International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Review of Smart Atm Security System Using ESP32

Patil Shruti J.[1], Bhat Sahil N.[2], Potdar Suraj R.[3], Prof.Somoshi Kavita M.[4]

[123]BE Student, Department Of Electronics and Telecommunication Engineering, SharadChandra Pawar College of Engineering, Otur, India.
[4]Project Guide, Professor, Sharadchandra Pawar College of Engineering, Otur, India.

Abstract - Automated Teller Machines (ATMs) are integral to modern banking but are also prime targets for theft, vandalism, and tampering. Conventional CCTV-based systems mainly provide post-incident evidence, failing to offer real-time preventive measures. This paper reviews the design and development of a Smart ATM Security System using ESP32-CAM, integrating IoT, sensor fusion, and machine learning (ML) for proactive, autonomous threat detection and response. The system utilizes sensors such as PIR motion, vibration, smoke, and gas detectors to monitor the ATM environment, transmitting data via Wi-Fi to a backend server for analysis using models like YOLO or MobileNet. Depending on the classified threat level, automated actions— such as buzzer, foam spray, or ink spray activation—are triggered. This review summarizes the architecture, working methodology, advantages, limitations, and potential future enhancements of such IoT-based ATM security systems.

Keywords: - ESP32-CAM, IoT Security, Smart Surveillance, Machine Learning, ATM Safety, Sensor Fusion, MQTT, YOLO, MobileNet, Embedded Systems.

1. INTRODUCTION

Automated Teller Machines (ATMs) are a vital component of modern banking, offering customers 24/7 access to financial services. However, their unattended and isolated nature makes them vulnerable to theft, vandalism, and tampering. Traditional security systems mainly rely on CCTV cameras and manual monitoring, which are reactive in nature—recording events rather than preventing them. As a result, many incidents are detected only after significant losses have occurred. Recent advancements in Internet of Things (IoT), Edge Computing, and Machine Learning (ML) have enabled the development of smarter, automated surveillance systems capable of real-time analysis and response. Among these, the ESP32-CAM microcontroller has emerged as a cost-effective and compact platform that combines computing, camera, and Wi-Fi capabilities. It supports multiple environmental and motion sensors, making it ideal for intelligent, IoT-based monitoring applications. The Smart ATM Security System using ESP32-CAM integrates various sensors—such as motion, vibration, gas, and smoke detectors—with a camera module for real-time data collection. This information is transmitted via Wi-Fi to a backend server, where an ML model (e.g., YOLO or Mobile Net) classifies threat levels as Normal, Minor, or Major. Based on this analysis, the system automatically activates deterrents such as buzzers, foam, or ink sprays and updates a live monitoring dashboard. By combining IoT and AI technologies, the proposed system transforms conventional ATM surveillance from a reactive to a proactive security model, capable of detecting, analyzing, and responding to threats autonomously in real time.

2. REVIEW OF EXISTING SYSTEMS

2.1 Traditional ATM Security: Conventional systems rely on CCTV cameras and manual supervision, which merely record events for post-incident investigation. While some advanced setups feature remote monitoring centers, they are still dependent on human interpretation and delayed response.

2.2 Limitations: Existing solutions suffer from several drawbacks: • Reactive monitoring, not preventive. • Dependence on human vigilance and high operational costs. • No automated action or ML-based detection. • Absence of environmental monitoring (gas, smoke, temperature). • Lack of IoT connectivity for real-time alerts. These limitations have prompted the need for autonomous, IoT-enabled systems capable of immediate response and continuous remote monitoring. To develop a system that detects whether the rider is wearing a helmet and permits the vehicle to start only when the helmet is properly worn, along with an accident-detection mechanism that reports the location to emergency contacts.

3. SYSTEM OVERVIEW

The Smart ATM Security System using ESP32- CAM introduces an intelligent, multi-layered design consisting of sensing, processing, and response layers

3.1 Hardware Components

• ESP32-CAM: Main controller with camera interface.

• PIR Sensor: Detects human motion.

• Vibration Sensor (SW-420): Detects tampering or drilling.

• Gas/Smoke Sensors (MQ-2, MQ-135): Detect chemical leaks or fire.

• DHT22 Sensor: Measures temperature and humidity.

• Relay Module: Controls actuators like buzzer and sprays.

• Actuators: Foam and ink sprays for deterrence.

• Power Supply: Stable 5V/12V regulated supply.

3.2 Software and Communication

• Firmware: Developed using Arduino IDE or PlatformIO.

• Protocols: MQTT or HTTP for IoT data transmission.

• Backend: Python (Flask/FastAPI) or Node.js handles server-side processing.

• ML Framework: TensorFlow or PyTorch for YOLO/MobileNet models.

• Database: SQLite. • Frontend: HTML + CSS.

4. WORKING PRINCIPLE

The ESP32-CAM continuously monitors the ATM environment. When any sensor detects an anomaly, the camera module captures an image and transmits both the sensor data and image to the backend server via Wi-Fi. The machine learning model (YOLO/MobileNet) processes this data to classify threat levels into:

• Normal Condition: No threat detected.

• Minor Threat: Suspicious activity; buzzer or foam spray activated.

• Major Threat: Confirmed intrusion; ink spray triggered and alert sent.

Real-time updates, logs, and alerts are displayed on a web-based dashboard for security personnel.

5. METHODOLOGY AND SYSTEM FLOW

1. Data Collection: Continuous monitoring by sensors and ESP32-CAM.

2. Data Transmission: Via Wi-Fi using MQTT or HTTP.

3. Analysis: ML model evaluates incoming data and classifies threat level.

4. Response: ESP32 receives command to activate actuators.

5. Notification: Dashboard updates with event logs and live images.

6. Loop: System resumes monitoring after each event.

7. This hybrid rule-based and ML-driven architecture ensures both speed and accuracy in threat management.

6. ADVANTAGES

• Real-time and automated detection.

• Integration of multiple sensors for contextual awareness.

• Low-cost and scalable IoT hardware.

• Immediate preventive action without human intervention.

• Remote monitoring and data logging.

• Energy-efficient design using low-power components. • Proactive security models compared to conventional CCTV systems

7. APPLICATIONS

Beyond ATMs, the system can be adapted for:

• Bank vaults and locker rooms.

• Cash transport vans.

• Data centers or high-security facilities.

• Industrial zones for fire/gas detection.

• Smart home or office surveillance.

8. CHALLENGES AND LIMITATIONS

• Dependence on network connectivity for real-time communication.

• Limited processing capability of ESP32 for complex on-board ML inference.

• Environmental factors (dust, lighting) may affect camera performance.

• Maintenance of actuators and sensors required periodically.

9. CONCLUSIONS

The Smart ATM Security System using ESP32 represents a significant advancement in low-cost, intelligent surveillance. By fusing IoT sensors, machine learning, and automated actuators, the system shifts ATM protection from reactive monitoring to proactive defense. It demonstrates the potential of combining embedded systems with AIdriven analytics to create a scalable and efficient solution for modern security challenges. This IoT-based prototype can be extended to other sectors requiring continuous, intelligent surveillance marking a vital step toward smart and autonomous security systems.

REFERENCES

[1] Espressif Systems, ESP32-CAM Technical Reference Manual, Espressif Systems, 2023.
[2] Adafruit Industries, DHT22 Temperature and Humidity Sensor Documentation, Adafruit, 2022.
[3] MQ Series, Technical Data Sheets for Gas Sensors (MQ-2, MQ-135), Henan Hanwei Electronics Co., Ltd., 2023.
[4] Arduino.cc, Arduino IDE and Library Reference Guide, Arduino, 2024.
[5] OASIS, MQTT Version 5.0: Specification for IoT Communication Protocol, OASIS Open, 2023.
[6] TensorFlow Developers and PyTorch Team, Model Training and Deployment Guidelines, Google Brain and Meta AI, 2024.
[7] IEEE Xplore, “Research on IoT-Based Smart Security Systems,” IEEE Access, vol. 12, pp. 14523–14537, 2021–2024.
[8] ResearchGate, “Machine Learning for Surveillance and Anomaly Detection,” International Journal of Advanced Computing Research, vol. 10, no. 3, pp. 221–229, 2023.

[9] Flask and FastAPI Documentation, Web Frameworks for IoT and ML Applications, Python Software Foundation, 2024.
[10] Mosquitto, MQTT Broker for IoT Applications: Developer Documentation, Eclipse Foundation, 2023.
[11] S. A. Khan, R. Kumar, and V. Gupta, "IoT-Based Real-Time Smart Surveillance System Using Edge Computing," IEEE Internet of Things Journal, vol. 9, no. 15, pp. 14367–14378, Aug. 2022.
[12] M. S. Patel and P. P. Desai, "Implementation of Smart ATM Security Using IoT and Image Processing," IEEE International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2023, pp. 672–678.
[13] S. Sharma and D. Mehta, "LowCost Embedded Monitoring System Using ESP32 and MQTT," International Journal of Embedded Systems Research, vol. 14, no. 2, pp. 105–114, 2022.
[14] J. Li, K. Kim, and T. Park, "Lightweight Deep Learning Models for Edge AI-Based Surveillance," IEEE Transactions on Consumer Electronics, vol. 68, no. 4, pp. 256–263, Dec. 2022.
[15] R. Singh and A. Sinha, "Enhancing ATM Security Using IoT and Artificial Intelligence," Proceedings of the 2023 IEEE Conference on Smart Technologies for Smart Nations (SmartTech), New Delhi, India, pp. 450–456, 2023.