Blynk-Enabled Notification Workflow for ESP8266 Security Alerts in Resource-Constrained Deployments

Abdul Halim Bin Dahalan*., Nurulhalim Bin Hassim

Centre for Telecommunication Research and Innovation, Fakulti Teknologi dan Kejuruteraan Elektronik dan Komputer, Universiti Teknikal Malaysia Melaka (UTeM), Durian Tunggal, Melaka 76100, Malaysia

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2025.91200093

Received: 17 December 2025; Accepted: 24 December 2025; Published: 01 January 2026

ABSTRACT

The increasing vulnerability of physical asset containers such as fund and donation boxes has highlighted the need for affordable and responsive security solutions. This paper presents a Blynk-enabled notification workflow integrated with an ESP8266-based alert system designed for deployment in resource-constrained environments. The proposed system combines ultrasonic and force sensors with an ESP8266 Wi-Fi module to detect unauthorized access, tampering, or movement. Upon trigger activation, the system generates a local audible alarm and transmits real-time notifications to stakeholders through the Blynk mobile application. The workflow emphasizes lightweight communication, minimal power consumption, and reliable message delivery over standard Wi-Fi networks. Experimental evaluation demonstrates effective threshold-based detection for force and distance sensing, along with acceptable battery consumption for continuous monitoring scenarios. Results indicate that the integration of Blynk simplifies remote monitoring while maintaining responsiveness under limited hardware and energy constraints. The findings confirm that low-cost IoT platforms can deliver practical security alerting solutions suitable for small-scale asset protection and similar applications.

Keywords - ESP8266; Internet of Things; Blynk platform; Security alert system; Resource-constrained devices; Embedded systems.

INTRODUCTION AND LITERATURE REVIEW

Background And Motivation

Physical fund and donation boxes remain widely used in public, religious, and institutional settings, yet they are frequently exposed to theft and tampering due to inadequate monitoring mechanisms. Conventional security approaches often rely on manual inspections or passive locking systems, which fail to provide timely alerts during intrusion events. Recent advancements in Internet of Things (IoT) technologies have enabled low-cost, network-connected monitoring systems capable of real-time alerting and remote supervision. Among these technologies, the ESP8266 Wi-Fi module has gained popularity due to its affordability, compact size, and native internet connectivity [1], [2].

IoT-based alert systems aim to bridge the gap between physical security and remote awareness by enabling sensors, microcontrollers, and cloud platforms to operate in a coordinated manner. However, many existing solutions are designed for environments with stable power supply and high computational resources, making them unsuitable for low-cost or battery-powered deployments. Therefore, designing a security alert workflow that operates efficiently under constrained resources remains a critical research challenge [3], [4].

Iot Security Alert Systems

Several studies have demonstrated the feasibility of IoT-enabled security monitoring using microcontrollers and wireless communication. Smart donation boxes incorporating IoT technologies have been reported to improve

transparency and theft detection through remote monitoring platforms. Similarly, ESP8266-based intruder alarm systems utilizing motion or proximity sensors have shown reliable real-time alert delivery via mobile applications and cloud services [5].

Other research has explored hybrid alert mechanisms combining local alarms with remote notifications to improve response effectiveness. GSM-based systems, for instance, provide SMS alerts but suffer from higher operational costs and dependency on cellular infrastructure. In contrast, Wi-Fi-based solutions using ESP8266 offer lower operating costs and seamless integration with IoT platforms such as Blynk [6].

Blynk Platform For Iot Notification

Blynk is a widely adopted IoT platform that enables rapid development of mobile dashboards, real-time notifications, and remote device control. Its lightweight architecture is well suited for microcontrollers with limited memory and processing capability. Prior studies have utilized Blynk for smart home automation, motion-activated security systems, and sensor monitoring applications, demonstrating its reliability and ease of deployment [7]

Despite its growing adoption, limited academic work has focused on systematically analysing Blynk-enabled notification workflows in resource-constrained security applications. This paper addresses this gap by evaluating a Blynk-integrated ESP8266 alert system deployed in a low-power, sensor-driven security scenario [8].[9]

Research Gap And Contribution

Although IoT security systems are widely reported, most studies emphasize system functionality rather than workflow efficiency under constrained conditions. This work contributes by:

- Designing a lightweight notification workflow using Blynk and ESP8266.
- Integrating force and ultrasonic sensors for multi-parameter intrusion detection.
- Experimentally analysing trigger thresholds and battery consumption.
- Demonstrating suitability for low-cost, resource-constrained security deployments.

METHODOLOGY

System Architecture

The proposed system consists of a NodeMCU ESP8266 microcontroller, an ultrasonic sensor, a force sensor, a buzzer, and a power supply unit. The ESP8266 acts as the central controller, responsible for sensor data acquisition, decision-making, and Wi-Fi communication with the Blynk cloud server.

Notification Workflow

The workflow begins with continuous sensor monitoring. When measured values exceed predefined force or distance thresholds, the ESP8266 triggers an audible alarm and immediately sends a notification to the Blynk application. The notification includes event status information, enabling stakeholders to respond promptly. This workflow minimizes data transmission overhead by sending alerts only during abnormal events. The current implementation prioritizes lightweight communication and responsiveness, while advanced security features such as encrypted payloads and authentication are reserved for future system enhancement.

Sensor Configuration and Thresholding

The ultrasonic sensor measures distance variations to detect movement or displacement of the fund box, while the force sensor detects applied pressure indicative of tampering. Threshold values were determined experimentally through repeated testing to balance sensitivity and false alarm reduction.

Experimental Setup

Testing was conducted under controlled conditions to evaluate detection accuracy, notification responsiveness, and power consumption. Battery usage was monitored across multiple alert events to assess system suitability for prolonged deployment.

RESULTS AND DISCUSSION

Figure 1 presents the real-time notification interface generated by the Blynk application upon trigger activation. Notifications were delivered consistently with minimal latency under stable Wi-Fi conditions, confirming the reliability of the Blynk workflow.

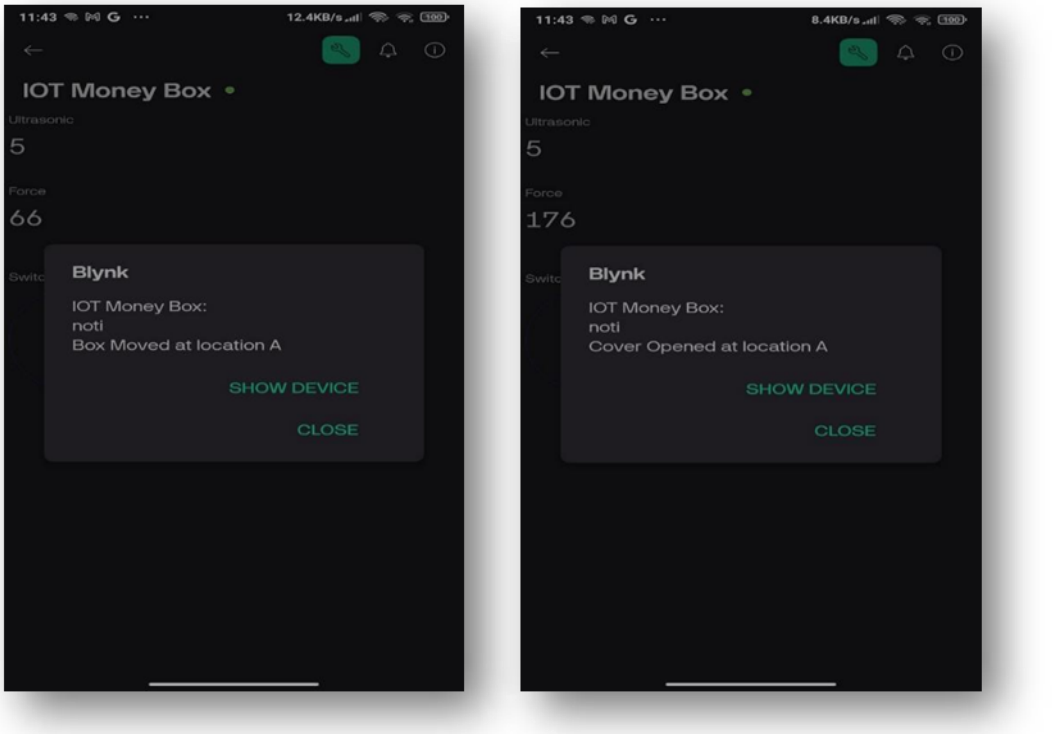

Figure 1: Real-time security alert notification displayed in the Blynk mobile application.

Table 1 shows the data gathered while investigating force versus trigger threshold for the force sensor. **Figure 2** illustrates the relationship between applied force and trigger activation. Results show a clear threshold region where alert activation becomes consistent, enabling effective tamper detection without excessive false alarms.

Table 1: Analysis of force versus trigger threshold

115	1.31
230	1.67
312	1.85
465	2.45
528	2.57
632	2.66

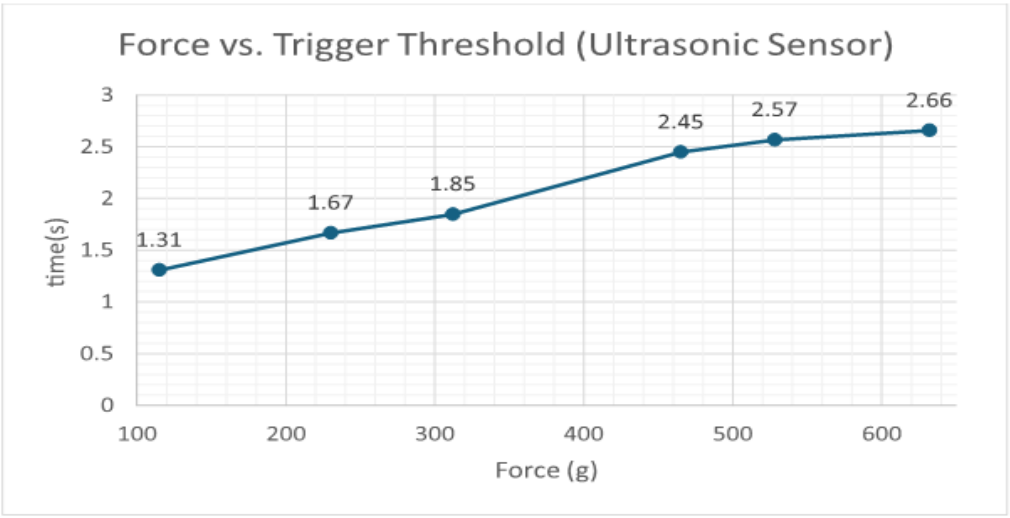

Figure 2: Force versus trigger threshold analysis for tamper detection.

Table 2 shows the data gathered for analysing distance vs trigger threshold for the ultrasonic sensor. **Figure 3** demonstrates distance variation measurements obtained from the ultrasonic sensor. Trigger activation occurred reliably when displacement exceeded the calibrated threshold, validating the suitability of ultrasonic sensing for movement detection.

Table 2: Analysis of distance versus trigger threshold

Distance (cm)	**Time (s)**
3	0
6	0
10	1.47
12	1.76
15	1.56

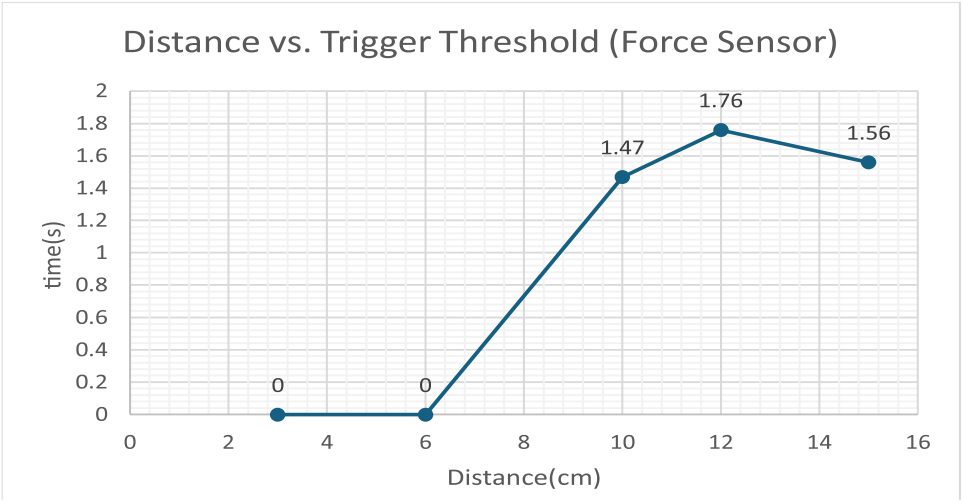

Figure 3: Distance versus trigger threshold analysis using ultrasonic sensing.

Table 3 displays the data collected used for the analysis of battery consumption. Battery consumption results vs alert events are shown in **Figure 4**. The system exhibited moderate power usage during idle monitoring and

increased consumption during alert transmission. Overall, the energy profile supports deployment in short-to-medium duration battery-powered scenarios.

Table 3: Battery consumption measurements

Day	Voltage (v)
0	9
1	8.7
2	8.1
3	7.4
4	6.8
5	6.3
6	5.7
7	4.9
8	4.1
9	3.6
10	1.2
11	0.2

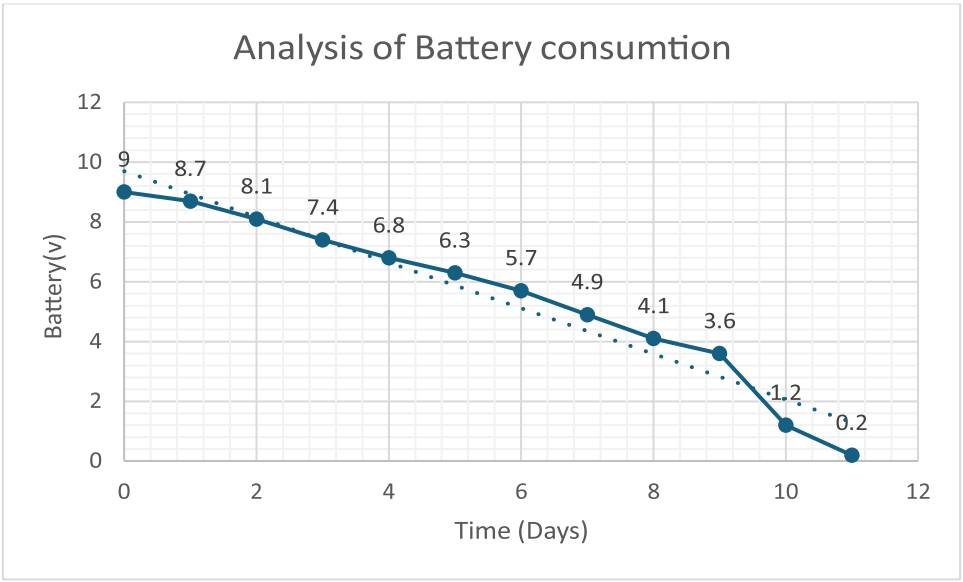

Figure 4: Battery consumption analysis during monitoring and alert events.

Despite the demonstrated effectiveness of the proposed system, certain limitations should be acknowledged. The reliance on stable Wi-Fi connectivity represents a deliberate design trade-off to minimize system cost and complexity, which may constrain deployment in environments with intermittent network availability. Furthermore, experimental validation was conducted under controlled conditions, and performance in highly dynamic real-world settings with interference or unpredictable user behavior was not explicitly evaluated.

Security mechanisms such as data encryption and authentication were not experimentally analyzed in this study and are considered beyond the present scope. Battery testing focused on short-to-medium duration operation aligned with typical low-cost asset protection use cases; extended lifetime validation remains an avenue for future investigation.

DISCUSSION AND CONCLUSION

The results confirm that combining local alarms with Blynk-enabled notifications enhances security responsiveness while maintaining low system complexity. Compared with GSM-based systems reported in prior studies, the proposed workflow offers reduced operating costs and simplified integration. However, reliance on Wi-Fi connectivity may limit performance in environments with unstable networks.

This paper presented a Blynk-enabled notification workflow integrated with an ESP8266-based security alert system designed for resource-constrained deployments. By combining ultrasonic and force sensors with real-time mobile notifications, the system effectively detects unauthorized access and promptly alerts stakeholders. Experimental evaluations demonstrated reliable threshold-based detection and acceptable battery consumption, confirming the practicality of the approach for low-cost security applications. The findings highlight the potential of lightweight IoT platforms to deliver effective asset protection solutions without requiring complex infrastructure. Future work may focus on optimizing power management through deep-sleep strategies, incorporating encrypted communication and authentication mechanisms, evaluating performance under unstable network conditions, and extending the workflow to support cloud-based data logging and predictive analytics.

ACKNOWLEDGEMENT

The authors would like to acknowledge the Centre for Telecommunication Research and Innovation, Fakulti Teknologi dan Kejuruteraan Elektronik dan Komputer, Universiti Teknikal Malaysia Melaka (UTeM), for providing the facilities and technical support necessary for the completion of this research. Appreciation is also extended to all individuals who contributed directly or indirectly to the successful development, testing, and evaluation of the ESP8266-based alert system.

REFERENCES

1. B. Alothman et al., “Development of an Electronic Smart Safe Box Using Private Blockchain Technology,” Applied Sciences, vol. 12, no. 13, p. 6445, Jun. 2022, doi: https://doi.org/10.3390/app12136445.
2. M. Omar Alshammari, A. A. Almulhem, and N. Zaman, “Internet of Things (IoT) : Charity Automation,” IJACSA) International Journal of Advanced Computer Science and Applications, vol. 8, no. 2, 2017, doi: https://dx.doi.org/10.14569/IJACSA.2017.080222.
3. E. Basha and D. Rus, “Design of Early Warning Flood Detection Systems for Developing Countries,” in 2007 International Conference on Information and Communication Technologies and Development, Bangalore, India: IEEE, Dec. 2007. doi: https://doi.org/10.1109/ICTD.2007.4937387.
4. R. Arabelli, D. Rajababu, D. Srinivas, S. Yedulapuram, and C. Banapuram, “A Novel Method to Monitor and Alert System for A Letter Box,” in IOP Conference Series: Materials Science and Engineering, IOP Publishing Ltd, Dec. 2020. doi: 10.1088/1757-899X/981/3/032020.
5. S. Sultana, A. Rahaman, A. Mahmud Jhara, A. Chandra Paul, and J. Uddin, “An IOT based Smart Drain Monitoring System with Alert Messages,” Springer, Cham, Feb. 2021. doi: https://doi.org/10.1007/978-3-030-68452-5_9.
6. M. Darwis, H. A. Al Banna, S. R. Aji, D. Khoirunnisa, and N. Natassa, “IoT Based Early Flood Detection System with Arduino and Ultrasonic Sensors in Flood-Prone Areas,” JURNAL TEKNIK INFORMATIKA, vol. 16, no. 2, pp. 133–140, Dec. 2023, doi: 10.15408/jti.v16i2.32161.
7. Nur Afrina Natasha Binti Apiza, “Smart Mosque Coinbox With IOT System,” Politeknik Sultan Salahuddin Abdul Aziz Shah, 2023. Accessed: Dec. 19, 2024. [Online]. Available: http://repository.psa.edu.my/handle/123456789/4323

8. M. V Sirisha, N. Bhavana, R. Padamavathi, A. U. Sankar, and K. Chandra Sekhar, "ATM SECURITY USING GSM AND MEMS SENSOR," International Research Journal of Engineering and Technology, vol. 545, 2008, [Online]. Available: www.irjet.net
9. M. S. Kumari, A. Tejesh, G. Aakash, B. S. Kiran, and I. Nagaraj, "IoT-based Dual Technology Motion Detector," in E3S Web of Conferences, EDP Sciences, Jun. 2023. doi: 10.1051/e3sconf/202339101156.