Project Brief: IoT-Based Server Room Monitoring and Access Control System

Project Overview

The Smart Server Room Monitoring and Access Control System is an IoT-based solution designed to enhance security and access management in a server room. The system integrates intrusion detection, video surveillance, and RFID-based access control, ensuring that only authorised personnel can enter. In the event of unauthorised access, the system will send real-time alerts to administrators via a dedicated Android application.

Key Features

1. Access Control

RFID-based authentication: Users must scan an RFID tag to gain access.

User roles and permissions: Different access levels (e.g., admin, IT staff, maintenance).

Logging and tracking: Record each access attempt with timestamps.

1. Intrusion Detection & Alerts

PIR Motion Sensors: Detect movement within the server room when unauthorised.

Door & Window Sensors: Alerts if forced entry is detected.

Android App Notifications: Immediate alerts to administrators upon intrusion.

SMS & Email Alerts: Backup notifications in case of app failure.

1. Video Surveillance & Logging

IP Camera Integration: Captures live footage when motion is detected.

Cloud Storage: Saves video clips of detected intrusions for future review.

Mobile App Live Feed: Admins can remotely monitor the server room in real time.

1. Environmental Monitoring

Temperature & Humidity Sensors: Monitors climate conditions in the server room.

Fire/Smoke Detection: Alerts in the event of a fire breakout.

Cooling System Control: Triggers an alert when temperatures exceed safe thresholds.

System Architecture

The system will consist of the following components:

Microcontroller/Gateway: Raspberry Pi / ESP32 for processing sensor data.

RFID Module: To handle access control.

CCTV/IP Cameras: For video surveillance.

Mobile Application: For real-time alerts and remote monitoring.

Database & Cloud Services: To store logs, video footage, and access records.

Additional Features (Optional Enhancements)

Facial Recognition: Instead of RFID, access could be granted based on facial authentication.

AI-based Anomaly Detection: Detect suspicious behaviour using machine learning.

Remote Locking System: Admins can lock/unlock the door remotely via the app.

Energy Monitoring: Track power consumption of the server room.

Development Roadmap

Phase 1: Research & Hardware Selection – Select microcontroller, sensors, and communication protocols.

Phase 2: Hardware Integration – Set up access control, video surveillance, and intrusion detection.

Phase 3: Software Development – Develop mobile app and cloud backend.

Phase 4: Testing & Security Hardening – Simulate attacks and enhance system robustness.

Phase 5: Deployment & Optimisation – Deploy and fine-tune for performance.