AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 4(2025)

IOT BASED ATM MONITORING USING CLOUD DATA WITH SENSORS

[1] Dr. G.Deepthi, [2] S. Shailaja, [3] P. Ganesh, [4] A. Hari Krishna, [5] A. Yashwanth,

[1] *Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301*

[2,3,4,5] *B. Tech Student, Department of Electronics and Communication Engineering, Samskruti College of Engineering and Technology, Hyderabad 501301*

ABSTRACT

The increasing number of ATM thefts, vandalism, and technical failures has raised concerns regarding the security and operational reliability of automated teller machines. This project proposes an IoT-based ATM monitoring system that integrates sensors, cameras, and cloud technology to ensure real-time surveillance, environmental monitoring, and intelligent alerting. The system utilizes NodeMCU or Raspberry Pi as the core controller to collect data from various sensors such as temperature, vibration, gas, and motion detectors. This data is then transmitted to a cloud server for analysis and storage. In case of suspicious activities like unauthorized access or smoke detection, alerts are instantly sent to authorities via email, SMS, or mobile application notifications. This approach enhances the security, efficiency, and reliability of ATM systems using IoT and cloud technologies.

Keywords: NodeMCU, Cloud Computing, Real-Time Monitoring, Vibration Sensor, Gas Sensor, Motion Detection, Surveillance System, Intelligent Alerting, Remote Monitoring, Smart Banking.

I. INTRODUCTION

Automated Teller Machines (ATMs) are vital financial infrastructures providing round-the-clock access to banking services. However, their exposure to physical tampering, environmental hazards, and mechanical failures makes them vulnerable to damage and misuse. Traditional ATM surveillance relies mainly on CCTV cameras and manual inspection, which are often reactive rather than preventive. The Internet of Things (IoT) introduces a new paradigm in ATM monitoring by enabling real-time, sensor-based data collection and cloud integration. Through IoT, multiple sensors can continuously track temperature, smoke, vibrations, or human presence within ATM kiosks. The collected data is uploaded to cloud servers for analysis and visualization, ensuring continuous monitoring and timely alerts. This project leverages IoT's capability to create an intelligent, connected ATM surveillance network that enhances security, operational uptime, and maintenance efficiency.

II. LITERATURE SURVEY

1. Sharma et al. (2019) – IoT-Enabled ATM Security System

Sharma et al. (2019) developed an IoT-based ATM security system using motion and gas sensors. Their model used an ESP8266 microcontroller to detect motion or smoke and send alerts via the Blynk cloud platform. The system demonstrated significant improvement in detecting unauthorized access in real time, minimizing property loss. However, it lacked integrated camera support and cloud data analytics, limiting post-event investigations.

2. Patel and Mehta (2020) – Smart ATM Surveillance Using Sensors and GSM

Patel and Mehta (2020) proposed a GSM-enabled ATM monitoring system integrating vibration and temperature sensors. The system could detect tampering or overheating conditions and send SMS alerts to authorities. While effective in remote alerting, it relied on GSM networks without cloud data storage or visualization, making long-term analytics difficult.

3. Reddy et al. (2021) – Cloud-Based ATM Monitoring System

Reddy et al. (2021) designed a cloud-based IoT monitoring system that connected ATMs to a centralized data platform. Using MQTT protocol

Received: 28-09-2025 | Accepted: 03-11-2025 | Published: 10-11-2025 | www.ajaccm.com

and AWS IoT Core, their system collected data from multiple kiosks, enabling real-time dashboard visualization. The study proved the scalability of cloud monitoring but noted that hardware complexity increased the system's cost.

4. Ali and Singh (2022) – Real-Time ATM Security Using Raspberry Pi

Ali and Singh (2022) implemented a Raspberry Pi-based ATM monitoring system integrating PIR motion sensors, cameras, and a gas sensor. The system could record real-time video and send cloud alerts during suspicious activity. Although it improved security, high power consumption and dependency on Wi-Fi were noted as limitations.

5. Kumar and Raj (2023) – Intelligent IoT Framework for ATM Protection

Kumar and Raj (2023) proposed an intelligent IoT-based ATM monitoring framework integrating multiple sensors and AI analytics. Their system performed pattern recognition on cloud data to identify unusual activity trends, improving predictive security measures. However, the framework required high computational resources and internet reliability for seamless operation.

III. EXISTING SYSTEM

The traditional ATM security systems primarily rely on CCTV cameras and manual inspection**.** These systems lack automation and real-time alert capabilities, making them inefficient during sudden break-ins or technical failures. Furthermore, conventional systems do not monitor environmental conditions like temperature, gas leaks, or fire hazards**.** Manual data collection and maintenance reports often result in delayed responses, increasing potential losses. The absence of an automated and cloud-integrated mechanism restricts authorities from obtaining instant notifications and analyzing system behavior remotely.

IV. PROPOSED SYSTEM

The proposed IoT-based ATM monitoring system integrates sensors, microcontrollers, and cloud platforms to enhance the safety and efficiency of ATM operations. The system employs NodeMCU (ESP8266) to interface with multiple sensors:

- **Vibration sensor** to detect physical tampering,
- **PIR motion sensor** to detect unauthorized human presence,
- **Gas and smoke sensor** to identify fire or smoke,
- **Temperature sensor** to detect overheating of ATM components.

All sensor data is transmitted to a cloud platform (ThingSpeak or AWS IoT) for real-time visualization and alert generation. If any abnormal activity is detected, alerts are sent to the security control center and bank officials through email or mobile notifications. Additionally, camera modules can be integrated to capture images during suspicious activity. This system not only ensures real-time monitoring but also data analytics for predictive maintenance and security assessment.

V. SYSTEM ARCHITECTURE

The system architecture consists of:

1. **Input Layer:** Sensors (PIR, gas, temperature, vibration) installed in the ATM booth.
2. **Processing Layer:** NodeMCU or Raspberry Pi processes data and communicates with the cloud.
3. **Cloud Layer:** Stores and visualizes sensor data in real time using ThingSpeak or Firebase.
4. **Alert Layer:** Sends notifications to authorities through SMS, email, or mobile app.

Received: 28-09-2025 | Accepted: 03-11-2025 | Published: 10-11-2025 | www.ajaccm.com

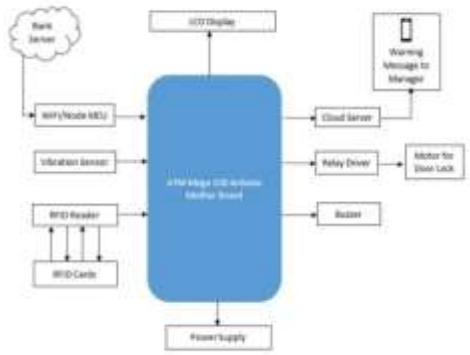

Fig.5.1: Block diagram for proposed model

NODE MCU:

NodeMCU is a low-cost open source IoT platform. It initially included firmware which runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which was based on the ESP-12 module.[6][7] Later, support for the ESP32 32-bit MCU was added

OVERVIEW:

NodeMCU is an open source firmware for which open source prototyping board designs are available. The name "NodeMCU" combines "node" and "MCU" (micro-controller unit).[8]. The term "NodeMCU" strictly speaking refers to the firmware rather than the associated development kits.[citation needed]

Both the firmware and prototyping board designs are open source.

The firmware uses the Lua scripting language. The firmware is based on the eLua project, and built on the Espressif Non-OS SDK for ESP8266. It uses many open source projects, such as lua-cjson[10] and SPIFFS.[11] Due to resource constraints, users need to select the modules relevant for their project and build a firmware tailored to their needs. Support for the 32-bit ESP32 has also been implemented.

The prototyping hardware typically used is a circuit board functioning as a dual in-line package (DIP) which integrates a USB controller with a smaller surface-mounted board containing the MCU and antenna. The choice of the DIP format allows for easy prototyping on breadboards. The design was initially was based on the ESP-12 module of the ESP8266, which is a Wi-Fi SoC integrated with a Tensilica Xtensa LX106 core, widely used in IoT applications

VI. IMPLEMENTATION

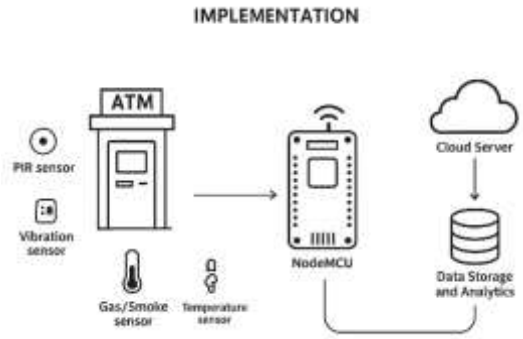

Fig.6.1: Implementation of proposed model

The IoT-based ATM Monitoring System using Cloud Data and Sensors is a connected solution that enhances security, reliability, and maintenance of ATM networks by continuously monitoring physical and operational parameters. Each ATM is equipped with sensors — including intruder/tamper sensors, vibration and shock detectors, temperature and humidity sensors, door-position switches, cash-dispense counters, and optional CCTV/video streams linked to an embedded gateway (e.g., NodeMCU, Raspberry Pi, or an industrial IoT modem). Sensor readings and event logs are securely transmitted over cellular or wired networks to a cloud platform where they are stored, analyzed, and visualized in real time. Cloud analytics detect anomalies (skimming attempts, forced entry, overheating, cash-out irregularities) and trigger automatic alerts to operations teams and law enforcement via SMS, email, or a mobile app; predictive maintenance algorithms also forecast component failures (e.g., dispenser jams or power-supply issues) to reduce downtime. Role-based dashboards provide branch managers and technicians with live status, historical reports, and incident trails, while end-to-end encryption, device authentication, and secure OTA update

mechanisms ensure system integrity and compliance with banking security standards.

VII. CONCLUSION

The IoT-based ATM monitoring system enhances security, safety, and operational reliability through real-time data acquisition and cloud integration. The proposed design offers continuous surveillance, instant alerts, and remote data access. It significantly reduces human dependency and response delay during emergencies like vandalism, overheating, or gas leaks. By integrating sensors and IoT analytics, the system ensures a cost-effective, scalable, and intelligent ATM monitoring solution adaptable to various banking environments.

VIII. FUTURE SCOPE

In future implementations, the system can be enhanced using:

- **AI-based video analytics** for face and behavior recognition.
- **Edge computing** to process alerts locally during internet outages.
- **Blockchain integration** for secure log storage and transaction validation.
- **Predictive analytics** for maintenance scheduling and anomaly detection.
- **Solar-powered modules** for sustainable and power-independent operation.

Such improvements will transform the ATM network into a self-learning, secure, and autonomous infrastructure for smart banking ecosystems.

IX. REFERENCES

[1] M. rule and Anita Julian, “Design and Implementation of Antitheft ATM Machine victimization Embedded Systems,” International Conference on Circuit, Power and Computing Technologies [ICCPCT], pp. 1 – 5, 2015

[2] Xiao Zhang, Lin Zhou, Tao Zhang, Jie Yang, “A Novel economical methodology for Abnormal Face Detection in ATM,” ICALIP, pp. 5 - 700, 2014

[3] I-Pin subgenus Chen, Li-Kui Liu, Wei-Wei Hong, “Image process based mostly stealer proof System victimization Silhouette Image,” ICMT, pp. 6394 – 6397, 2011

[4] Hiroshi Sako, Takashi Watanabe, HirotoNagayoshi, and Tatsuhiko Kagehiro, “Self-Defense-Technologies for automatic teller machine Machines,” International Machine Vision and Image process Conference IMVIP, pp. 177 – 184, 2007.

[5] Che-Yen cyst, Shih-Hsuan Chiu, Jiun-Jian Liaw, ChuawPin Lu, “The safety helmet detection for ATM’s closed-circuit television via the changed Hough rework,” International Carnahan Conference Security Technology, Proceedings IEEE thirty-seventh Annual 2003, pp. 364 – 369, 2003

[6] F. Puente, J.D. Sandoval, P. Hernandez, C.J. Molina, “Improving on-line Banking Security with Hardware Devices,” thirty-ninth Annual International Carnahan Conference on Security Technology, CCST, pp. 174 – 177, 2005

[7] Yiping Tang, Zuling He, Yaoyu Chen, Jinyi Wu, “ATM Intelligent police work supported Omni-directional Vision,” WRI World Congress on engineering science and Knowledge Engineering, pp. 660 – 664, 2009

[8] R. Ashok Rajan, R. Angelinjosphia, Ms.PVS.Gayathri, T. Rajendran, P. Anandhakumar, “A Novel Approach for Secure ATM Transactions victimization Fingerprint Watermarking,” Fifth International Conference on Advanced Computing (ICOAC), pp. 547 – 552, 2013

[9] H. Lasisi and A.A. Ajisafe, “Development of Stripe Biometric based mostly Fingerprint Authentications Systems in automatic teller machine Machines,” ordinal International Conference on Advances in process Tools for Engineering Applications (ACTEA), pp. 172 – 175 2013.

Received: 28-09-2025 | Accepted: 03-11-2025 | Published: 10-11-2025 | www.ajaccm.com