

# Integration of RFID and Low-Cost IoT for Storeroom Monitoring: A Prototype Development Approach

Marliza Ramly, Muhammad Aminuddin Hasibuan Supirno

Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi,  
University Technical Malaysia Melaka, Malacca, Malaysia

DOI: <https://dx.doi.org/10.47772/IJRISS.2025.909000723>

Received: 27 September 2025; Accepted: 02 October 2025; Published: 28 October 2025

## ABSTRACT

The integration of the current storeroom monitoring system is a crucial solution to overcome the traditional storeroom management systems. It relies heavily on manual operations with minimal technological adoption, which may often lead to lack of adequate security measures and real-time monitoring. Therefore, it will be leaving valuable assets vulnerable to unauthorized access, stealing, and environmental hazards such as fire or extreme temperature fluctuations. This paper presents an integrated low-cost Internet of Things (IoT) for storeroom monitoring system designed to address these shortages by providing a comprehensive accessible solution for storeroom monitoring and security purposes. The proposed system is integrated with Radio-Frequency Identification (RFID) module for secure access control. It also included low-cost IoT devices such as MQ2 Smoke Gas Sensor for real-time fire and smoke detection and implemented with Closed-Circuit Television (CCTV) for live visual surveillance. The system architecture is centered around an ESP32 microcontroller, which processes data from the sensors and transmits it via Wi-Fi to the Blynk cloud platform, enabling real-time alerts and data visualization on a user's mobile device. A set of functionality tests were conducted using a black-box methodology to validate the performance of each component. The results demonstrated the system's effectiveness, with successful connectivity, accurate sensor readings, reliable access differentiation between authorized and unauthorized users, and seamless remote video streaming. This integrated IoT and RFID module shows to be an efficient solution for enhancing both the security and operational system.

**Keywords** - Internet of Things (IoT), RFID Access Control, Remote Surveillance Dashboard

## INTRODUCTION

The most common monitoring storeroom system management is relying on the significant of operational efficiency and asset protection for any storeroom users. These operations and protection provide more safety and environmental security. However, the traditional monitoring management operational methods [1], that often rely on manual key-based systems and periodic physical checking are tense to be vulnerable.

The traditional systems are inefficient, difficult to scale, and offer no real-time visibility in the storeroom's status. The owner of the storeroom is exposed to significant risks. The shortcomings of traditional storeroom management present numerous problems. It causes a high vulnerability to environmental fire hazards, where there are no automated early-warning systems being implemented. The lack of complete real-time monitoring frequently makes it easy to compromise reliance on physical risk access techniques. It keeps users unaware about important elements of any exposure. The urgent need for a cutting-edge, contemporary solution that can offer integrated, real-time monitoring for the conventional system is highlighted by this combination of risks.

The development of the monitoring system is to create and validate a system that addresses traditional monitoring problems. In this development main goal is to create a reliable smoke and fire detection system integrated with sensor technologies to give an immediate and accurate alert. A secure RFID-based access control system will be installed to record access events and stop any unauthorized entry to the system. The integration of CCTV cameras will then enable real-time remote monitoring and recording of all sorts of storeroom activity.

This paper is divided as follows. Section II presents a comprehensive literature review examining digital divide issues in fire detection system, IoT surveillance and Security, Automated Access Control, and comparative analysis of keys technologies of prior research study. Section III describes the system design, development process, and black box methodology, including the system architecture, and hardware component. Section IV presents implementing and monitoring testing results, which are inclusive of prototype implementation and testing protocol. Section V presents the result and discussions of findings for functionality of test result. Finally, Section VI concludes with key contributions and recommendations for future work in low-cost IoT storeroom monitoring system.

## **Related Work**

This section critically reviews existing research in the domains of fire detection, IoT-based surveillance, and automated access control. By analyzing prior work, this review identifies the current progressive, highlights technological gaps, and positions the unique contribution of the integrated system proposed in this study.

### **A. Fire Detection Systems**

The evolution of fire detection has moved from conventional alarms to more intelligent, sensor-based systems. Research by [3], [4], [5] provides a comprehensive review of traditional methods. These systems often had limitations such as slow response times and high false alarm rates, especially in dynamic or complex environments. Generally, the basic function of these systems needed human interaction to alert fire departments, which might lengthen response times and increase the possibility of danger [5]. The capacity of gas sensors to detect flames in their early stages have shown huge potential in detecting specific gases and compounds connected to early-stage fires, offering advantages over traditional smoke and temperature-based detection methods. These are a few important results [6], from recent research highlighting their effectiveness in detecting specific gases and compounds associated with early-stage fires and [6], [7] a comprehensive review of the fire detection. [8], [9] developed an IoT-based fire alarm system using temperature and smoke sensors to transmit data via GSM, demonstrating the feasibility of remote monitoring. Similarly, [10], proposed a fuzzy rule-based intelligent system to improve the accuracy of fire recognition and reduce false positives, showcasing the value of adding computational intelligence to detect hardware. These studies underscore the importance of multi-modal sensing and remote communication for effective fire safety, but often treat fire detection as an isolated system, separate from physical security infrastructure.

### **B. IoT Surveillance and Security**

Smart surveillance has become a cornerstone of modern security frameworks. The work of [11] presents a smart surveillance system using IoT and cloud computing to detect and monitor suspicious behavior in real-time, leveraging machine learning for object classification. [12], [13], [14] conducted a systematic survey on Arduino-based smart home security systems, analyzing the prevalence of motion sensors and various system architectures. Furthermore, [15] developed a real-time monitoring system using a Raspberry Pi and PIR sensor that sends email alerts upon detecting motion, though it lacked on-demand video access. These studies demonstrate a clear trend towards networked, intelligent surveillance, yet they predominantly focus on intrusion or motion detection, overlooking the integration with environmental hazard monitoring.

### **C. Automated Access Control**

Intelligent door systems [16], [17], [18] have advanced significantly with the integration of technologies like RFID. [19] proposed an automated door control system based on a smart camera that uses path analysis to predict user intent, thereby reducing unintended activity. A recent work by [20] explored a smart home system integrating RFID for security with SMS and email alerts. More recently, [21] developed an IoT enhanced smart door lock using RFID and Arduino to address more secure methods of locking and unlocking, while [18] focused on optimizing an RFID door lock system for corporate environments by integrating it with presence monitoring. While these studies confirm the efficacy of RFID for access control, they consistently treat it as a standalone security feature, rarely integrating it with comprehensive environmental monitoring, leaving a critical gap in unified asset protection.

Table I. Comparative Analysis Of Key Technologies In Prior Research

| Title                                                                                    | Authors | Key Technologies Employed         |                                                                     |                    |
|------------------------------------------------------------------------------------------|---------|-----------------------------------|---------------------------------------------------------------------|--------------------|
|                                                                                          |         | Microcontroller                   | Sensor                                                              | Communication      |
| Wireless Fire Safety Monitoring System Based on Digital Twin                             | [22]    | Digital twin, decision support    | Temperature, Smoke                                                  | Wireless protocols |
| Design of remote electronic fire monitoring system based on K-means clustering algorithm | [23]    | K-means clustering, high accuracy | Smoke, temperature, image collector                                 | Wireless           |
| Enhancing cold storage efficiency using image processing and IoT enabled notifications   | [24]    | Node-MCU Microcontroller          | DHT11 Temperature and Humidity Sensor, the MQ-3 Ethylene gas sensor | Wi-Fi-enabled      |

The related work in Table 1 reveals that effective solutions exist for individual aspects of security on fire detection, surveillance, or access control. There is a notable research gap in the development of a single, cost-effective framework that seamlessly integrates all three. Most systems focus on one or two of these areas, leaving users to manage multiple disconnected platforms. The proposed project aims to address this gap by creating a unified system that combines environmental safety, secure access control, and live visual surveillance into one remotely manageable platform.

## SYSTEM DESIGN AND METHODOLOGY

This section outlines the system architecture and development process used for the system. It details the selection of hardware and software components, the overall system architecture, and the structured development process followed to ensure the system objectives were achieved systematically.

### A. System Architecture

The system architect in Fig. 1 is using a centralized processing hub, the ESP32 microcontroller. It is chosen for its robust processing capabilities and has a built-in Wi-Fi connectivity for basic system architecture. The set of input users such as the RFID RC522 module, the IR flame sensor, the MQ2 gas sensor, and RFID RC522 module are integrated for continuously collecting access data from the ESP32 processes.

After processing information at the ESP32 that uses it integrated Wi-Fi module, the data is transmitted to the Blynk server. This platform acts as the middleware serving the controls event triggers, managing data storage, and communication between the hardware and the end user.

The Blynk mobile application allows the user to communicate and interacts with the system. The system provides a real time dashboard for data visualization, system control, and push notifications for critical alerts.

In corresponding, the Wireless IP Camera operates on a separate but integrated path, connecting directly to the local Wi-Fi network and streaming its feed to the dedicated VI365 mobile application. This hybrid architecture; a centralized ESP32 for sensing and a parallel IP camera stream; represents a practical and cost-effective approach, decoupling the high-bandwidth video feed from the low-bandwidth sensor data to ensure real-time alert delivery without compromising surveillance quality.

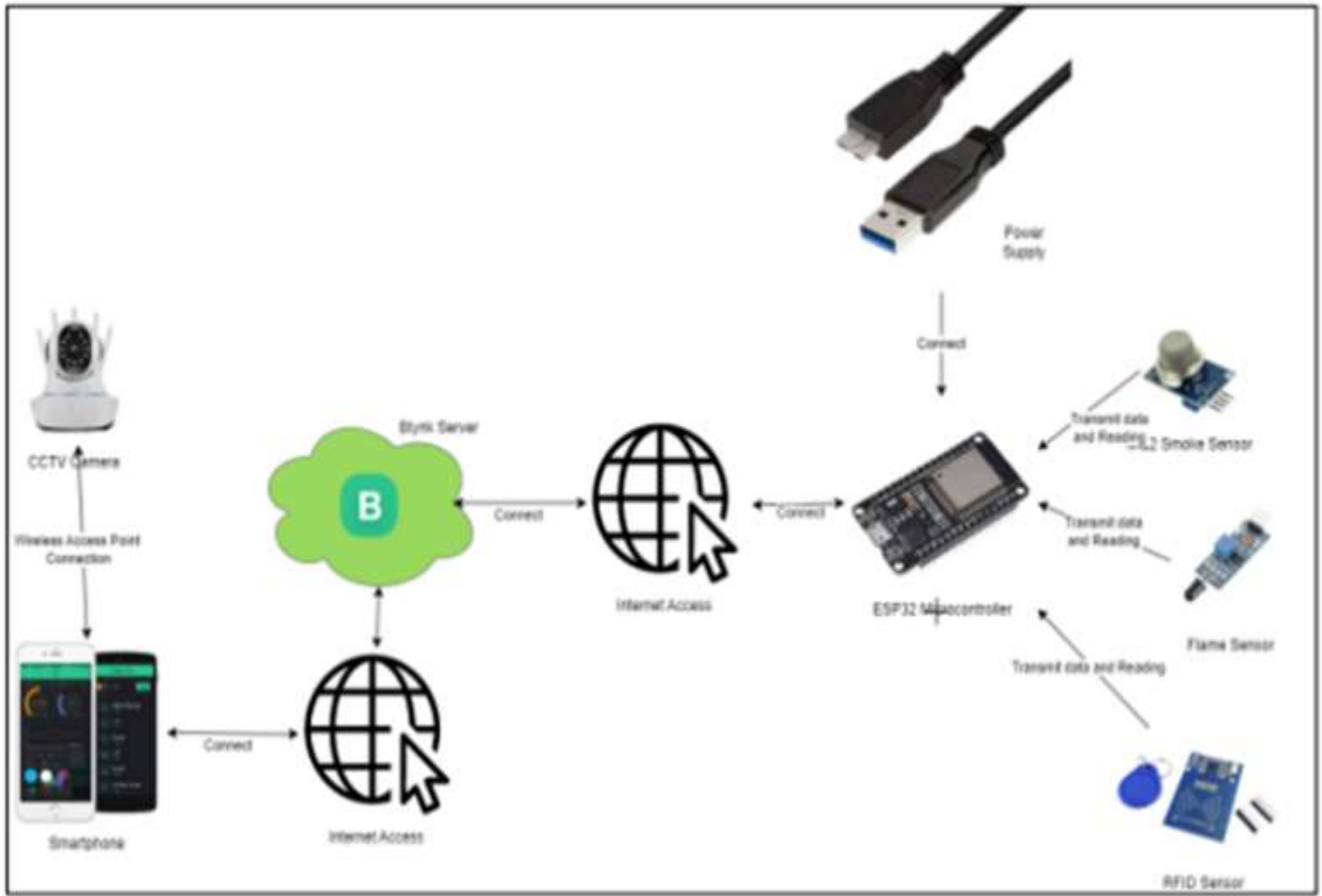


Fig. 1 System Architecture

## B. Hardware Components

The following hardware components listed in Fig. 2 below were selected for developing a monitoring system that is reliable, low cost priced, effective.

- 1) ESP32 Development Board: is selected as the core controller due to its integrated Wi-Fi and Bluetooth capabilities, dual-core processor, and sufficient GPIO pins. It makes it ideal hardware for managing multiple sensors and network communications simultaneously.
- 2) MQ2 Gas Sensor: being chosen because it has high sensitivity to a wide range of combustible gases and smoke detection, which leads by providing a primary layer of defense for fire detection.
- 3) IR Flame Detection Sensor: included due to its ability to detect the infrared radiation emitted by flames. This provides a rapid and direct method of fire identification. Furthermore, MQ2 sensor is complemented sensor for its faster and more reliable alerts.
- 4) RFID RC522 Module: utilized to implement a secure, contactless access control system. This module allows for the authentication of users via RFID cards or tags, which offers a more secure alternative to traditional keys.
- 5) Wireless IP Camera: is integrated to provide real-time visual surveillance. Its wireless connectivity and dedicated application allow users to remotely monitor the storeroom visually, record footage, and respond to incidents with greater context.

The following hardware components listed in Fig. 2 below were selected for developing a monitoring system that is reliable, low cost priced, effective.

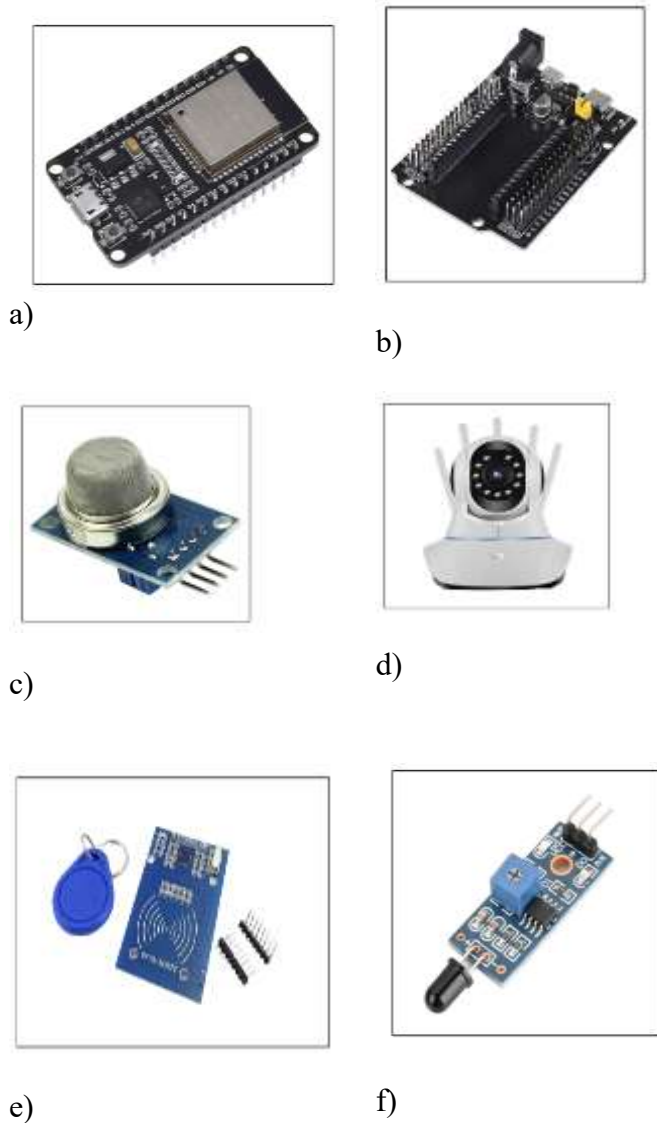


Fig. 2 Identified sensors important for the system -

- a) ESP32 Development Board Wi-Fi + Bluetooth
- b) ESP32 Expansion Board
- c) MQ2 Smoke Gas LPG Butane Hydrogen Gas Sensor Detector
- d) Wireless IP Camera Module
- e) RFID RC522 Sensor
- f) IR Infrared 3 Wire Flame Detection Sensor

### C. Software Components

The software component was chosen for its accessibility, robust community support, and ease of integration.

1) Arduino IDE: is used as the primary integrated development environment for programming the ESP32 microcontroller. Its extensive library support and straightforward interface facilitate rapid development and debugging of the embedded firmware.

2) Blynk Platform (Mobile and Web): is selected as the central user interface for the IoT system. It enables the creation of a custom dashboard with widgets for real-time data visualization (gauges, charts), system control, and receiving push notifications for critical events, without requiring complex app development.

3) VI365 Application is dedicated to a third-party application that serves as the interface for the Wireless IP Camera, providing functionalities for live viewing, recording, and remote camera control.

Fig. 3 shows the interaction between a software and hardware sequence, and the following Fig.4 illustrates the system design and development process for monitoring system.

Fig. 3 Software and Hardware Interaction Sequence

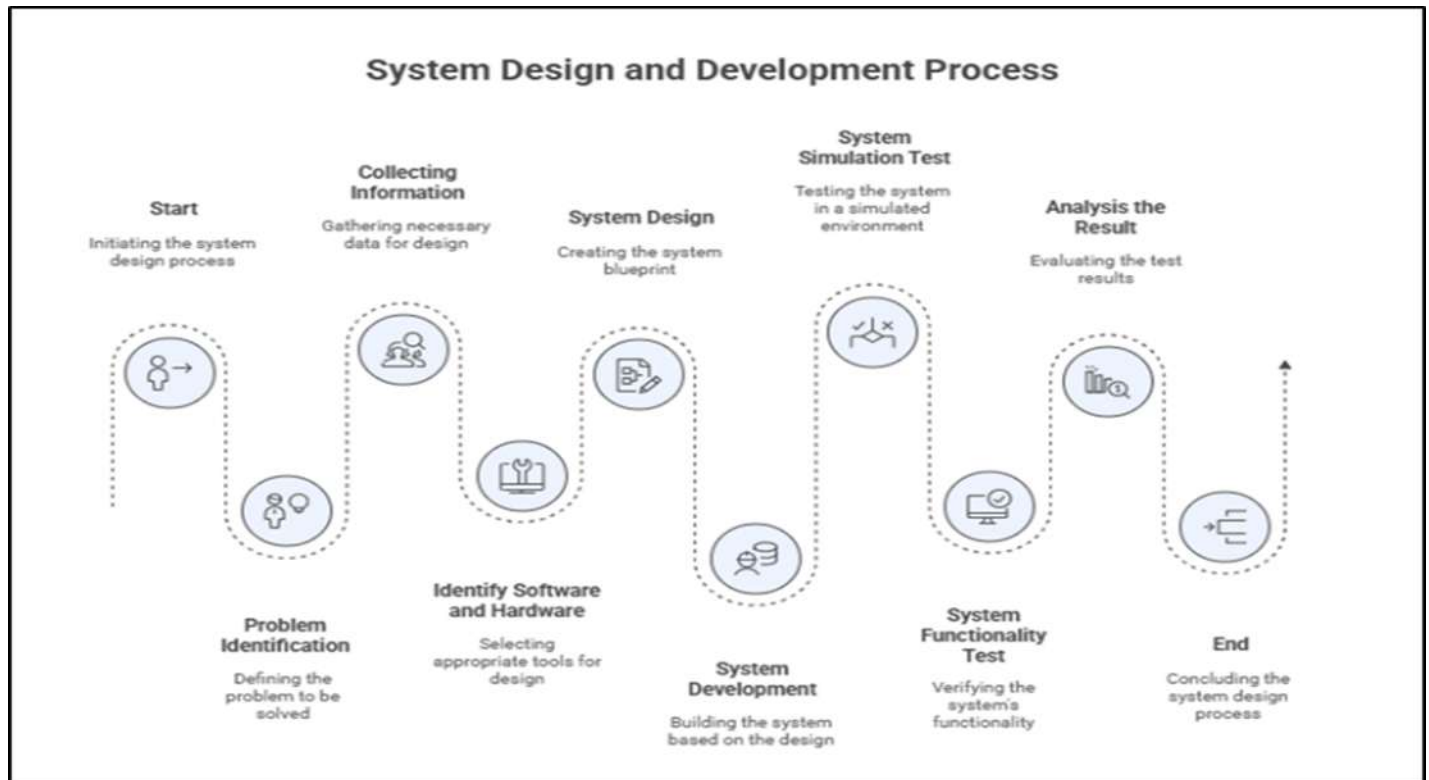


Fig. 4 System Design and Development Process

The black-box methodology [25] is used in this system design and development process to evaluate the functionality of a system based on its specifications without examining the internal workings of the system. This approach involves providing specific input and observing the resulting outputs to ensure the system behaves as expected. Black box testing focuses on testing the connectivity test and functionality test such as user interface and features of each prototype implementation. Because black-box testing does not test the program's source code, but rather the appearance of the hardware and software operations and functionality, the focus of this testing is only on the information and component functionality of each implementation's components.

## Implementation And Monitoring Testing

This section details the physical construction of the system prototype and the structured testing protocol designed to validate its functionality, reliability, and performance against the project's core objectives. The outcomes of the Implementation prototype phase are shown in Fig. 5. The testing protocol was employed to evaluate the system's functionality.

### A. Prototype Implementation

The implementation phase began with the physical assembly of the hardware. The MQ2 gas sensor, IR flame sensor, and RFID RC522 module were systematically connected to the GPIO pins of the ESP32 development

board mounted on a breadboard. Jumper wires were used to establish the necessary power (VCC), ground (GND), and data signal connections as specified in the circuit diagrams.

Simultaneously, the software was configured. The Arduino IDE was set up with the required libraries for the ESP32 board, Blynk platform, and RFID module. The firmware was developed in C++ to read data from each sensor, process it, and transmit it to the Blynk cloud using the specified authentication token. Within the Blynk application, a custom dashboard was created. This involved adding and configuring various widgets: Gauge and Super Chart widgets were set up to visualize real-time and historical data from the MQ2 and flame sensors, while an LCD widget was configured to display the status of the RFID access control system ("Authorized" or "Denied").

Fig. 5 Fertilizing User Interface

## B. Testing Protocol

A black box testing strategy was employed to evaluate the system's functionality. This approach focuses on testing the system's external behavior by providing inputs and examining the outputs, without inspecting the internal code structure. This method successfully verifies the IoT integrated systems module and RFID module with user experience alert expectations.

The indoor setting test environment equips with stable Wi-Fi connectivity to ensure reliable communication with the Blynk server and the VI365 application. The tests were categorized to systematically assess each component's performance, focusing primarily on two classes:

- 1) Connectivity Tests: Verifying that each hardware component could successfully establish a connection with the ESP32 and that the ESP32 could connect to the Wi-Fi network and the Blynk server.
- 2) Functionality Tests: Evaluating the operational performance of each sensor and actuator by simulating real-world scenarios and observing the system's response.

Fig. 6 shows the Blynk Dashboard Integration of layers for the IoT storeroom monitoring system.

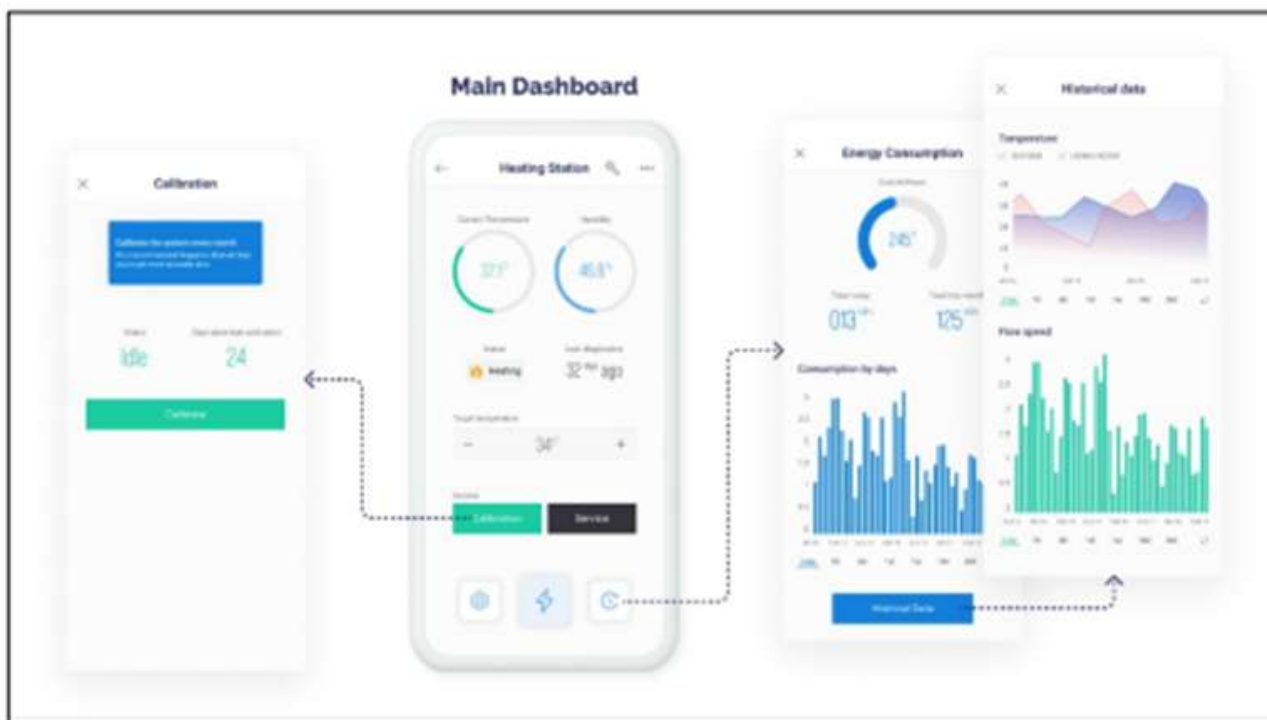


Fig. 6 The Blynk Dashboard Integration of layers for the IoT storeroom monitoring system.

The successful integration of the IoT system layers comprising the sensing, data acquisition, data processing, and application layers the prototype was developed to enable real-time monitoring of monitoring storeroom system. To illustrate the functionality and user interaction of the developed system, a screenshot of the IoT platform is presented in Fig. 7 below. This visual representation highlights the key features such as live sensor data display, intuitive interface design, and the system's capability to support informed decision-making by end users.



Fig. 7 Successful Connectivity NodeMCU and RFID Sensor.

## RESULTS AND DISCUSSION

The data collected from the IoT storeroom monitoring system's experimental testing are shown in this section. The findings are detailed to provide a clear account of the system's performance, followed by a critical discussion of their implications in relation to the initial project objectives.

### A) Functionality Test Results

A series of tests were conducted to validate the functionality and connectivity of each system component. The black box testing approach yielded clear, observable outcomes that confirmed the system's operational integrity. The results are summarized in Table 2.

Table II. Sensor And Component Functionality Test Results

| Component          | Test Performed                                                 | Expected Result                                                        | Observed Outcome                                                                                            |
|--------------------|----------------------------------------------------------------|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| ESP32 Connectivity | Upload code via Arduino IDE and connect to local Wi-Fi network | Successful code upload and stable connection to Wi-Fi and Blynk server | The code was uploaded successfully, and the device connected to the network and appeared as "Online" in the |

|                     |                                                                                 |                                                                                                                                      |                                                                                                                                                                                                    |
|---------------------|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     |                                                                                 |                                                                                                                                      | Blynk app.                                                                                                                                                                                         |
| MQ2 Gas Sensor      | Introduce a controlled amount of gas (from a lighter) and smoke near the sensor | A significant increase in the sensor value displayed on the serial monitor and Blynk Gauge widget                                    | The sensor value increased immediately upon exposure to gas/smoke, with real-time updates reflected on both the serial monitor and the Blynk app                                                   |
| Flame Sensor        | Introduce a flame (from a lighter) within the sensor's detection range          | The sensor's digital output state changes from '1' (idle) to '0' (flame detected), triggering an alert in the Blynk app              | The serial monitors correctly registered the state change from '1' to '0', and the corresponding gauge in the Blynk app updated instantly.                                                         |
| RFID Access Control | Scan a pre-authorized RFID card and an unauthorized RFID card                   | The system correctly identifies the authorized card, displaying "Authorized." The unauthorized card is rejected, displaying "Denied" | The Blynk LCD widget accurately displayed "Authorized" for the registered card and "Denied" for the unregistered card, confirming the system's ability to perform its core access control function |
| CCTV Camera         | Connect the camera to the Wi-Fi network and access the feed via the VI365 app   | A stable, real-time video stream is accessible remotely through the mobile app, with functional controls.                            | The camera successfully connected to the app, providing a clear live video feed and responding to pan and tilt commands.                                                                           |

The experimental results provide compelling evidence that the prototype successfully achieved its primary research objectives. The successful state change of the IR Flame Sensor from '1' to '0' upon flame introduction Table 2 directly validates the first project objective of developing a reliable fire detection system. Similarly, the system's accurate differentiation between registered and unregistered cards on the Blynk LCD widget fulfills the second objective of implementing secure RFID access control. Finally, the ability to establish a stable video stream via the VI365 application confirms the attainment of the third objective: integrating CCTV for real-time remote surveillance. The consistent transmission of all sensor data to the Blynk platform for remote visualization and alerts confirms the system's efficacy as a cohesive and effective IoT framework.

Despite the successful validation of the prototype, several limitations were identified during the project. These constraints provide important context for the current system's capabilities and suggest directions for future development.

1) Hardware Processing Limitations: Although ESP32 can process data, its memory and computing capability are limited. Therefore, the system scales must include more sensors or more complex data processing algorithms (e.g., machine learning for anomaly detection).

2) Reliance on Wi-Fi Connectivity: The system's functionality is entirely dependent on the stability of Wi-Fi connection. If the event of a network failure that may cause real-time monitoring and remote alerts would dismiss, it is suggested to include future iterations that could incorporate backup communication channels like GSM as a backup communication channel.

3) Dependence on Third-Party Platforms: The system relies on external cloud services, namely Blynk and VI365. This simplifies the development process; however, it also adds dependent on these third-party suppliers' availability, pricing structures, and security guidelines. The long-term sustainability of the system may be impacted by any interruption in service or modification in terms.

## B) Backup Communication Component Test Results

An interdependent variable that are essential to the effectiveness of IoT implementations in this system. Table 3, discuss about the test fields in a of real-world settings to record performance in various scenarios such as integrate GSM, LoRa, or Bluetooth as backup communication channels can reduce dependence on Wi-Fi. It includes latency, alert delivery time, and energy consumption. Across all IoT applications, dependable, timely, and energy-efficient operations are ensured by effective control of these parameters.

Table 3: Backup Component Test Results

| Component | Test Performed: Data Transmission Latency                                                         | Expected Result: alert delivery Response Time                                                                                           | Observed Outcome: energy consumption                                      |
|-----------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| GSM       | between 0.05s and 0.15s using MQTT                                                                | Not specified<br>send real-time alerts and notifications via SMS critical events such as unauthorized access or environmental anomalies | Current consumption doubles with -30 dBm RSSI                             |
| LoRa      | >1 second (high SF) and (>15km)<br>between 33.67 ms to 53 ms second (short SF) and (>= 110meters) | Suitable for non-real-time applications; latency increases with distance and SF                                                         | Low Power Consumption longer operational life without frequent recharging |
| Bluetooth | Near-zero to variable                                                                             | Short-Range Communication facilitating quick data transfer between integrated devices                                                   | Low power consumption frequent data transmission with minimal power usage |

The functionality of an integrated RFID and IoT solution for storeroom monitoring can be greatly improved by integrating GSM, LoRaWAN, and Bluetooth. GSM guarantees dependable, wide-area network access and real-time notifications; Bluetooth enables effective short-range data transfer; and LoRa gives long-range, low-power communication. The storeroom monitoring system which incorporates with GSM, LoRaWAN, and Bluetooth provides different measures for power consumption, response time, and data transmission latency. LoRaWAN offers comprehensive metrics regarding delay times due to its energy efficiency, While BLE provides reduced latency and power consumption appropriate for battery-operated devices, GSM/GPRS shows better real-time performance but lacks reliable latency values. This integration creates a comprehensive and efficient storeroom or warehouse monitoring system suitable for a variety of applications.

RFID systems can be made far more secure and private by combining logic encryption, timestamps, and security and privacy access control protocols. These safeguards make RFID systems more resilient and dependable in a range of applications by ensuring data confidentiality, reciprocal authentication, and defense against several security threats. We suggest to add more powerful controllers with extension modules for example ESP32Ext and other extension modules can improve the ESP32's performance in applications that demand more power or complex processing. By solving the shortcomings of the conventional ESP32, these modules can enhance motor control, AI image processing, and data transmission capabilities. Although video streaming is not specifically covered in the development prototype, the concepts of encryption and secure data transfer can be used. Video data can be shielded from alteration and unwanted access by being encrypted both during transmission and storage.

## C) Cost comparison with commercial solutions

The ESP32 is a popular choice for low cost IoT purposes because of its reputation for cost and versatility. It's excellent for developing gadgets that can readily connect and communicate with one another because it has built-in Bluetooth and Wi-Fi. The initial setup cost can be much cheaper, often between RM 40 and RM 210 per unit,

depending on the system's features and complexity. Meanwhile, commercial RFID system solutions frequently include customized software and hardware, which raises the initial spending of costs. Normally it depends on the manufacturer, features, and capabilities, the devices can cost anywhere from RM420 to several thousand ringgits. The advantages of low-cost design include increased affordability due to the much lower initial and ongoing expenses, which enable RFID technology to be used by a larger spectrum of customers, including small enterprises and startups. Additionally, it is customization and flexibility. Low-cost designs remove the limitations of proprietary systems and enable more customization and adaptability to particular demands. The user can increase their RFID capabilities as needed. Based to the scalability approach, which makes it possible for the system to scale affordably, growth and innovation are encouraged. When it comes to community assistance, open-source solutions usually provide access to an enormous amount of information, documentation, and group knowledge.

In summary, the system did remarkably well within the constraints of its design parameters, yet these drawbacks underscore the inherent trade-offs between low cost, complexity, and robustness in these kinds of IoT initiatives projects.

## CONCLUSION AND FUTURE WORK

This system serves as a verified roadmap for creating low-cost, multi-modal IoT security systems. By successfully integrating environmental sensing, access control, and video surveillance on an accessible platform like ESP32 and Blynk, this research demonstrates that comprehensive, real-time monitoring is no longer exclusively the domain of high-cost, proprietary enterprise solutions. The resulting system effectively solves the problems of inadequate fire safety, insecure access control, and a lack of real-time visibility by uniting these disparate functions into a single, cohesive, and remotely manageable platform. The prototype design approves that the prototype is viable and capable for enhancing both of the security and monitoring efficiency of storeroom management. By building based on this successful prototype, several paths for future research and development are proposed to further enhance the system's capabilities, robustness, and applicability:

- 1) Enhancing Scalability: the future system should consider more powerful microcontrollers and optimized power management for battery operation.
- 2) Advanced Analytics: it should include developing a custom application with machine learning algorithms for predictive maintenance and anomaly detection even though it is a low-cost monitoring system.
- 3) Improving Security: includes the integration of blockchain technology for securing access logs and data integrity.
- 4) Real-World Validation: the system should collaborate with industry partners to deploy and validate the low-cost system in commercial or industrial environments.

## ACKNOWLEDGEMENT

The author would like to thank the Centre of Research and Innovation Management of University Technical Malaysia Melaka (UTeM) for sponsoring the publication fees under the Tabung Penerbitan CRIM UTeM.

## REFERENCES

1. M. K. Hasan, M. Junjie, A. K. M. Ahasan Habib, A. Al Mamun, T. M. Ghazal, and R. A. Saeed, "IoT-Based Warehouse Management System," in 2022 International Conference on Cyber Resilience (ICCR), IEEE, Oct. 2022, pp. 1–6. doi: 10.1109/ICCR56254.2022.9995768.
2. M. J. Bixler and D. Honhon, "Exploring the Connections between Backrooms, Inventory Record Inaccuracies, and Waste," *Sustainability*, vol. 13, no. 17, p. 9490, Aug. 2021, doi: 10.3390/su13179490.
3. M. Ali et al., "A Comprehensive Review of Advanced Sensor Technologies for Fire Detection with a Focus on Gasistor-Based Sensors," *Chemosensors*, vol. 13, no. 7, p. 230, Jun. 2025, doi: 10.3390/chemosensors13070230.

4. A. M. Kassim et al., "Performance Evaluation of Intelligent Fire Alarm System with Multi Data Fusion Sensor by Using IoT Platform," 2022, pp. 199–209. doi: 10.1007/978-981-16-8954-3\_20.
5. N. Sharma, R. Angmo, V. K. Tayal, K. Pandey, and R. Gupta, "Design of Fire Detection System with Extended Range," in 2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST), IEEE, Apr. 2025, pp. 1–5. doi: 10.1109/ICTEST64710.2025.11042436.
6. A. Solórzano et al., "Early fire detection based on gas sensor arrays: Multivariate calibration and validation," *Sensors Actuators B Chem.*, vol. 352, p. 130961, Feb. 2022, doi: 10.1016/j.snb.2021.130961.
7. C. You et al., "A Latent-Fire-Detecting Olfactory System Enabled by Ultra-Fast and Sub-ppm Ammonia-Responsive Ti<sub>3</sub>C<sub>2</sub>T<sub>x</sub> MXene/MoS<sub>2</sub> Sensors," *Adv. Funct. Mater.*, vol. 32, no. 44, Oct. 2022, doi: 10.1002/adfm.202208131.
8. S. Srivastava, R. B. Dan, S. D. Kaipa, N. Jadhav, C. G. H S, and C. K R, "IoT-Based Smart Lake Fire Detection and Alarming System," in 2024 5th International Conference on Communication, Computing & Industry 6.0 (C2I6), IEEE, Dec. 2024, pp. 1–7. doi: 10.1109/C2I663243.2024.10895908.
9. O. M. Abed Al-Isawi, K. H. Alkhater, S. H. Alrubae, A. H. AlMarzooqee, and A. H. Mohammed, "An Early Warning System for Fires in Hospitals and Health Centers via the Internet of Things to Reduce Human and Material Losses," in 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), IEEE, Jun. 2023, pp. 1–5. doi: 10.1109/HORA58378.2023.10155784.
10. Y. Wang, "Simulation Study of Fuzzy Neural Control Fire Alarm System Based on Clustering Algorithm," in 2022 2nd International Conference on Algorithms, High Performance Computing and Artificial Intelligence (AHPCAI), IEEE, Oct. 2022, pp. 217–221. doi: 10.1109/AHPCAI57455.2022.10087561.
11. S. Sekar, S. Narayanan, P. Sirenjeevi, and R. Sethuraman, "Enhancing real-time video surveillance: a circular queue-guided stacked parallel convolution network for efficient suspicious activity detection," *Earth Sci. Informatics*, vol. 18, no. 3, p. 452, Sep. 2025, doi: 10.1007/s12145-025-01879-w.
12. V. Sasikala, A. Harini, B. Trisha, and K. Na, "Ble Based Home Automation," in 2024 International Conference on Communication, Computing and Internet of Things (IC3IoT), IEEE, Apr. 2024, pp. 1–6. doi: 10.1109/IC3IoT60841.2024.10550306.
13. M. Hardyan, F. A. Haqqi, and Yohandri, "Arduino based smart home security design using biometric recognition," *J. Phys. Conf. Ser.*, vol. 2582, no. 1, p. 012025, Sep. 2023, doi: 10.1088/1742-6596/2582/1/012025.
14. A. M. S. V Sushma, A. Aswini Priyanka, A. N. G. Lakshmi, N. Khatri, and H. Sharma, "Integrated IoT-Based Smart Home Security System: Real-Time Hazard Detection and Alerts Using Multi-Sensor Fusion," in 2024 International Conference on Intelligent & Innovative Practices in Engineering & Management (IIPeM), IEEE, Nov. 2024, pp. 1–6. doi: 10.1109/IIPeM62726.2024.10925672.
15. S. S. Mazlan, N. Mohamed, and F. Majid, "Development of Monitoring System using Raspberry Pi with Instant Notification," *J. Emerg. Technol. Ind. Appl.*, vol. 2, no. 1, pp. 1–6, 2023, [Online]. Available: <https://jetia.mbot.org.my/index.php/jetia/article/view/15%0Ahttps://jetia.mbot.org.my/index.php/jetia/article/download/15/14>
16. K. Chenchireddy, S. Jatavath, K. K. K. Yadav, M. Harsha, N. Ontedhu, and J. Varghese, "Radio-frequency identification door lock access control system by using Arduino," 2025, p. 020003. doi: 10.1063/5.0269167.
17. G. Harshitha, G. S. N, G. B, G. P, G. L, and S. Nalinakshan, "RFID based Access Control System," in 2025 International Conference on Electronics and Renewable Systems (ICEARS), IEEE, Feb. 2025, pp. 182–186. doi: 10.1109/ICEARS64219.2025.10941511.
18. A. A. Nair, R. Adithyan, A. Unni, and S. Nalinakshan, "RFID Door Lock Access Control Systems: Trends, Technologies and Applications," in 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), IEEE, Feb. 2025, pp. 906–912. doi: 10.1109/IDCIoT64235.2025.10914928.
19. M. U. Kiru, B. Belaton, S. M. S. Mohamad, G. M. Usman, and A. A. Kazaure, "Intelligent Automatic Door System based on Supervised Learning," in 2020 IEEE Conference on Open Systems (ICOS), IEEE, Nov. 2020, pp. 43–47. doi: 10.1109/ICOS50156.2020.9293673.

20. S. D. Diga, R. A. Cribello, and J. L. Meneses, "Development of Alarm System Using GSM Technology and RFID Integration," *Int. J. Progress. Sci. Technol.*, vol. 46, no. 2, p. 421, Sep. 2024, doi: 10.52155/ijpsat.v46.2.6601.
21. J. Guntur, S. S. Raju, T. Niranjana, S. K. Kilaru, R. Dronavalli, and N. S. S. Kumar, "IoT-Enhanced Smart Door Locking System with Security," *SN Comput. Sci.*, vol. 4, no. 2, p. 209, Feb. 2023, doi: 10.1007/s42979-022-01641-9.
22. J. Qiang, "Wireless Fire Safety Monitoring System Based on Digital Twin," in *2025 Asia-Europe Conference on Cybersecurity, Internet of Things and Soft Computing (CITSC)*, IEEE, Jan. 2025, pp. 918–923. doi: 10.1109/CITSC64390.2025.00172.
23. Y. Lang and G. Shan, "Design of remote electronic fire monitoring system based on K-means clustering algorithm," *Int. J. Ind. Syst. Eng.*, vol. 39, no. 3, p. 429, 2021, doi: 10.1504/IJISE.2021.119710.
24. S. Nagarale, V. Bora, and S. Sonaskar, "Enhancing cold storage efficiency using image processing and IoT-enabled notifications," 2024, p. 020008. doi: 10.1063/5.0230493.
25. G. W. Sasmito and M. A. Mutasodirin, "Black Box Testing with Equivalence Partitions Techniques in Transcrop Applications," in *2023 6th International Conference of Computer and Informatics Engineering (IC2IE)*, IEEE, Sep. 2023, pp. 53–58. doi: 10.1109/IC2IE60547.2023.10331562.