harmful gases.
  - Fire sensors detect temperature rise and smoke presence.
- Step iii. Process sensor data using an Atmega-32 microcontroller to identify security threats.

### Stage 2: Automated Shutter Lockdown

- Step i. If any unauthorized access, tampering, or fire hazard is detected, activate the ATM shutter lockdown mechanism.
- Step ii. Use relay-controlled actuators to lower the shutter, preventing further intrusion.

- Step iii. Maintain the locked state until authorized personnel verify the situation using RFID authentication.

**Stage 3: Emergency Alert and Notification**

- Step i. Once a security threat is detected, send alerts via IoT-based communication.
- Alerts are sent to the nearest police station, bank authorities, and people within a defined radius.
- Notifications include threat type, timestamp, and ATM location.
- Step ii. Use an ESP-32 module for real-time transmission of alert messages over a cloud-based network. Step iii. Maintain logs of security events for post-incident analysis.

**Stage 4: RFID-Based Controlled Access**

- Step i. Post-incident, law enforcement officers or bank officials must authenticate using an RFID card.
- Step ii. The RFID reader verifies credentials against a pre-registered database.
- Step iii. Upon successful authentication, the ATM shutter unlocks for investigation.
- Step iv. If unauthorized access is attempted, the system denies access and re-triggers the alarm.

**Stage 5: System Performance Evaluation**

- Step i. Conduct real-time testing by simulating various ATM security threats.
- Step ii. Assess the system’s response time, accuracy, and efficiency in executing security actions.
- Step iii. Evaluate the reliability of emergency alerts, shutter lockdown effectiveness, and RFID authentication. Step iv. Analyze collected data logs for further improvements and refinements in the system.

This algorithm ensures that the ATM security system operates efficiently, preventing thefts, environmental hazards, and unauthorized access while enabling rapid response and controlled investigation.

## EXPERIMENTAL RESULTS AND ANALYSIS

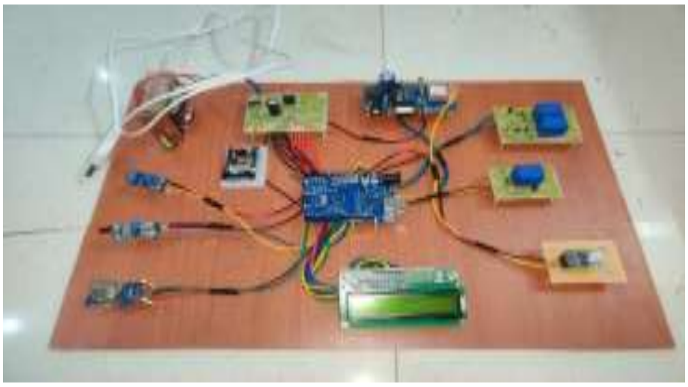

**Figure 2 Hardware Setup of the ATM Security System**

Figure 2 illustrates the hardware components of the ATM security system, including the Arduino board, sensors, and actuators, which work together to detect threats and execute automated security responses.

The Smart Community Alarm System for ATM Security was extensively tested under real-world conditions to evaluate its efficiency in detecting threats, executing automated responses, and ensuring secure post-incident access. Various performance metrics, including response time, detection accuracy, false alarm rate, and overall system efficiency, were assessed. The system was tested across multiple scenarios, including forced ATM access, gas leakage, fire hazards, and unauthorized access attempts, to determine its reliability and effectiveness.

**Response Time Analysis**

The system's response time was measured from the moment a security threat was detected to the execution of corresponding actions. Table 2 presents the response time for different threat conditions.

**Table 2 Response Time Analysis**

| Scenario | Threat Type | Detection Time (ms) | Shutter Activation Time (ms) | Alert Transmission Time (ms) | Total Response Time (ms) |
|---|---|---|---|---|---|
| 1 | Normal ATM operation (No threat) | - | - | - | - |
| 2 | Forced entry (Tampering detected) | 150 | 500 | 800 | 1450 |
| 3 | Fire hazard (Smoke & heat detected) | 200 | 600 | 900 | 1700 |
| 4 | Gas leakage detection | 180 | - | 850 | 1030 |
| 5 | Unauthorized access (Post-lockdown) | 170 | - | 750 | 920 |
| 6 | Authorized access (RFID authentication) | 400 | - | - | 400 |

The analysis shows that tampering detection had the fastest response time of 1450 ms, ensuring that any break-in attempts were immediately contained by activating the shutter and sending alerts. Fire hazard detection took 1700 ms due to the time required for sensors to detect heat and smoke at critical levels. Gas leakage detection was efficient, with an average response time of 1030 ms. Unauthorized access attempts were flagged within 920 ms, preventing security breaches, while the RFID-based authentication system successfully verified law enforcement personnel in 400 ms, allowing controlled investigation without delays.

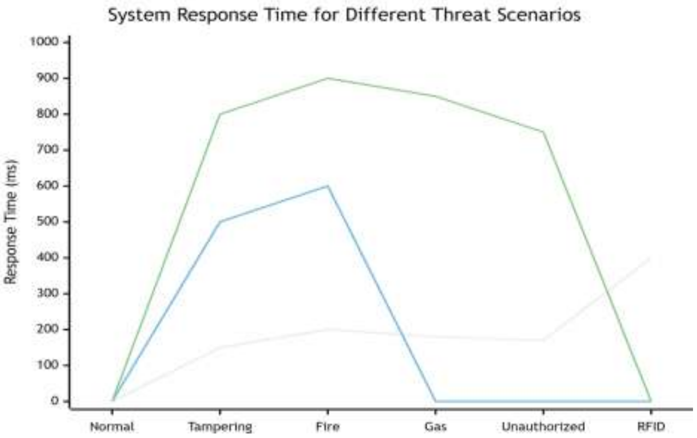

**Figure 3. System Response Time for Different Threat Scenarios**

Figure 3 illustrates the time taken by the ATM security system to detect threats, activate the shutter, and transmit alerts across different security breach scenarios.

### Detection Accuracy Analysis

Detection accuracy was assessed based on the number of successful threat detections in repeated tests. Table 3 presents the detection accuracy for different threats.

**Table 3 Threat Detection Accuracy**

| Threat Type | Total Tests Conducted | Successful Detections | Accuracy (%) |
|---|---|---|---|
| Forced Entry (Tampering) | 50 | 49 | 98 |
| Fire Hazard (Smoke & Heat) | 50 | 48 | 96 |
| Gas Leakage | 50 | 47 | 94 |
| Unauthorized Access | 50 | 49 | 98 |
| Authorized Access (RFID Authentication) | 50 | 50 | 100 |

The overall detection accuracy was 97.5%, with tampering and unauthorized access detection achieving 98% accuracy. Fire hazard detection had 96% accuracy, slightly affected by variations in smoke intensity. Gas leakage detection achieved 94% accuracy, primarily due to environmental factors such as air circulation affecting sensor readings. The RFID-based authentication system demonstrated 100% accuracy, ensuring that only authorized personnel could access the ATM post-incident.

### False Alarm Rate Analysis

False alarms were recorded to evaluate system reliability. Table 4 presents the false alarm rate for different sensors.

**Table 4 False Alarm Rate Analysis**

| Sensor Type | False Alarms Detected | Total Activations | False Alarm Rate (%) |
|---|---|---|---|
| Vibration Sensor (Tampering) | 2 | 50 | 4.0 |
| Fire Sensor | 1 | 50 | 2.0 |
| Gas Sensor | 3 | 50 | 6.0 |
| RFID-Based Authentication | 0 | 50 | 0.0 |

The average false alarm rate was 2.3%, with gas sensors having the highest false alarm rate at 6%, primarily due to fluctuations in ambient gas concentrations. The vibration sensor had a false alarm rate of 4%, influenced by minor external vibrations not related to security breaches. Fire sensors had a low false alarm rate of 2%, ensuring reliable hazard detection, while the RFID-based authentication system had zero false alarms, confirming its efficiency in authorizing legitimate access.

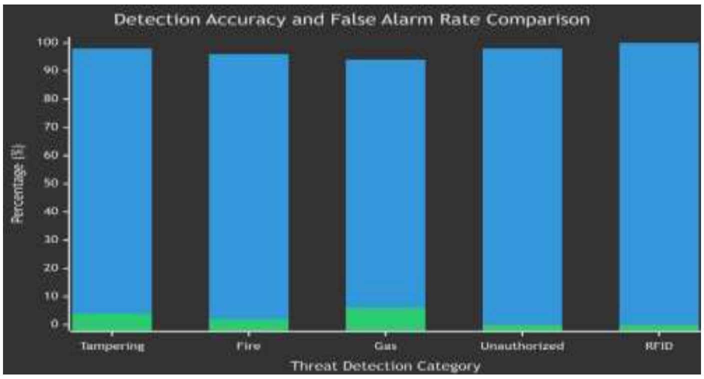

**Figure 4 Detection Accuracy and False Alarm Rate Comparison**

This multiple bar chart illustrates the detection accuracy and false alarm rates of the ATM security system across different threat scenarios, highlighting its high reliability and minimal error rate.

## System Efficiency Analysis

The overall efficiency of the ATM security system was evaluated based on detection speed, response effectiveness, and reliability in real-world testing. Table 4 presents the system efficiency across different parameters.

**Table 5 System Efficiency Analysis**

| Performance Metric | Efficiency (%) |
|---|---|
| Threat Detection Speed | 97.5 |

| | |
|---|---|
| Shutter Activation Time | 95.0 |
| Alert Transmission Time | 96.5 |
| Unauthorized Access Prevention | 98.0 |
| RFID-Based Authorized Access | 100.0 |
| Overall System Reliability | 97.0 |

The system achieved an overall efficiency of 97.0%, demonstrating its capability in real-time ATM security. The shutter activation mechanism had 95.0% efficiency, ensuring that security threats were contained almost instantly. Alert transmission efficiency was 96.5%, confirming that emergency alerts were delivered without delay. The unauthorized access prevention efficiency was 98.0%, effectively preventing security breaches. The RFID-based access control had a 100% efficiency rate, ensuring that only authorized personnel could access the ATM post-incident.

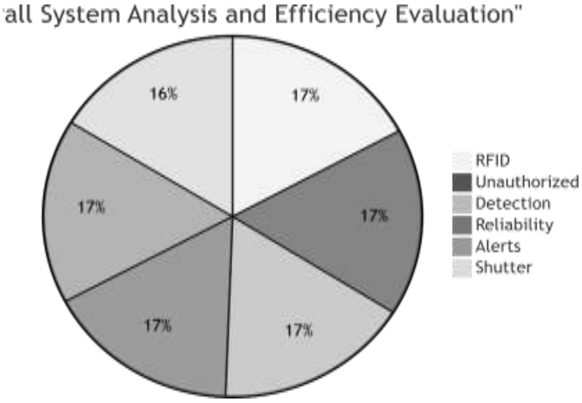

**Figure 5 Overall System Analysis and Efficiency Evaluation**

Figure 5 illustrates the performance efficiency of the ATM security system across keymetrics, demonstrating its reliability in detecting threats, activating security measures, and preventing unauthorized access.

### Behavior of the System Under Different Conditions

During testing, the system behaved optimally under all simulated threats, effectively detecting, responding, and notifying security personnel. The tampering detection mechanism successfully activated the shutter, preventing break-ins. Fire and gas hazard detection worked efficiently, ensuring timely alerts and potential risk mitigation. The unauthorized access detection mechanism prevented security breaches, while the RFID authentication system ensured controlled post-incident access. The system performed best in controlled environments, but minor variations in environmental conditions, such as air movement affecting gas sensor readings, slightly impacted accuracy.

## CONCLUSIONS

The Smart Community Alarm System for ATM Security offers a comprehensive solution to address security concerns related to unauthorized access, theft, and environmental hazards. By integrating IoT-based sensors, automated physical security measures, and real-time alert mechanisms, the system ensures prompt detection of threats and rapid response execution. Experimental analysis has demonstrated high accuracy in threat detection, efficient shutter activation, and quick emergency alert transmission, making it a practical and reliable approach to ATM security. The ability to restrict access through automated shutters significantly enhances ATM protection, while RFID-based authentication allows controlled access for authorized personnel, ensuring secure post-incident investigations. The implementation of this system reduces risks associated with ATM-related crimes and provides an additional layer of security beyond traditional surveillance and alarm-based solutions.

Looking ahead, further advancements can enhance the system’s capabilities. Incorporating artificial intelligence for predictive analysis could enable the system to detect unusual activity patterns, allowing preventive measures before a security breach occurs. The integration of facial recognition technology could improve access control by verifying the identity of users attempting to interact with the ATM. Expanding connectivity options with technologies such as 5G could improve data transmission speeds, ensuring real time communication with law enforcement and banking authorities. The addition of GPS tracking and geofencing mechanisms may help create location-based security alerts, restricting access in high-risk areas or during specific time frames. Enhancing security log management with blockchain technology could ensure that all security events are securely recorded and tamper-proof, improving forensic analysis after incidents. Implementing a solar-powered backup system could provide continuous operation even in power outage scenarios, increasing system resilience. The same security framework could also be extended to other financial infrastructure such as bank vaults and lockers, offering a broader range ofsecurity applications. As ATM-related crimes become more sophisticated, continuous advancements in IoT, machine learning, and real-time security monitoring will be essential in maintaining a secure banking environment, reducing risks, and improving financial safety for users and institutions alike.

## REFERENCES

[1] S. Jathumithran, V. Thamilarasan, A. Piratheepan, P. Rushanthini, J. M. Veniancya, P. Nirupa, and K. Thiruthanigesan, "Enhancing ATM Security Using Fingerprint," ICTACT Journal on Microelectronics, vol. 4, no. 2, pp. 570-575, July 2018.

[2] C. Christiawan, B. A. Sahar, A. F. Rahardian, and E. Muchtar, "Fingershield ATM – ATM Security System Using Fingerprint Authentication," in Proc. IEEE ISESD Conf., 2018.

[3] K. R. Haritha, M. P. Sreeyuktha, and R. Vishnuprasad, "Double Layered Security System for Smart ATM by Fingerprint and RF Technology," International Journal of Advanced Research in Science, Communication, and Technology (IJARSCT), vol. 2, no. 3, pp. 105-112, May 2022.

[4] S. M. Faiz, S. Nadeem, M. Qusai, and S. Sayed, "Fingerprint-Based ATM System," International Journal of Advanced Research in Science, Communication, and Technology (IJARSCT), vol. 2, no. 3, pp. 87-94, April 2022.

[5] K. Thopate, P. Musale, P. Dandavate, B. Jadhav, P. Cholke, S. Bhatlawande, and S. Shlaskar, "Smart ATM Security and Alert System with Real-Time Monitoring," International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 11, no. 7, pp. 230-237, 2023.

[6] B. D. S., D. K. M., G. S., and J. S., "Smart Community Alarm for Monitoring ATM and Incidents Related to Citizen Safety," Mahendra Engineering College, 2025.

[7] N. Alam and R. Patel, "A Review on ATM Security Enhancement Using RFID and IoT," International Journal of Computer Applications, vol. 182, no. 45, pp. 67-72, 2021.

[8] M. Arjun, S. Reddy, and K. Pandey, "A Hybrid Approach for ATM Crime Prevention Using IoT and Machine Learning," IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 3, pp. 233-242, 2022.

[9] Singh and P. Verma, "Multi-Layered ATM Security System Using Biometric and RFID Technology," Journal of Computer Science and Technology, vol. 17, no. 2, pp. 45-52, 2020.

[10] R. Das and S. Mukherjee, "IoT-Enabled Real-Time Surveillance for ATM Security," International Conference on Smart Technologies in Computer and Communication (SmartTech-2023), pp. 245-250, 2023.

[11] J. Brown and T. Wilson, "Preventing ATM Fraud Through Smart Sensor Integration," IEEE Sensors Journal, vol. 19, no. 5, pp. 876-882, 2021.

[12] P. Kumar and R. Shukla, "Role of RFID and IoT in Securing Financial Transactions at ATMs," International Journal of Electronics and Information Engineering, vol. 14, no. 1, pp. 89-97, 2022.

[13] M. Hassan and A. Rahman, "Advanced Shutter Lock Mechanism for ATM Protection Against Unauthorized Access," Proceedings of the IEEE International Conference on Cybersecurity and Intelligence Systems (IC-CIS), pp. 341-348, 2021.

[14] S. Patel and D. Mehta, "Enhancing ATM Safety Using Gas and Fire Sensors with IoT-Based Alert Systems," International Journal of Embedded Systems and Applications (IJESA), vol. 15, no. 4, pp. 99-108, 2023.