SMART SECURE BANK SYSTEM

ORGANIZATION PROJECT

- Mennatallah Gamal Mohamed Abdelfatah
- Mariam Nader Farouk Tadros
- Manal Ali Abdallah Elsayed
- Naira Ibrahim Eldosoky mohamed Ahmed
- Shrouk Abdelraheem Abdallah Bahy

Superwised by:

DR. SHAIMAA NABIL

INTRODUCTION

Banks face constant threats from theft, unauthorized access, and emergencies, yet traditional security systems often lack real-time monitoring and rapid response capabilities. The Smart Bank Security System using ESP32 addresses these challenges by integrating multiple sensors (fire, smoke, DHT11 and IR) and secure keypad access into a unified IoT platform. Powered by the ESP32 microcontroller, the system enables remote supervision, instant alerts, and automated security protocols for critical areas such as counters, employee zones, and vaults. With distinct Day and Night operating modes, this solution enhances security, reduces manual oversight, and ensures swift action against potential breaches.

ABSTRACT

This project designs a hardware-based security system for banks using the ESP32 microcontroller integrated with multiple sensors (fire, smoke, IR, DHT11), a keypad, an LCD and Buzzer, and a simple website for real-time monitoring. The system aims to enhance bank security by:

- Monitoring environmental hazards (fire, smoke, temperature, humidity)
- Detecting unauthorized access (using IR sensors for motion detection)
- Implementing secure access control (via a keypad-based PIN system)
- Providing real-time alerts (A buzzer and LCD provide on-site alerts, while a website displays real-time sensor data remotely. The system processes sensor inputs, performs computations)

MOTIVATION

CONSTANT SECURITY THREATS

UNAUTHORIZED ACCESS

(theft, break-ins)

FIRE HAZARDS

(electrical faults, arson)

ENVIRONMENTAL RISKS

(high temperature/humidity damaging equipment)

VISION STATEMENT

FIRE & SMOKE DETECTION

Immediate alerts using flame & smoke sensors.

ACCESS CONTROL

Keypad-based PIN entry (more secure than keycards).

INTRUSION DETECTION

IR sensors detect unauthorized movement.

ENVIRONMENTAL MONITORING

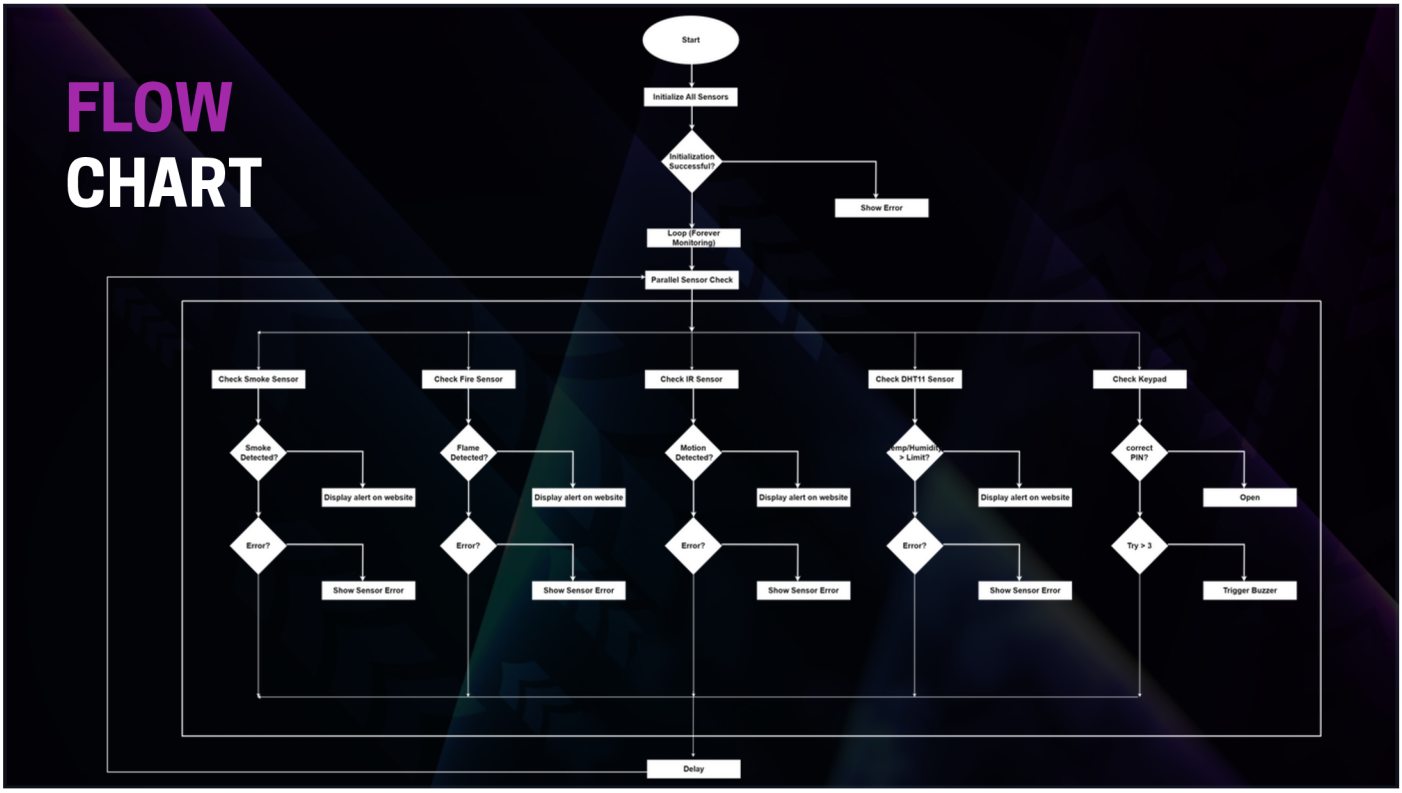
DHT11 tracks temperature/humidity to prevent equipment damage.

REAL-TIME ALERTS

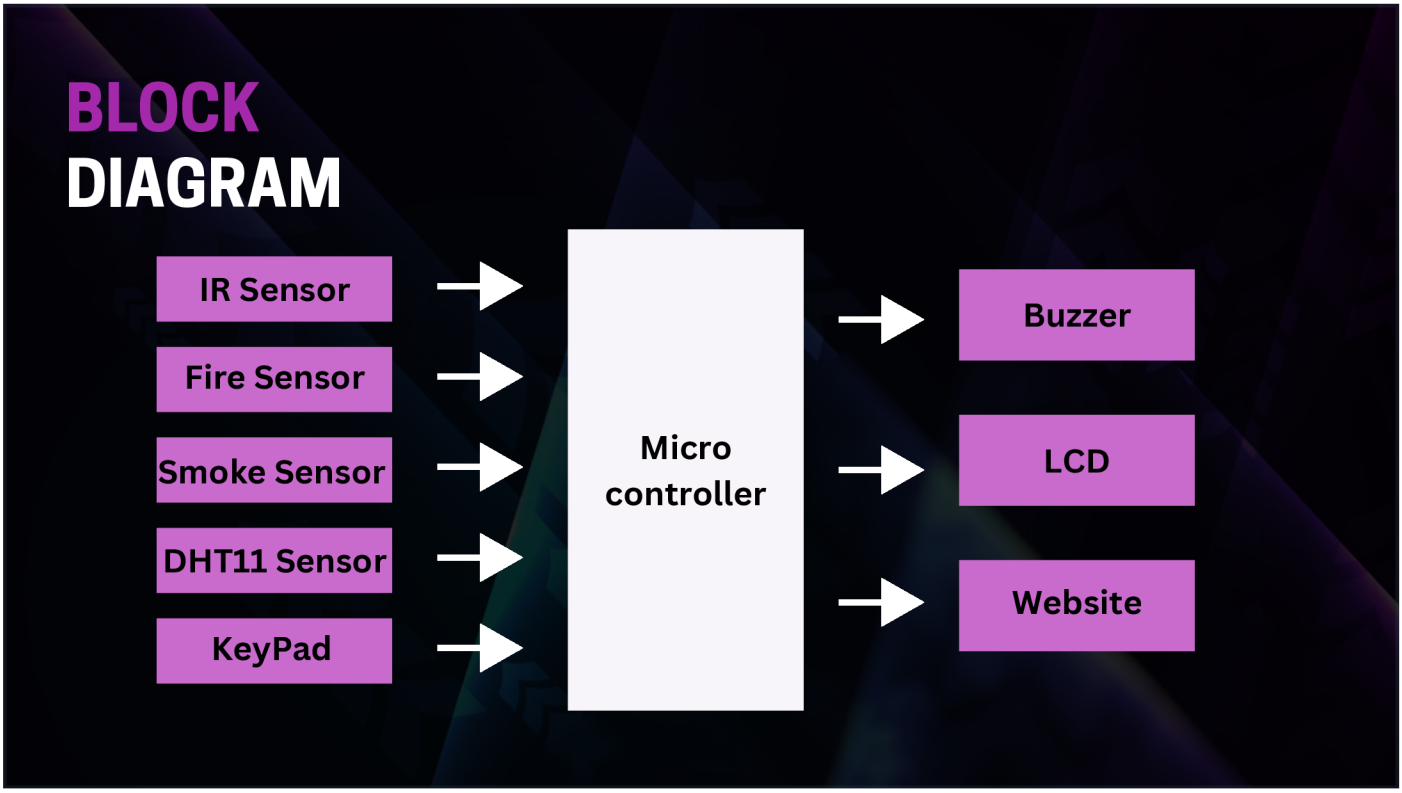
LCD display + Wi-Fi notifications (via ESP32).


IR SENSOR
Detect Motion
SMOKE SENSOR
Detect Smoke
DHT11
Tempreture & Humidity
FIRE SENSOR
Detect Fire
KEYBAD
Enter Password
LCD
Show Password
ESP32
Controle all
BUZZER
give alert
HARDWARE
In The System

FLOW CHART


Start
Initialize All Sensors
Initialization Successful?
Show Error
Loop (Forever Monitoring)
Parallel Sensor Check
Check Smoke Sensor
Check Fire Sensor
Check IR Sensor
Check DHT11 Sensor
Check Keypad
Smoke Detected?
Flame Detected?
Motion Detected?
> Limit?
correct PIN?
Display alert on website
Display alert on website
Display alert on website
Display alert on website
Open
Error?
Error?
Error?
Error?
Try > 3
Show Sensor Error
Show Sensor Error
Show Sensor Error
Show Sensor Error
Trigger Buzzer
Delay

BLOCK DIAGRAM



RELATION
COURSE MATERIAL

Internal Memory Technology: The ESP32's SRAM stores sensor data and program variables, with error-checking mechanisms to ensure reliability.

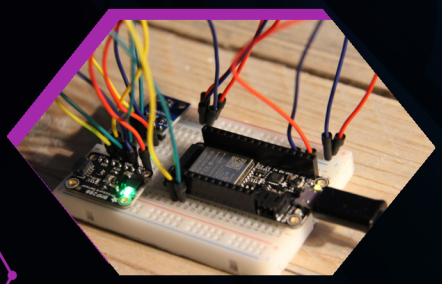
External Memory: Sensor logs could be stored on an SD card (future scope), leveraging magnetic/optical storage principles.

Input/Output: The system uses programmed I/O for keypad input and interrupt-driven I/O for sensor triggers, optimizing response times.

Computer Arithmetic: Integer comparisons (e.g., PIN validation) and floating-point calculations (e.g., temperature thresholds) are central to system logic.

Processor Structure and Function: The ESP32's dual-core processor and register organization enable efficient instruction pipelining for real-time processing.

ADVANTAGES
OF USING ESP32



High Performance: Dual-core 32-bit CPU at 240 MHz and approximately 520 KB of SRAM enable complex tasks and multitasking under FreeRTOS.

Integrated Wireless: On-board Wi-Fi and Bluetooth support reduces BOM and simplifies IoT integration .

Rich I/O & Peripherals: Abundant GPIOs, ADC channels, capacitive touch sensors, hardware PWM, and multiple serial interfaces .

Low Cost: ESP32 dev-boards are available for around USD 6, offering strong performance per dollar.

Extensible Ecosystem: Compatible with Arduino IDE, PlatformIO, and Espressif's ESP-IDF, backed by an active community .

PAPER(1)

REFRENCE

DESCRIPTION	ANALYSIS	ADVANTAGES	DISADVANTAGES	DESIGN & IMPLEMENTATION
• An access-control system using dual authentication: voice recognition and RFID card. Designed as a low-cost automated replacement for mechanical locks in small/medium offices. • Opens the door automatically upon identity verification. • The aim of this developed system is to restrict the access of an office/location using Radio Frequency Identification (RFID) and voice recognition authentication, thus offering security to the lives and properties of people.	**Hardware:** • Arduino Uno • RFID reader (RC522) + active tags (~200 mm read range)· • Voice-recognition module(5 V; Tx→D2,Rx→D3) • PIR motion sensor → D7 on Arduino • 16x2 LCD via 12C (SCL→A5, SDA→ A4) • Solenoid lock + relay + servo • motor to open door for 5s • Power: SMPS 12 V • buck converter to 5 V • +12 V rechargeable battery backup authentication to increases security.	• Prevents unauthorized access, thereby safeguarding lives and property. • Automates authentication (recognition, authorization), ensuring complete protection. • Simplifies entry for authorized personnel and eliminates the need for security guards. • Reduces data breaches and theft by granting access only to trusted users • Eliminates carrying multiple physical keys—RFID tags work non-line-of-sight and can be read in bulk • Voice biometrics are unique to each individual and cannot be stolen • Dual-factor design provides a secure RFID fallback when voice recognition is impaired	• Voice recognition is unreliable in noisy environments or when the user is ill • RFID cards can be easily lost or stolen • RFID has a short read range (~20 cm), requiring close proximity • PIR sensor may trigger falsely due to pets or heat sources • No internal memory or database to log access events • Lacks multi-factor fallback (e.g. no PIN or fingerprint option) • Arduino lacks built-in Wi-Fi or memory—ESP32 could offer better storage, wireless logging, and expansion options	• Startup: LCD shows • ACCESS CONTROL SYSTEM AUTHENTICATED BY RFID AND VOICE RECOGNITION • Motion detected (PIR): LCD → “WELCOME” then “SPEAK” • Voice verification: • If match → LCD “ACCESS GRANTED” / “WELCOME, USER”; energize relay → solenoid unlocks → servo opens door • Else → LCD “SWIPE CARD” • RFID verification: reader scans tag (≤200 mm) via serial link • If UID match → LCD “ACCESS GRANTED” / “WELCOME, USER”; unlock and open as above • If no match → LCD “ACCESS NOT GRANTED”; door remains locked • Auto-close: servo shuts door after 5 seconds

PAPER(2)

REFRENCE

DESCRIPTION	ANALYSIS	ADVANTAGES	DISADVANTAGES	DESIGN & IMPLEMENTATION
• A smart locker security solution using loT + Machine Learning+ Cloud. • Combines biometric (face + fingerprint) and traditional (PIN) authentication. • Uses image processing techniques like Viola-Jones and Gabor Filters. • Sends real-time alerts via Telegram & SMS. • Integrated with safety sensors (fire/smoke).	**Hardware:** • Arduino Uno, LCD, R305 Fingerprint Scanner. • PIR, Fire/Smoke Sensors, Camera. • Buzzer, WiFi Module. • Software: • Face recognition (OpenCV + Haar). • Fingerprint authentication, OTP via Telegram. • Image matching uses GLCM(texture analysis) and HOG (feature orientation). • Smart decision logic for access validation. • Buzzer and message alert for unauthorized attempts. • monitoring through loud + logging system.	• Multi-layered security using face recognition + fingerprint + PIN/ OTP. • Real-time alerts through Telegram/SMS in case of unauthorized access. • Highly accurate face detection using OpenCV, Haar Classifier, and Gabor filters.-Suitable for home, bank, and enterprise environments. • Cloud-based storage and real-time image Comparison. • Eliminates physical keys, reducing risk of loss or duplication. • Cost-effective and scalable for various security setups. • Can be used by visually impaired individuals since iris remains unaffected. • Uses human-vision-like algorithms (Gabor filters) to enhance recognition accuracy even with slight image differences.	• System relies on stable internet for real-time cloud access and alerts. • False positives/negatives possible in facial recognition due to lighting, angles. • Fingerprint sensor may fail with wet/dirty fingers. • Needs clean facial dataset in cloud for accuracy. • Telegram/SMS alerts may not be received if network is down. • Not ideal for rugged industrial use without adaptation.	• System activates sensors and Arduino Uno at startup. • PIR sensor detects motion; camera captures the intruder's image. • Captured face is compared with cloud-stored images using Haar Classifier. • If face matches, fingerprint verification is requested via R305 sensor. • If both are verified, the locker unlocks. • If not, Telegram alert is sent, and OTP or password is required. • Buzzer is triggered for unauthorized attempts. • Fire and smoke sensors monitor environment and send alerts. • All events are logged in the cloud.

PAPER(3)

REFRENCE

DESCRIPTION	ANALYSIS	ADVANTAGES	DISADVANTAGES	DESIGN & IMPLEMENTATION
The Smart Bank Security System using ESP32 is an IoT-based project that provides intelligent surveillance and real-time monitoring for a bank setup. It utilizes the ESP32 microcontroller, multiple sensors, and a web-based dashboard to detect breaches and send alerts. The system operates in two modes: **Day Mode:** Normal operation with restricted access to the vault via a PIN-authenticated keypad. **Night Mode:** Full lockdown; any unauthorized entry triggers alerts.	This system simulates a secure environment using multiple sensors to monitor different areas (Counter, Employee, Vault). It demonstrates how IoT and microcontrollers like the ESP32 can be effectively used in real-time security systems. Key features: • Web-based monitoring via ESP32 WebServer • PIN authentication using 4x4 Keypad for vault access • Visual alerts using an I2C LCD • Mode switching (Day/Night) to adapt security levels	Real-Time Monitoring: Data is uploaded instantly to the server interface. Internet Connectivity: ESP32 enables remote alerts and web interface. Modular Design: Different sections (Vault, Employee, Counter) can be customized. **Interactive UI**: Web interface and LCD provide a user-friendly experience. **Secure Access:** Vault protected with PIN authentication.	**Limited to Local WiFi:** System depends on the WiFi range of the ESP32. Basic Authentication: PIN system is vulnerable without encryption. **Single-point Failure:** ESP32 failure would halt the entire system. **No Database:** Data is not stored or logged permanently.	**System Design:** • ESP32 acts as the brain, collecting sensor data and controlling modules. • IR Sensors monitor physical presence or breaches at key entry points. • Fire and Smoke Sensors provide safety alerts. • 4x4 Keypad is used for user authentication for vault access. • I2C LCD displays status messages (e.g., vault status, alerts). • Web Server hosted on ESP32 shows real-time sensor data and control buttons for Day/Night modes

PAPER(4)

REFRENCE

DESCRIPTION	ANALYSIS	ADVANTAGES	DISADVANTAGES	DESIGN & IMPLEMENTATION
The paper proposes an IoT-based multi-layered bank security system It aims to replace conventional security with a cost-effective, automated solution for small/medium banks.	**Hardware:** • Microcontrollers: Arduino Uno (logic), NodeMCU (Wi-Fi). • Sensors: IR, ultrasonic, PIR (motion/temperature). • Cameras: ESP32 module (live video + OpenCV for face detection). • Authentication: Fingerprint sensor (R307), RFID (RC522). • Actuators: Servo (door control), buzzer, LED. • Power: 230V to 5V converter (transformer + rectifier + regulator). • Software: • Arduino IDE (C++ for firmware). • Lua/Python (NodeMCU scripting).	• Multi-layered security: Combines biometrics, sensors, and cameras. • Real-time monitoring: ESP32 streams video to a web server. • Scalability: Modular design (supports additional sensors). • Cost-effective: Uses affordable components (Arduino) • Remote alerts: Notifications via email/SMS .	• Limited range: IR/ultrasonic sensors work only within short distances. • Power dependency: Requires stable 5V supply. • Complexity: Integration of multiple protocols (SPI, I2C, UART). • False alarms: Environmental factors (e.g., heat) may trigger PIR sensors	**Access Control:** Employees authenticate via fingerprint/RFID/keypad. Servo unlocks doors upon validation. **Intrusion Detection:** IR/ultrasonic sensors detect unauthorized entry → trigger buzzer/LED. PIR monitors motion in restricted areas. **Surveillance:** ESP32 camera captures live footage; motion detection alerts security. OpenCV processes images for facial recognition. **Microcontrollers:** Arduino interfaces with sensors (I2C/SPI) and LCD. NodeMCU handles Wi-Fi (connects to Cayenne IoT for cloud logging).

PAPER(5)

REFRENCE

DESCRIPTION	TECH/ANALYSIS	ADVANTAGES	DISADVANTAGES	DESIGN & IMPLEMENTATION
The Smart Banking Security System enhances bank locker security using advanced technologies like Face Recognition, RFID, GSM, and sensors. It ensures only authorized individuals can access lockers.	• Face Recognition: Biometric identification to verify user identity. • RFID: User authentication through RFID tags. • GSM: Sends alerts to the bank manager for unauthorized access. • Sensors: Vibration and temperature sensors detect security breaches. • User Authentication: Users present RFID tags; face recognition captures and verifies identity. • Security Measures: Vibration and temperature sensors trigger alerts and a timer locks the locker if access exceeds a set duration. • Communication: GSM module sends alerts.	• Enhanced Security: Reduces unauthorized access risks. • Real-time Alerts: Immediate notifications improve response time. • User-Friendly: Minimal action needed for authorized users. • Cost-Effective: Reduces costs associated with theft.	• Technical Complexity: Integration of multiple technologies can complicate implementation. • False Positives/Negatives: Face recognition may inaccurately identify users. • Dependence on Technology: Reliability depends on proper functioning of components. • Privacy Concerns: Biometric data raises privacy issues.	• Block Diagram: Visual representation of system architecture. • Microcontroller Integration: Uses PIC and ARM microcontrollers for processing. • Software Development: Developed in Embedded C, programmed into microcontroller. • Testing and Calibration: Rigorous testing for sensor thresholds and performance metrics

PAPER(6)

REFRENCE

DESCRIPTION	ANALYSIS	ADVANTAGES	DISADVANTAGES	DESIGN & IMPLEMENTATION
A multi-layered security system for bank lockers combining RFID authentication, face recognition (Viola-Jones/PCA), GSM alerts, and sensors (vibration/temperature). Automatically locks after timeout.	• Flow: RFID → Face recognition → Access grant. • Sensors: Trigger GSM alerts for tampering/fire. • Hardware: PIC (RFID), ARM (face processing), SIM900A (GSM). • Software: MATLAB (image processing), Embedded C (microcontrollers).	• Enhanced Security: Dual authentication (RFID + biometrics). • Real-time Alerts: GSM notifies manager during breaches. • Cost-Effective: Uses off-the-shelf components. • Automation: Timer limits access duration.	• RFID Vulnerability: Lost/stolen tags risk unauthorized access. • Lighting Dependence: Face recognition may fail in low light. • False Alarms: Sensors sensitive to environmental noise. • Power Reliance: System fails during outages.	• RFID Reader: PIC microcontroller (serial communication). • Camera: Face capture → MATLAB processing → ARM verification. • Sensors: Vibration/temperature thresholds trigger GSM via ARM. • Timer: Auto-lock via PIC/ARM.

PAPER(7)

REFRENCE

DESCRIPTION	ANALYSIS	ADVANTAGES	DISADVANTAGES	DESIGN & IMPLEMENTATION
This IoT-based system monitors industrial processes in small-scale industries using the ESP32-Dev module. It integrates sensors (DHT11 for temperature/humidity, flame, smoke) to track environmental parameters. Data is uploaded to the Cayenne cloud platform and monitored via the Blynk app on smartphones or PCs. If sensor values exceed predefined thresholds, the system triggers automated actions (e.g., stopping a DC motor, activating cooling fans) and sends SMS/email alerts to enhance safety and prevent accidents like fires.	The system leverages ESP32's built-in Wi-Fi for cloud connectivity, offering a cost-effective alternative to complex SCADA systems. It monitors multiple parameters (temperature, humidity, gas, fire), surpassing ZigBee/Bluetooth systems limited by range and data rate. However, scalability for large industries is unclear, and internet dependency poses risks in unstable network areas. Security measures for cloud data are not thoroughly addressed, and sensor response times (e.g., smoke sensor ~20 seconds) may limit critical applications.	• Cost-effective with affordable ESP32 and open-source Blynk/Cayenne platforms. • Enables remote monitoring and control, reducing on-site personnel needs. • Enhances safety with real-time SMS/email alerts for hazards like fires. • Wireless design eliminates long wiring, simplifying installation. • Energy-efficient automation optimizes industrial processes.	• Relies on stable internet, limiting use in remote areas. • Limited scalability for large-scale industrial applications. • Sensor constraints (e.g., flame sensor range ~100 cm, smoke sensor delay) may affect performance. • Lacks detailed cybersecurity protocols for cloud communication. • Requires regular sensor calibration, increasing maintenance.	• Hardware: ESP32-Dev module, DHT11 (temperature/humidity), flame sensor (760–1100 nm), smoke sensor, DC motor, 4-channel relay, buzzer. • Software: Blynk app, Cayenne project builder, Arduino IDE, Tuniot (visual programming). • Process: Sensors interface with ESP32, sending data to Cayenne cloud via Wi-Fi. Blynk app/PC dashboards display real-time data. Thresholds trigger relays (e.g., motor stop) and alerts (SMS/email). Tested for fire detection and motor control, ensuring accurate operation and safety responses.

PAPER(8)

REFRENCE

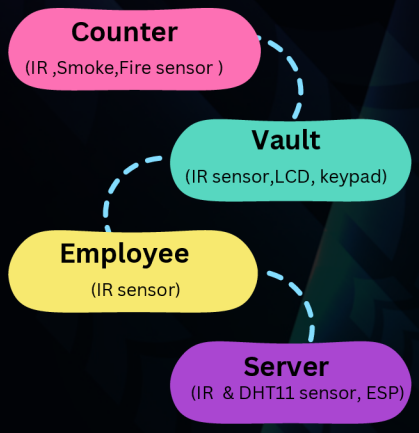
DESCRIPTION	ANALYSIS	ADVANTAGES	DISADVANTAGES	DESIGN & IMPLEMENTATION
This IoT-based environmental monitoring system uses the ESP32 microcontroller to measure air temperature, humidity, carbon monoxide (CO), and air quality (e.g., ammonia, benzene, smoke) via DHT11, MQ-7, and MQ-135 sensors. Data is transmitted to the Blynk cloud platform for real-time visualization on mobile apps or web interfaces. The system supports user-defined thresholds for alerts and is low-power, suitable for battery/solar operation in applications like smart cities, precision agriculture, and industrial monitoring. It was tested alongside a commercial station, proving	The system provides a cost-effective, scalable alternative to commercial environmental monitoring systems, focusing on air quality parameters absent in industrial-focused systems. The ESP32's Wi-Fi and low-power design enhance deployment flexibility. However, the DHT11 sensor is less accurate than alternatives (e.g., DHT22), and the MQ-135's inability to distinguish specific gases requires calibration. Internet dependency and unaddressed security concerns (e.g., data encryption) limit reliability in critical applications.	• Low-cost with affordable ESP32 and open-source Blynk platform. • Real-time remote monitoring with customizable Blynk dashboards. • Scalable for diverse applications (e.g., agriculture, smart cities). • Low-power design supports battery/solar operation. • User-friendly alerts enhance responsiveness to environmental changes. • Portable with OLED display for local data visualization.	• DHT11's lower accuracy and MQ-135's lack of gas specificity reduce precision. • Internet dependency hinders use in areas with poor connectivity. • Security measures for cloud data are not detailed. • Lacks automated actuation (e.g., relays), limiting control capabilities. • Sensors require regular calibration, adding maintenance effort.	• Hardware: ESP32, DHT11 (temperature/humidity), MQ-7 (CO), MQ-135 (air quality), OLED display, buzzer, LEDs. • Software: Blynk platform, likely Arduino IDE for firmware. • Process: ESP32 reads sensor data periodically, transmitting it to Blynk cloud via Wi-Fi. Blynk dashboards display real-time data (e.g., temperature graphs, gas levels). Thresholds trigger buzzer/LED alerts and notifications. OLED shows local data. Tested against a commercial station, confirming accuracy and scalability for environmental monitoring.

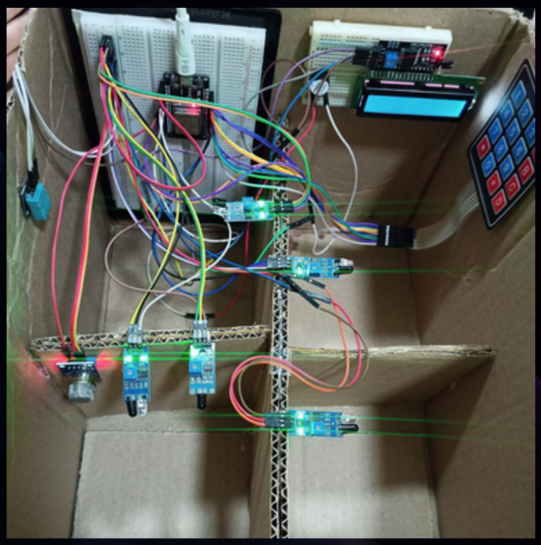
PAPER(7)

REFRENCE

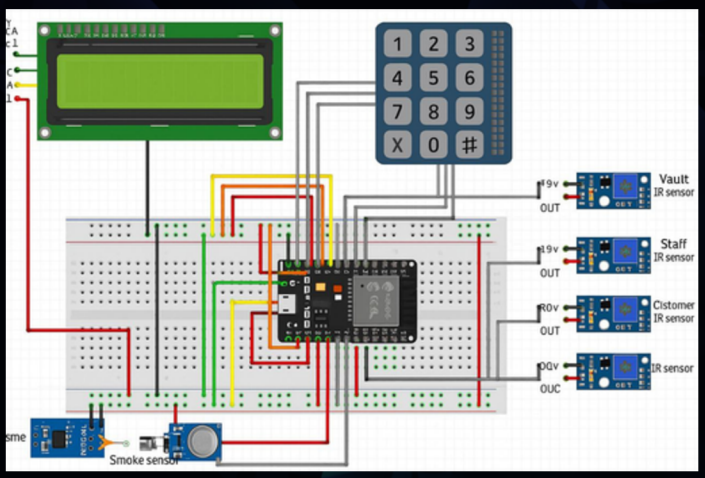
DESCRIPTION	ANALYSIS	ADVANTAGES	DISADVANTAGES	DESIGN & IMPLEMENTATION
This IoT-based bank security system enhances locker room protection using the ESP32 microcontroller. It employs the EM-18 RFID reader for card authentication, IR sensors for motion detection, and voice control for secondary verification. The Blynk app provides remote monitoring of locker status (open/closed) and sends alerts for unauthorized access. A 16x2 LCD displays status, and a buzzer sounds during operations or alerts. Designed for banks and secure environments, it ensures only authorized access and logs user activity.	The system's multi-factor authentication (RFID + voice) offers stronger security than traditional locks or single-factor systems, with Blynk enabling remote oversight. It surpasses GSM-based systems by integrating IoT and voice control. However, voice control reliability is unclear due to missing implementation details, and RFID systems risk spoofing without robust encryption. Wi-Fi dependency and untested scalability for large banking networks are concerns, as is the lack of cybersecurity specifics.	• Multi-factor authentication (RFID + voice) ensures high security. • Cost-effective with low-cost ESP32, passive RFID, and Blynk. • Remote monitoring via Blynk app enhances oversight. • Compact, low-power, and standalone for easy deployment. • Logs user access for audits; buzzer/LCD provide local feedback. • IR sensors optimize scanner operation, saving power.	• Wi-Fi dependency limits use in poor network areas. • Voice control reliability and implementation unclear. • RFID spoofing and lack of encryption details pose security risks. • Scalability for large-scale banking untested. • Maintenance needed for RFID cards and sensors. • Single-point failure risk if ESP32/RFID reader malfunctions.	• Hardware: ESP32 DevKit V1, EM-18 RFID reader (125 kHz), passive RFID cards, IR sensors, 16x2 LCD, buzzer. • Software: Blynk app, Arduino IDE with Blynk library. • Process: IR sensors detect motion, activating RFID scanner. Valid RFID card prompts voice authentication; correct inputs open locker. Blynk app shows status (IN/OUT with green/red indicators), sends alerts. LCD displays card ID/status; buzzer sounds for operations/alerts. Tested for authentication and door control, ensuring secure access and real-time monitoring.

SECTIONS
OUR SYSTEM



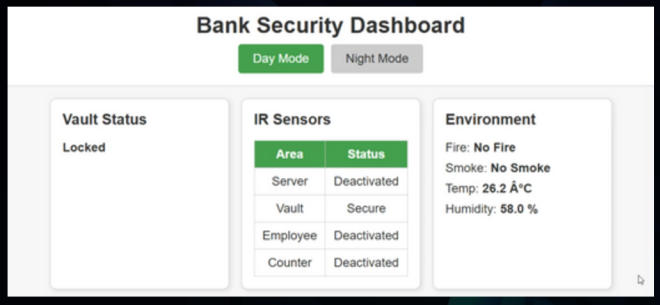


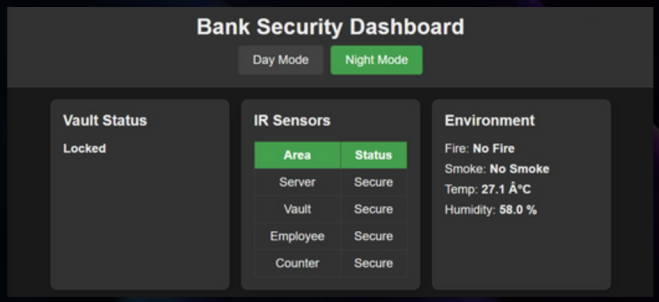
ESP32 PINS



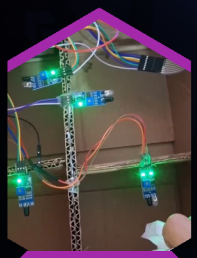
D2 → Buzzer
D4 → Server IR
D5 → DHT11
D18 → Smoke sensor
D19 → Vault IR
D21 → SDA
D22 → SCL
D23 → Fire Sensor
D13 → Row1
D12 → Row2
D14 → Row3
D27 → Row4
D26 → Column1
D25 → Column2
D33 → Column3
D32 → Column4
D35 → Employee IR
D34 → Counter IP

WEBSITE
OUR SYSTEM



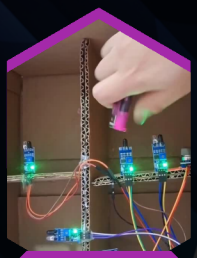


TEST
COMPONENTS



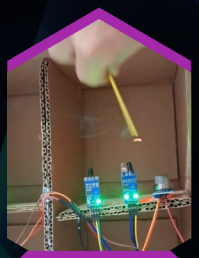
IR SENSOR

video



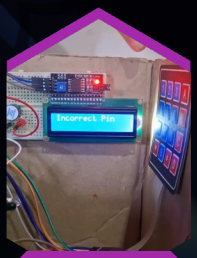
FIRE SENSOR

video



SMOKE SENSOR

video

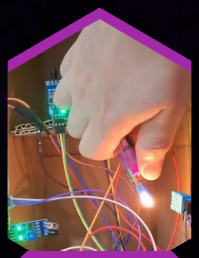


KEYBAD & LCD

video

BUZZER

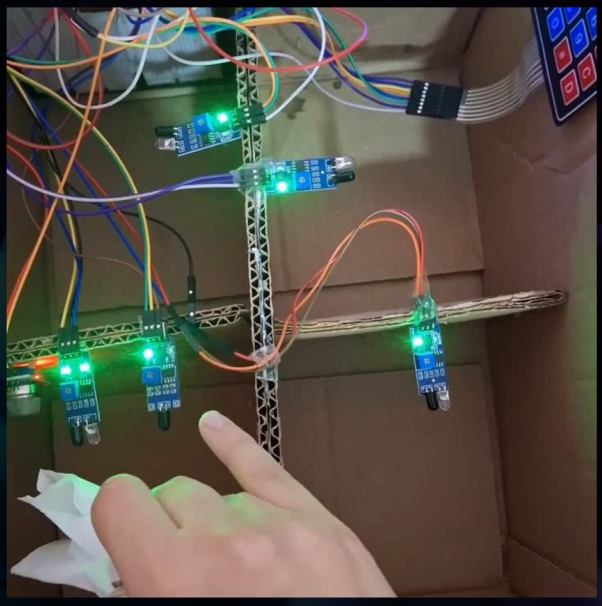
video



DHT11

video

FINAL video RESULT

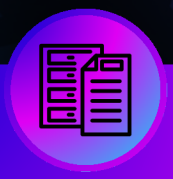


QR CODE

Challenges
OF OUR SYSTEM

Power Supply Reliability

Continuous power is needed for the system to function effectively. In areas with power instability, this can be a major concern unless a battery backup is included.



No Local Storage:

Without an SD card or external memory module, the system may not store past logs locally if internet/cloud fails.

No Redundancy Mechanism

If a component like a sensor or ESP32 board fails, there might not be a backup system in place unless specifically implemented.


CONCLUSTION
This project successfully demonstrates the implementation of a smart and real-time bank security system using the ESP32 microcontroller and various sensors (fire, smoke, motion, temperature, and humidity). The system efficiently detects emergency situations and provides instant visual alerts via an LCD display. Throughout the development, we applied several concepts from the Organization course such as memory management, processor structure, input/output mechanisms, and computer arithmetic to build a reliable and responsive system. The project emphasizes the importance of real-time embedded systems in enhancing safety and security in critical environments like banks. It also highlights how low-cost and power-efficient hardware like the ESP32 can be used to create scalable and smart security solutions.

FUTURE WORK

microSD Logging: Add a cad slot for local storage of sensor events and video snapshots results in enabling offline audits and long-term record-keeping .

RFID-Based Multi-Factor Authentication: Integrate an MFRC522 so users must present both a registered card and a fingerprint or PIN result in raising security by layering credentials.

Cellular Backup: Use a SIM800L or Notecard for SMS alerts and connectivity if Wi-Fi drops.

On-Device AI: Upgrade to an ESP32-S3/S3-CAM with ML face detection to reduce false alarms.

Secure Boot & Encryption: Enable Espressif's secure boot and flash encryption (or move to ESP32-H2).

Cloud & OTA: Connect via MQTT/HTTPS to AWS/Azure IoT for real-time dashboards and firmware updates.

Solar/UPS & Deep-Sleep: Implement solar/UPS power with intelligent deep-sleep scheduling for uninterrupted operation

REFERENCES

[1] M. A. Khan and S. A. Khan, "Door Access Control Using RFID and Voice Recognition System," ResearchGate, Mar. 2022.

[2] IoT Based Smart Bank Locker Security System Using Two-Way Authentication

[3] SMART BANK SECURITY SYSTEM USING EMBEDDED SYSTEM AND IOT, International Journal of Creative Research Thoughts (IJCRT), Vol. 11, No. 4, pp. 139–145, April 2023. https://ijcrt.org/papers/IJCRT2304139.pdf

[4] Smart Bank Locker Security System Using Biometric Fingerprint and GSM Technology https://drive.google.com/file/d/1oPMsotsNXeaPDzZize5I0DIdWw0mJYYM/view

[5] SMART BANKING SECURITY SYSTEM

[6] HQ Online, "Smart Bank Security System using ESP32," https://www.hqonline.com/blog/smart-bank-security-system-using-esp32

[7] R. Sharma and A. Patel, "Smart bank locker system using two-step authentication," in Proceedings of the 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, 2020, pp. 1–

[5].https://ieeexplore.ieee.org/document/9078655

[8] An IoT Based Bank Locker Security System, International Journal of Engineering Research & Technology (IJERT), Vol. 8, No. IS07, pp. 1–4, 2020. https://www.ijert.org/research/an-iot-based-bank-locker-security-system-IJERTCONV8IS07008.pdf

[9] P. K. Goyal, M. Giri, and S. Verma, "IoT-Based Smart Door Lock System with Face Recognition Using ESP32 CAM and Android App," in Lecture Notes in Electrical Engineering, vol. 1030, Singapore: Springer, 2024, pp. 365–376

[10] https://www.jetir.org/papers/JETIR2304A97.pdf

[11]. International Research Journal of Modernization in Engineering Technology and Science

[12] IOSR Journal of Electronics and Communication Engineering

[13] International Journal of Recent Technology and Engineering (IJRTE)


THANK YOU