PROJECT ABSTRACT

IoT ATM Security Monitor using Vibration Sensor

An ESP32-based ATM tamper monitor: SW-420 vibration sensing with confirmed-event logic, reed-switch door input, local buzzer/strobe deterrent, Telegram/MQTT alerts and a severity-graded event-log dashboard. Delivered built-to-order with prototype, firmware, dashboard, report, PPT and viva kit.

01. Title

IoT ATM Security Monitor using Vibration Sensor

02. Introduction / Background

ATMs hold cash in public, often unguarded spaces, and physical attacks — drilling, cutting, gas explosions, ram-raiding — keep evolving. Guards and CCTV record what happened; they rarely stop it happening. A low-cost sensor layer that reacts the instant the machine body is attacked changes the equation: a vibration event can trigger a local deterrent and a remote alert within seconds. The engineering is deliberately simple and robust — a vibration switch with adjustable threshold, a door-tamper input, an ESP32 to judge and report, and a buzzer plus strobe for the local response. This project builds the complete monitor: the SW-420 sensing chain with a buyer-run sensitivity tuning procedure, confirmed-event logic that rejects single knocks, Telegram and MQTT alerting, a dashboard with a severity-graded event log, and arm/disarm plus service mode.

03. Problem Statement

Existing ATM protection is mostly passive recording. The project addresses the detection gap with a demonstrable IoT tamper monitor: vibration sensing on the machine body with confirmed-event logic, an independent door-tamper channel, an immediate local deterrent, instant remote alerts with timestamps, and a dashboard log — showing the full sense-judge-alert loop on a model ATM rig with honest notes on threshold tuning and limits.

04. Objectives

- Detect attack-class vibration with an SW-420 module and adjustable sensitivity.
- Reject isolated knocks with confirmed-event logic (repeated triggers in a time window).

- Monitor the service door independently with a reed switch.
- Fire a local buzzer and strobe LED deterrent on confirmed events, offline-capable.
- Push instant Telegram and MQTT alerts with event type, severity and timestamp.
- Render a severity-graded, timestamped event log with arm/disarm controls on a dashboard.
- Provide a buyer-run knock-test tuning procedure for the vibration threshold.
- Deliver the complete student kit: prototype, firmware, dashboard, report, PPT and viva Q&A.

05. Proposed Methodology

The system has three parts. (1) Sensing: the SW-420 on the machine body and the reed switch on the service door are sampled continuously by the ESP32. (2) Decision: a vibration trigger opens a confirmation window; only repeated triggers inside it escalate to a confirmed attack, firing the buzzer and strobe and queuing remote alerts, while isolated knocks log as minor. (3) Reporting: events publish over MQTT and through a Telegram bot; the dashboard keeps the severity-graded log with arm/disarm and service mode. The student tunes sensitivity with the knock-test procedure on their own rig.

06. System Architecture / Working

The ESP32 samples both sensor channels continuously. A vibration trigger starts the confirmation window; on confirmation the buzzer and strobe fire immediately and the event — type, severity, timestamp, channel — is published over MQTT and sent via the Telegram bot. The dashboard appends it to the log and updates the machine status card. Arm/disarm commands from the dashboard change state; service mode suspends vibration alarms during maintenance while door monitoring stays active. Local outputs and event buffering never depend on Wi-Fi.

07. Hardware / Software Requirements

- ESP32 development board (Wi-Fi)
- SW-420 vibration sensor module with sensitivity adjustment
- Reed switch for door-tamper sensing
- Buzzer and strobe LED
- Telegram bot plus MQTT broker
- Web dashboard (status, event log, controls)
- 5 V adapter with battery backup
- Arduino IDE (C/C++ firmware)

08. Expected Outcomes

- A working tamper monitor distinguishing confirmed attacks from isolated knocks.

- Immediate local deterrent plus timestamped remote alerts on confirmed events.
- A severity-graded event log with arm/disarm and service-mode history.
- A documented sensitivity-tuning procedure with measured false-trigger notes.
- A complete report, PPT and viva Q&A on vibration sensing, event logic and IoT alerting.

09. Applications

- Demonstrating physical-security IoT concepts for ATM and kiosk protection studies.
- Teaching threshold sensing, event-confirmation logic and multi-channel alerting.
- Prototyping tamper-alert ideas for remote equipment shelters and cabinets.

10. Future Scope

- GSM fallback alerting for sites without Wi-Fi.
- Camera snapshot capture on confirmed events.
- Multi-ATM fleet view with per-machine status.
- Accelerometer-based intensity grading as a sensor upgrade.