Journal of Hypermedia & Technology-Enhanced Learning
Vol. 3, No. 1, February (2025), Pages 1–15
e-ISSN: 2985–9166 | 10.58536/j-hytel.158

RESEARCH ARTICLE

IoT-Enabled Smart Fence: Remote Security and Monitoring Using NodeMCU ESP32 and Blynk

Fadhilah Putri Syahrani[1]*, Hadi Kurnia Saputra[1], Sartika Anori[1], Winda Agustiarmi[1], Firas Tayseer Ayasrah[2], Pham Van Thanh[3]

[1] Department of Electronics Engineering, Faculty of Engineering, Universitas Negeri Padang, **Indonesia**
[2] College of Education, Humanities and Science, Al Ain University, Al Ain 64141, **United Arab Emirates**
[3] Faculty of Engineering, Dong Nai Technology University, Bien Hoa City, **Vietnam**

*Corresponding Author: *fadhilah.putri.syahrani@gmail.com*

This article contributes to:

ABSTRACT

The Internet of Things (IoT) has transformed home security by enabling automated remote monitoring and control systems. This study presents an IoT-enabled smart fence prototype that utilizes the NodeMCU ESP32 microcontroller and the Blynk application to provide secure, efficient remote gate operations. The system allows users to remotely open, close, and lock gates via mobile devices, addressing the limitations of traditional manual methods. Core components include ultrasonic sensors for real-time obstacle detection, relays, and motors, all integrated into a robust hardware-software framework. Testing revealed consistent system responses within two seconds under stable network conditions, with accurate obstacle detection ensuring the safety zone is maintained. Despite network stability challenges, the system is practical, user-friendly, and scalable for residential security applications. Future improvements could incorporate dual connectivity options to enhance network resilience and advanced sensor calibration to improve reliability across varied environments. This cost-effective prototype demonstrates significant potential for modern smart home security applications and future advancements.

KEYWORDS

IoT-based home security; automated fence system; Blynk application; NodeMCU ESP32

Received: Oct. 26, 2024; *Revised:* Nov. 18, 2024; *Accepted:* Dec. 18, 2024; *Published Online:* Jan. 15, 2025

How to Cite: Syahrani, F. P., Saputra, H. K., Anori, S., Agustiarmi, W., Ayasrah, F. T., & Thanh, P. V. (2025). IoT-Enabled Smart Fence: Remote Security and Monitoring Using NodeMCU ESP32 and Blynk. *Journal of Hypermedia & Technology-Enhanced Learning*, *3*(1), 1–15. https://doi.org/10.58536/j-hytel.158

Published by *Sagamedia Teknologi Nusantara*

1. INTRODUCTION

The rapid advancement of Internet of Things (IoT) technology has profoundly transformed daily life, especially in home automation. By 2025, the global number of IoT-enabled devices is expected to surpass 75 billion, underscoring the growing demand for enhanced connectivity, safety, and efficiency

in residential settings [1]. IoT enables physical objects to communicate and interact over networks, facilitating remote control capabilities that enhance security, convenience, and responsiveness in smart homes. Mobile applications empower users to manage essential devices, including lighting, door locks, and surveillance systems, providing integrated and user-friendly home automation solutions [2], [3].

Despite significant advancements in home automation, home security remains a critical challenge, particularly with traditional fencing systems reliant on manual operation. These systems are often inconvenient, prone to failure, and vulnerable to security breaches. For instance, research indicates that weaknesses in manual locking mechanisms significantly increase the risk of unauthorized access, as intruders can easily tamper with or bypass locks [4]. These limitations underscore the pressing need for innovative solutions that enhance residential fence security while improving operational efficiency.

To address this gap, this study presents an IoT-enabled smart fence that integrates the NodeMCU ESP32 microcontroller and the Blynk mobile application to provide secure, automated, and remote control of fence operations. Unlike traditional systems, this prototype enables users to remotely open, close, and lock gates via mobile devices, eliminating manual vulnerabilities and improving overall security. The NodeMCU ESP32 is the central controller, processing real-time sensor data and managing motor operations to ensure low-latency responses. Simultaneously, the Blynk app offers an intuitive, user-friendly interface, enabling seamless monitoring and control of the system [6].

Compared to existing systems, which often lack reliable remote control, real-time responsiveness, or seamless integration with smart home platforms, this prototype delivers a robust hardware-software framework adaptable to varied residential environments. Test results have validated its practicality and scalability, establishing it as a cost-effective, user-friendly solution for modern home security applications [7].

The integration of IoT into home automation has transitioned from a trend to a necessity, driving advancements in security, convenience, and quality of life [8], [9]. As the demand for smart, connected homes continues to grow, technologies enabling automated monitoring and control have become indispensable [10], [11]. In this context, this study introduces a versatile and scalable smart fence system designed to enhance home security through real-time responsiveness and IoT-enabled automation.

2. METHODS

This study adopted an experimental-prototyping approach to design and develop an IoT-enabled smart fence. This method was chosen for its iterative nature, which supports incremental testing, refinement, and optimization of hardware and software components [12]. The approach is particularly suited to IoT projects, enabling continuous evaluation of component functionality and integration throughout development [13]. The prototyping process was divided into six stages, as shown in Figure 1.

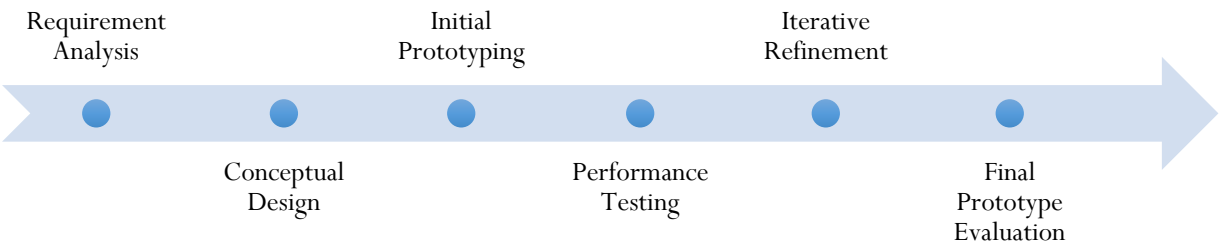


Figure 1. Experimental prototyping

2.1. Requirement analysis

The requirements analysis phase identified functional and non-functional requirements based on user needs and technical specifications [14]. This stage ensured that the system aligned with an IoT-enabled smart fence's operational criteria and performance expectations.

2.1.1. Functional Requirement

The functional requirements specified the system's core capabilities, including remote fence control through mobile devices for opening, closing, and locking. Ultrasonic sensors were integrated to detect nearby objects, ensuring operational safety by halting actions within a designated safety zone [15]. Additional functionalities included real-time user notifications and an intuitive mobile interface for streamlined operation and monitoring.

2.1.2. Non-functional Requirements

The non-functional requirements focused on ensuring smooth, efficient, and secure system operation. The system was designed to respond to user commands with minimal latency, targeting a response time of less than two seconds and maintaining a reliability rate exceeding 95%. Robust security protocols were implemented to safeguard against unauthorized access, while the design was optimized for power efficiency to enable long-term, sustainable use.

2.2. Conceptual Design

The conceptual design phase involved developing the system architecture, including block diagrams, flowcharts, and a preliminary physical layout, which served as the blueprint for the prototype's development. Figure 2 illustrates the system's key components, detailing the inputs (ultrasonic sensors, RFID), the controller (NodeMCU ESP32), the actuators (relay, motor), and the outputs (mobile app notifications).

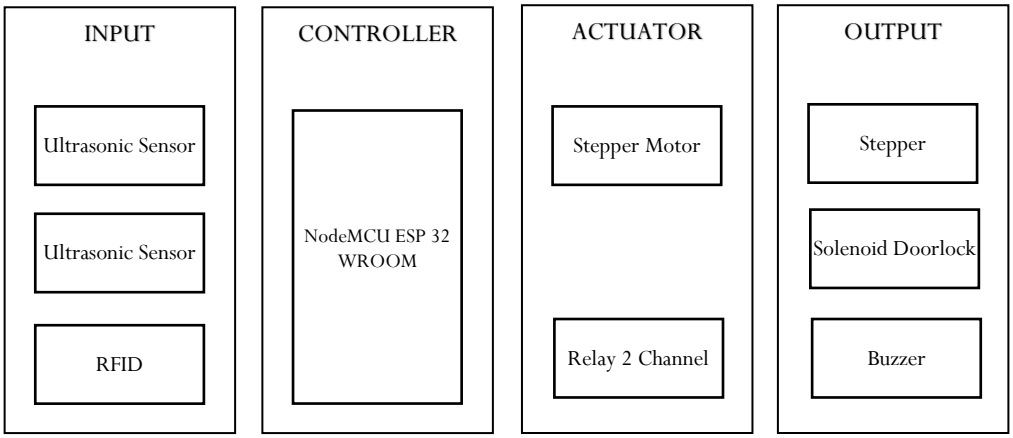


Figure 2. System block diagram for automatic fence system

Figure 3 outlines the operational sequence, beginning with object detection, followed by the receipt of a user command, which triggers the motor to move the gate. The physical design, presented in Figure 4, was created using SketchUp software and includes a 3D model visualizing the component configuration within the system. This model facilitated spatial planning and optimized component placement.

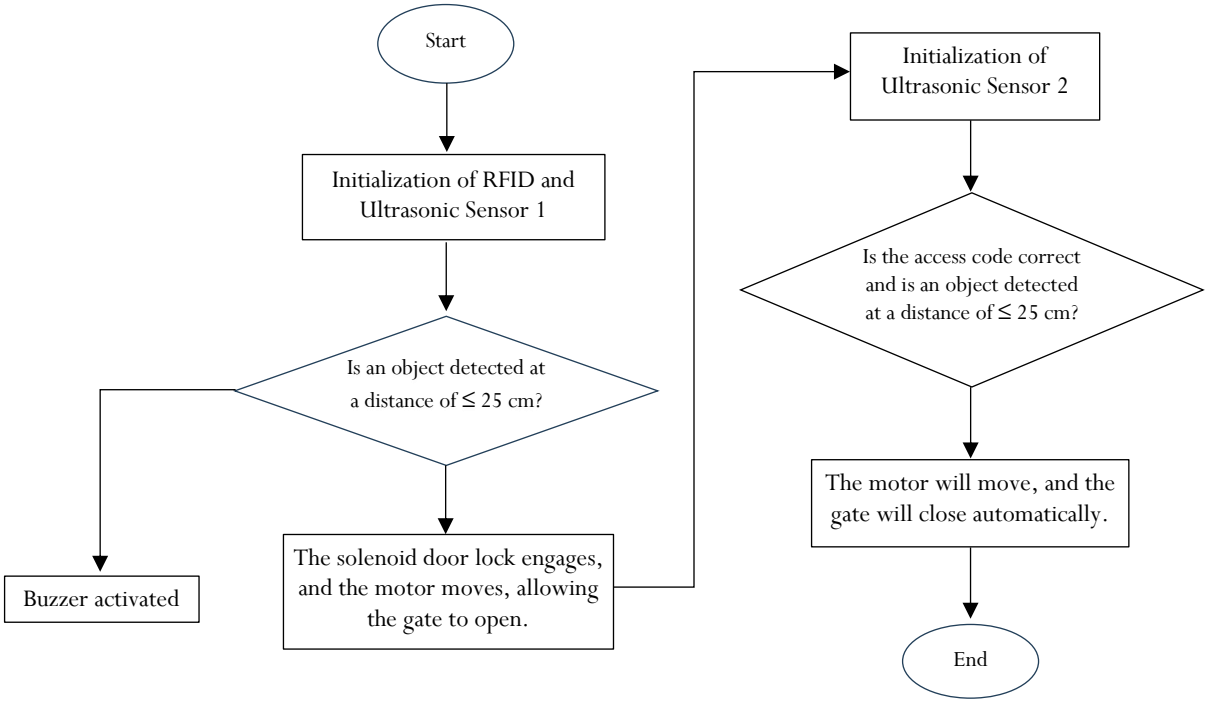
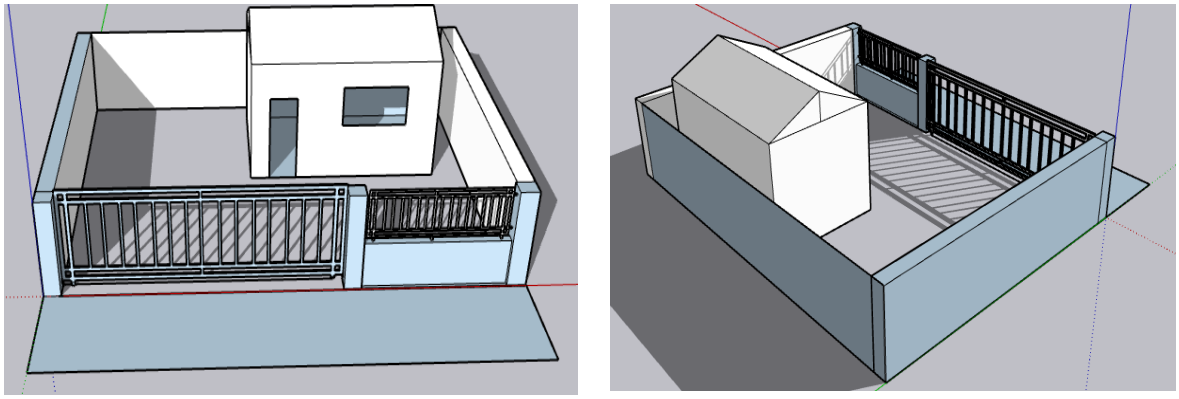


Figure 3. Operational flowchart of automatic fence system



(a) (b)

Figure 4. Physical design of the automatic fence system: (a) Front view, (b) Side view

2.3. Initial Prototyping

During the initial prototyping stage, the primary components of the automatic fence system were assembled and configured to create a basic operational model. This phase validated the functionality of core features and established a foundation for iterative refinement in subsequent development stages.

2.3.1. NodeMCU ESP32 Microcontroller Setup

The NodeMCU ESP32 was chosen as the primary controller for its integrated Wi-Fi and Bluetooth capabilities, essential for IoT applications. The microcontroller was programmed using the Arduino IDE to handle sensor inputs and actuator outputs. The initial code incorporated commands for reading data from ultrasonic sensors and RFID, activating relays, and controlling the gate movement through motor signals.

2.3.2. Blynk Application Configuration

The Blynk application was configured to serve as the user interface on mobile devices, enabling remote control of the fence system. The interface includes buttons for opening and closing the gate and displays widgets for Ultrasonic Sensor 1 and Ultrasonic Sensor 2 to present real-time sensor data. A unique authentication token was used to connect the Blynk app to the NodeMCU, ensuring secure communication over Wi-Fi.

2.3.3. Basic Circuit Assembly

A fundamental circuit was constructed on a breadboard to evaluate component interconnectivity and operational functionality. Ultrasonic sensors were connected to the NodeMCU to detect objects near the gate, with their trigger and echo pins assigned to specific GPIO pins for accurate distance measurements. The relay served as an electronic switch, controlling the solenoid lock and the motor for gate movement. The system was initially powered using 5V and 12V sources to support all components. Figure 5 illustrates the circuit design, detailing component connections and interactions.

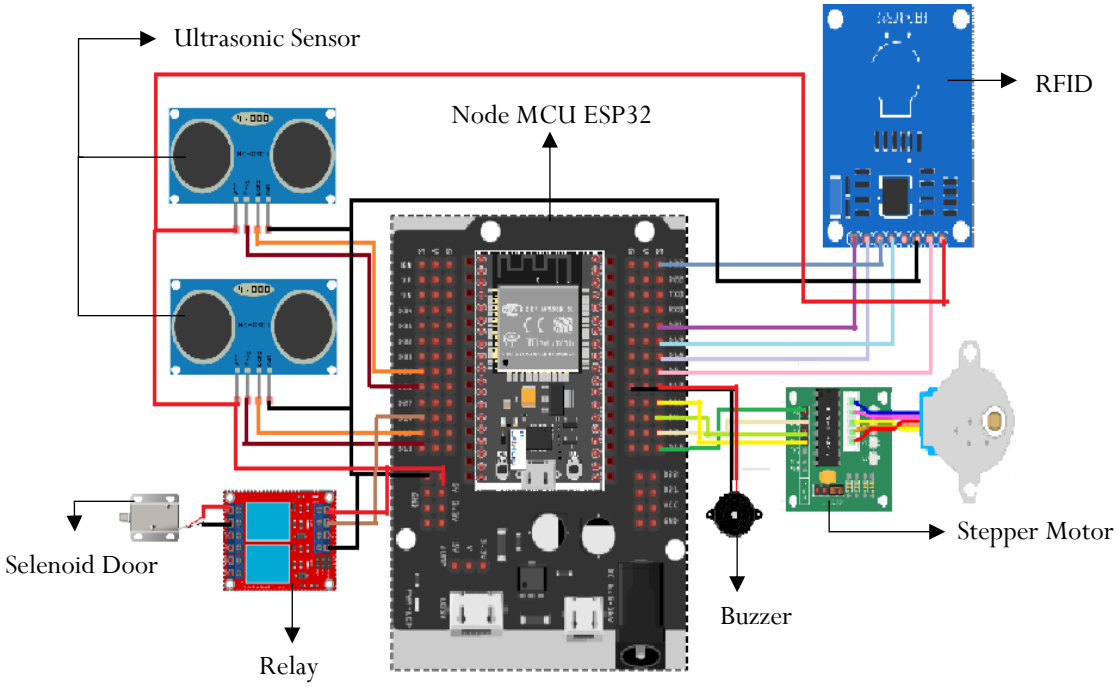


Figure 5. Circuit design layout

2.3.4. Functionality Testing

Each component underwent a series of tests to verify its basic functionality after assembly. The motor was activated to confirm its capability to move the gate, while the ultrasonic sensors were tested for accurate object detection within the designated safety zone. The relay was evaluated for its ability to switch between open and closed states, controlling the solenoid lock and motor based on inputs from the sensors and the Blynk application. Additionally, as shown in Figure 6, the system's response time to remote commands via the Blynk application was measured to ensure that latency remained within acceptable limits, ideally under two seconds. Figure 6 illustrates the Blynk user interface used for remote control of the automatic fence system, highlighting the intuitive design that facilitates real-time interaction with the system.

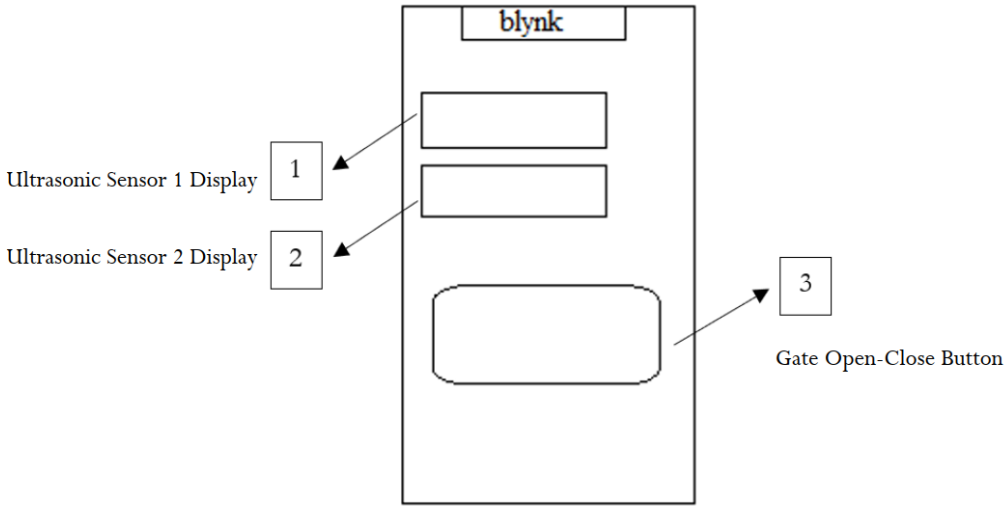


Figure 6. Blynk user interface for remote control of the automatic fence system

2.4. Performance Testing

The performance testing phase assessed the initial functionality and performance of the prototype to ensure it met minimum operational standards. This stage was crucial for identifying potential areas for improvement before further refinement. As detailed below, multiple tests were conducted to evaluate the system's responsiveness, reliability, accuracy, and connectivity.

2.4.1. Latency Testing

Latency testing measured the response time from when a user command was sent via the Blynk application to when the motor activated the gate. This test ensured that the system provided a swift response, ideally within two seconds, to deliver a seamless user experience. Any delays or inconsistencies in response time were documented for further analysis, allowing for adjustments to optimize system performance in future iterations.

2.4.2. Reliability Testing

Reliability was assessed by operating the system repeatedly over an extended period to verify its stability and endurance under continuous use. The goal was to ensure that the system consistently functioned as expected under diverse conditions, achieving a reliability rate of over 95%. This testing phase helped identify any weaknesses in both hardware and software that could affect long-term performance, highlighting areas for potential improvement.

2.4.3. Sensor Accuracy Testing

Sensor accuracy testing focused on the ultrasonic sensors' ability to detect objects within the designated safety zone, ensuring a precise response to nearby objects. The sensors were calibrated to measure distances accurately, halting gate operation when an object entered the safety perimeter. Multiple trials were conducted under varied conditions to assess sensor precision, with sensitivity settings adjusted to enhance detection accuracy.

2.4.4. Connectivity Testing

Connectivity testing was conducted to ensure a stable and reliable Wi-Fi connection between the NodeMCU ESP32 and the Blynk application. Consistent connectivity was critical for seamless remote control and real-time notifications. The system was tested under varying network conditions to assess its ability to maintain uninterrupted communication and minimize latency, thereby supporting effective remote operation.

2.5. Iterative Refinement

During this phase, the system underwent multiple rounds of testing and refinement to optimize its functionality and efficiency. This iterative approach, fundamental to experimental prototyping, allowed for continuously optimizing hardware and software components based on performance data. In each iteration, targeted adjustments addressed specific limitations, such as reducing latency by optimizing command execution code and enhancing sensor accuracy through refined placement and sensitivity settings. Power efficiency improvements were also implemented by programming the NodeMCU ESP32 to enter low-power modes during idle periods. After each modification, the system was retested to verify that the adjustments met the expected performance standards. This process resulted in a reliable and responsive prototype that met all functional and non-functional requirements by the conclusion of this phase.

2.6. Final Prototype Evaluation

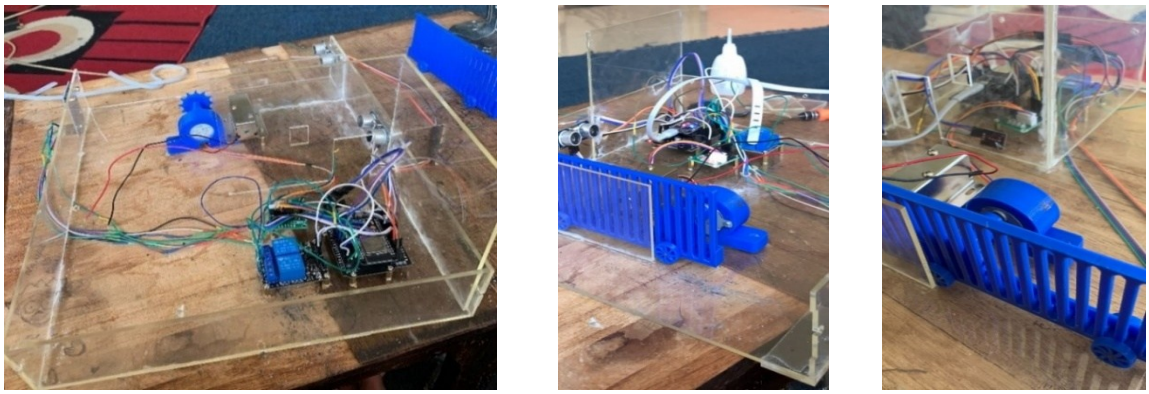
The final prototype evaluation involved comprehensive testing of the fully developed system to validate its functionality and reliability. This included assessing remote control capabilities via the Blynk application, verifying accurate sensor detection within the designated safety zone, and ensuring timely notification delivery. Each feature was thoroughly tested to confirm seamless integration and responsiveness, ensuring the prototype met all predefined operational requirements and provided a user-friendly, reliable experience.

3. RESULTS

3.1. Physical Prototype Overview

The final prototype of the IoT-enabled smart fence, shown in Figure 7, features a user-friendly interface accessible via the Blynk mobile application. This interface allows users to remotely control key functionalities, including opening and closing the gate, with the motor responding promptly to ensure a seamless user experience. Real-time sensor data from the ultrasonic sensors is transmitted to the Blynk app, and if an object is detected within the safety zone, the system automatically halts gate movement, prioritizing user safety. Additionally, a notification system alerts users in real-time whenever the gate is accessed, or movement is detected within the safety zone, informing them of nearby activity.

Figure 7 illustrates three key aspects: (a) the overall IoT-enabled smart fence prototype, showcasing the complete setup of sensors, controllers, and other components; (b) the gate in an open position, with this status displayed on the control application as a visual indicator, allowing users to verify the gate's open status in real-time; and (c) the gate in a closed position, with the system displaying the closed status on the application, confirming that the gate is secure. This real-time monitoring and control capability enables users to manage and observe the gate's status remotely, enhancing security and convenience.



(a) (b) (c)

Figure 7. The final prototype: (a) Complete system setup; (b) Gate in open position; (c) Gate in closed position

3.2. Latency Testing Results

Latency testing measured the time the system took to respond to a command from the Blynk application, reflecting overall responsiveness. Table 1 summarizes these results, documenting the commands sent, response times, and calculated latency in seconds. The quality of the Wi-Fi network was categorized as 'Good,' 'Fair,' or 'Poor,' with notes highlighting any anomalies. Under Good network conditions, latency consistently remained below two seconds, meeting the non-functional requirement of a 95% reliability threshold. Minor delays were observed as network conditions deteriorated, illustrating the relationship between network quality and system responsiveness.

Table 1. Latency testing results

No.	Command Sent Time	Response Time	Latency (seconds)	Network Condition (Good/Fair/Poor)	Notes
1	12:01:05	12:01:07	2	Fair	Acceptable
2	12:02:15	12:02:18	3	Fair	Slight delay due to moderate signal
3	12:03:25	12:03:30	5	Poor	Noticeable delay, network instability
4	12:04:35	12:04:36	1	Good	-
5	12:05:45	12:05:47	2	Fair	Acceptable

3.3. Reliability Testing Results

The reliability testing results include assessments of both hardware and software components to ensure the system operates stably and performs consistently under repeated use.

3.3.1. Hardware Testing Results

Table 2 shows the results of hardware testing under repeated operation. Each component—input (Power Supply, RFID, Ultrasonic Sensors), processing (NodeMCU ESP32), and output (Relay, Stepper Motor, Solenoid Doorlock, and Buzzer)—was tested to ensure stability and consistent performance within the expected voltage ranges.

Table 2. Hardware testing results

No.	Component	Ideal Voltage	Measured Voltage	Status	Notes
1	Power Supply	12 V	11.74 V	Pass	Voltage stable for optimal operation
2	RFID	5 V	4.77 V	Pass	Functions well, with slight variance
3	Ultrasonic Sensor 1	5 V	4.86 V	Pass	Accurate object detection
4	Ultrasonic Sensor 2	5 V	4.94 V	Pass	Accurate object detection
5	NodeMCU ESP32	5 V	4.94 V	Pass	Stable control performance
6	Relay	5 V	4.91 V	Pass	Functions as expected
7	Stepper Motor	5 V	4.94 V	Pass	Reliable motor operation
8	Solenoid Doorlock	12 V	11.76 V	Pass	Engages and disengages effectively
9	Buzzer	5 V	4.91 V	Pass	Sound output as expected

The testing demonstrated that all components operated within the expected voltage ranges, each meeting its functional requirements. These results indicate high hardware reliability, as minimal variance was observed, supporting the system's ability to function effectively over extended periods.

3.3.2. Software Testing Results

The software reliability of the IoT-enabled smart fence was validated by testing the connectivity between the Blynk application and the NodeMCU-controlled gate. The tests confirmed that commands from the Blynk app, such as opening and closing the gate, were executed promptly by the NodeMCU with minimal latency. This quick response highlights the system's compliance with non-functional reliability standards, ensuring smooth and dependable operation (Figure 8). Additionally, real-time sensor readings from the ultrasonic sensors, displayed within the Blynk interface, provided accurate feedback, allowing users to monitor obstacle proximity effectively.

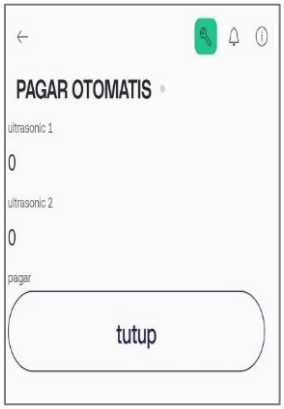


Figure 8. Blynk app interface

3.4. Sensor Accuracy Testing Results

The sensor accuracy testing results, shown in Table 3, demonstrate the ultrasonic sensors' ability to detect objects within the 25 cm safety zone. Most of the tests (6 out of 8) yielded detections within the acceptable tolerance range of ±3 cm, indicating reliable sensor performance. Specifically, the

differences between the actual and detected distances ranged from 0 to 3 cm, which are considered acceptable variances for the system's operational requirements. However, in two instances, the difference exceeded the tolerance range (5 cm and 6 cm, respectively), resulting in detection failures. These discrepancies suggest periodic recalibration is necessary to maintain sensor accuracy and ensure operational reliability. Despite these minor failures, the system consistently demonstrated effective detection, with most results falling within the acceptable tolerance range.

Table 3. Sensor accuracy testing

No.	Actual Distance (cm)	Detected Distance (cm)	Difference (cm)	Detection Success (Yes/No)	Notes
1	25	23	2	Yes	Within tolerance range
2	25	23	2	Yes	Consistent minor variance
3	25	20	5	No	Detection failed; recalibration suggested
4	25	24	1	Yes	Accurate detection, acceptable tolerance
5	25	22	3	Yes	Within acceptable range
6	25	19	6	No	Detection failed; recalibration suggested
7	25	25	0	Yes	Perfect detection
8	25	26	1	Yes	Minor acceptable variance

3.5. Connectivity Testing Results

Connectivity testing assessed the stability of the Wi-Fi connection between the NodeMCU ESP32 and the Blynk application, focusing on the system's ability to maintain low latency and consistent performance under varying network conditions. Under optimal conditions, connectivity remained stable, with latency consistently under 2 seconds. However, under fair and poor network conditions, latency increased to between 2 and 5 seconds, and occasional brief disconnections were observed. These results highlight the system's dependence on network quality, suggesting that improving network robustness could further enhance system reliability.

4. Discussion

This study has successfully demonstrated the effectiveness of an IoT-enabled smart fence in enhancing both home security and user convenience. The system consistently achieved its core functional objectives: responsive remote control, accurate object detection, and real-time notification delivery. Under optimal network conditions, latency remained below 2 seconds, ensuring responsiveness that met user expectations. These results align with prior research on IoT-enabled home automation, highlighting user convenience and real-time control as primary advantages of IoT security solutions [16]. The prototype's performance in these areas underscores its practicality and potential as a viable residential security solution.

Expected results were achieved mainly, such as consistent latency and reliable performance across hardware and software components. However, unanticipated latency variation was observed under fair and poor network conditions, highlighting the system's dependence on stable network quality—an inherent limitation in IoT applications [17]. This finding suggests that future designs could incorporate

advanced connectivity strategies, such as dual-mode connectivity (Wi-Fi and Bluetooth), to mitigate latency fluctuations in varying network conditions. Additionally, sensor accuracy testing revealed slight deviations at specific distances, which is consistent with prior studies on ultrasonic sensor calibration sensitivity [18]. Addressing this sensitivity through improved calibration techniques could enhance the system's reliability and safety, particularly in environments with children or pets.

The system integrates real-time notifications, automatic gate halting upon obstacle detection, and mobile control via the Blynk application, marking an advancement over traditional manually operated systems [19]. Previous research underscores the advantages of automated home security, including continuous monitoring and rapid response capabilities [20], [21]. This prototype further extends these benefits by consolidating multiple IoT functionalities into a cohesive and user-friendly system. These findings highlight the growing relevance of IoT in smart home security, with this system offering a more integrated and responsive experience than conventional setups.

Sensor accuracy testing confirmed that the ultrasonic sensors detected objects within the designated safety zone with high precision, triggering the automatic halting of the gate to prevent accidental contact. While minor inaccuracies were observed at certain distance thresholds, these deviations did not compromise user safety. Future iterations could benefit from improved calibration techniques to minimize detection variance, particularly in environments with small children or pets. Additionally, implementing protective housing for the sensors could enhance durability and performance, especially in outdoor settings where exposure to weather conditions may affect sensor functionality [22], [23].

Several challenges were encountered, primarily related to network dependency. Connectivity testing revealed that network quality directly impacts system performance, with increased latency and occasional brief disconnections observed under poor network conditions [24]. This limitation highlights the need for enhanced connectivity solutions, such as dual-mode Wi-Fi and Bluetooth support, to ensure reliable operation in low-signal environments. These improvements would enable seamless performance even under variable network conditions, strengthening the system's resilience and expanding its applicability in diverse residential settings.

This study contributes to IoT-enabled home security by presenting a user-centered, practical approach to automated safety. The results demonstrate the feasibility of scalable IoT applications in residential security, and the successful implementation of this prototype underscores its potential for integration into comprehensive smart home systems, including surveillance, emergency alerts, and other security functionalities [20], [25]. This IoT-enabled system could significantly advance home automation by addressing the identified limitations and enhancing connectivity options, aligning with the growing demand for connected user-friendly, innovative security solutions.

5. CONCLUSION

In conclusion, this study's IoT-enabled smart fence successfully met its primary objectives of enhancing residential security and user convenience. The system demonstrated reliable latency, operational stability, accuracy, and connectivity performance, meeting or exceeding expectations across these parameters. Several improvements are proposed to enhance functionality and resilience further. Integrating dual connectivity options, such as Wi-Fi with Bluetooth fallback, could address network instability issues and ensure continuous operation under suboptimal conditions. Future iterations could also benefit from enhanced sensor calibration and protective housing to improve detection accuracy and durability, especially in outdoor environments. Upgrading the Blynk interface with customizable alerts and expanded monitoring features, such as access logs, could enhance the user experience and strengthen the system's

security. This study contributes to IoT-enabled security solutions by presenting a practical, user-centered approach to home automation, aligning with current trends emphasizing security, convenience, and connectivity. The successful implementation of this prototype not only demonstrates the feasibility of IoT applications in residential security but highlights its potential for scalability and integration into broader smart home systems, including surveillance and emergency alert functionalities.

DECLARATIONS

Author Contributions

Fadhilah Putri Syahrani: Conceptualization, Methodology, Investigation, Formal Analysis, Data Curation, Software, Writing - Original Draft, Writing - Review & Editing. **Hadi Kurnia Saputra:** Validation, Supervision, Writing - Review & Editing. **Sartika Anori:** Validation, Supervision, Writing - Review & Editing. **Winda Agustiarmi:** Validation, Supervision, Writing - Review & Editing. **Firas Tayseer Ayasrah:** Validation, Writing - Review & Editing. **Pham Van Thanh:** Writing - Review & Editing. All authors have reviewed and approved the final version of this manuscript.

Acknowledgments

The authors would like to express their sincere gratitude to all individuals and institutions who provided invaluable support and resources throughout the research process.

Ethical Approval

This study did not involve human or animal participants; therefore, ethical approval was not required.

Competing Interests

The authors declare that they have no competing interests.

Funding

This research received no external funding.

Generative AI and AI-Assisted Technologies Statement

While preparing this manuscript, the author(s) used ChatGPT and Grammarly to enhance its readability, language, and overall structure. Following these tools, the author(s) performed a comprehensive review and editing process to ensure the content's accuracy, integrity, and quality. The author(s) accept full responsibility for the content and conclusions presented in this publication.

REFERENCES

[1] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends, and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[2] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, "A review and state of the art of Internet of things (IoT)," *Arch. Comput. Methods Eng.*, vol. 29, no. 3, pp. 1395–1413, May 2022, doi: 10.1007/s11831-021-09622-6.

[3] M. A. Rahman et al., "A cloud-based cyber-physical system with industry 4.0: Remote and digitized additive manufacturing," *Automation*, vol. 3, no. 3, pp. 400–425, Aug. 2022, doi: 10.3390/automation3030021.

[4] P. Marwedel, *Embedded System Design*, 2nd ed. Springer, 2021, doi: 10.1007/978-3-030-60910-8.

[5] M. Ojha and R. Sikka, "An overview on applications of microcontroller," *Int. J. Innov. Res. Eng. Manag.*, vol. 8, no. 6, pp. 4020–4405, 2021. [Online]. Available: https://acspublisher.com/journals/index.php/ijirem/article/view/11574

[6] D. Hercog, T. Lerher, M. Truntič, and O. Težak, "Design and implementation of ESP32-based IoT devices," *Sensors*, vol. 23, no. 15, p. 6739, Jul. 2023, doi: 10.3390/s23156739.

[7] J. Eriksson and T. Nilson, "The house as a machine for living: Dreams of domestic automation, 1923–2023," in *The De Gruyter Handbook of Automated Futures: Imaginaries, Interactions, and Impact*, vol. 2, p. 105, 2024.

[8] W. A. Jabbar et al., "Design and fabrication of smart home with Internet of Things enabled automation system," *IEEE Access*, vol. 7, pp. 144059–144074, 2019, doi: 10.1109/ACCESS.2019.2942846.

[9] D. C. Khedekar, A. C. Truco, D. A. Oteyza, and G. F. Huertas, "Home automation—A fast-expanding market," *Thunderbird Int. Bus. Rev*, vol. 59, no. 1, pp. 79–91, Jan. 2017, doi: 10.1002/tie.21829.

[10] K. Scheerlinck and Y. Schoonjans, "Garden streetscapes: Front yards as territorial configurations," *Landsc. Rev.*, vol. 16, no. 2, Sep. 2016, doi: 10.34900/lr.v16i2.955.

[11] M. West, "Preventing System Intrusions," in *Network and System Security, 2nd ed., Elsevier, 2014*, pp. 29–56, doi: 10.1016/B978-0-12-416689-9.00002-2.

[12] C. Zechmeister, M. Gil Pérez, J. Knippers, and A. Menges, "Concurrent, computational design and modeling of structural, coreless-wound building components," *Autom. Constr.*, vol. 151, p. 104889, Jul. 2023, doi: 10.1016/j.autcon.2023.104889.

[13] G. Fortino, C. Savaglio, G. Spezzano, and M. Zhou, "Internet of things as a system of systems: A review of methodologies, frameworks, platforms, and tools," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 51, no. 1, pp. 223–236, Jan. 2021, doi: 10.1109/TSMC.2020.3042898.

[14] E. Sherif, W. Helmy, and G. H. Galal-Edeen, "Proposed framework to manage non-functional requirements in agile," *IEEE Access*, vol. 11, pp. 53995–54005, 2023, doi: 10.1109/ACCESS.2023.3281195.

[15] A. S. Rao et al., "Real-time monitoring of construction sites: Sensors, methods, and applications," *Autom. Constr.*, vol. 136, p. 104099, Apr. 2022, doi: 10.1016/j.autcon.2021.104099.

[16] J. Singh, D. Singh, L. Verma, and S. Singh, "IoT-based remote control and monitoring of electrical appliances," *Int. J. Digit. Technol.*, vol. 3, no. 1, p. 74, Jun. 2024. [Online]. Available: https://journal.nielit.edu.in/index.php/01/article/view/107

[17] S. Dilek, K. Irgan, M. Guzel, S. Ozdemir, S. Baydere, and C. Charnsripinyo, "QoS-aware IoT networks and protocols: A comprehensive survey," *Int. J. Commun. Syst.*, vol. 35, no. 10, p. e5156, Jul. 2022, doi: 10.1002/dac.5156.

[18] A. R. Lawson *et al.*, "Multi-site calibration and validation of a wide-angle ultrasonic sensor and precise GPS to estimate pasture mass at the paddock scale," *Comput. Electron. Agric.*, vol. 195, p. 106786, Apr. 2022, doi: 10.1016/j.compag.2022.106786.

[19] A. Jain, S. Singh, P. S. Chauhan, and A. Shukla, "Management of COVID-19 patients through IoT-based smart ambu bag," in *Distributed Intelligence in Circuits and Systems*, pp. 181–215, Jan. 2024,

doi: 10.1142/9789811279539_0006.

[20] B. Hammi, S. Zeadally, R. Khatoun, and J. Nebhen, "Survey on smart homes: Vulnerabilities, risks, and countermeasures," *Comput. Secure.*, vol. 117, p. 102677, Jun. 2022, doi: 10.1016/j.cose.2022.102677.

[21] W. Li, T. Yigitcanlar, I. Erol, and A. Liu, "Motivations, barriers, and risks of smart home adoption: From a systematic literature review to the conceptual framework," *Energy Res. Soc. Sci.*, vol. 80, p. 102211, Oct. 2021, doi: 10.1016/j.erss.2021.102211.

[22] Y. Zhang, A. Carballo, H. Yang, and K. Takeda, "Perception and sensing for autonomous vehicles under adverse weather conditions: A survey," *ISPRS J. Photogramm. Remote Sens.*, vol. 196, pp. 146–177, Feb. 2023, doi: 10.1016/j.isprsjprs.2022.12.021.

[23] H. Omidvarborna, P. Kumar, J. Hayward, M. Gupta, and E. G. S. Nascimento, "Low-cost air quality sensing towards smart homes," *Atmosphere*, vol. 12, no. 4, p. 453, Apr. 2021, doi: 10.3390/atmos12040453.

[24] V. Demiroglou, S. Skaperas, L. Mamatas, and V. Tsaoussidis, "Adaptive multiprotocol communication in smart city networks," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 20499–20513, Jun. 2024, doi: 10.1109/JIOT.2024.3372624.

[25] T. Magara and Y. Zhou, "Internet of things (IoT) for smart homes: Privacy and security," *J. Electr. Comput. Eng.*, vol. 2024, no. 1, p. 7716956, Jan. 2024, doi: 10.1155/2024/7716956.

AUTHOR BIOGRAPHIES

Fadhilah Putri Syahrani is a faculty member in the Electronics Engineering Education Program at Universitas Negeri Padang, specializing in embedded systems, microcontrollers, and electronics education. Her research interests include developing innovative methods and applications in embedded systems and microcontroller-based projects to enhance electronics education.

Hadi Kurnia Saputra is a lecturer at Universitas Negeri Padang, teaching information technology and security courses. Born in Mandailing Natal, North Sumatra, he holds a bachelor's degree in Electronics Engineering Education from Universitas Negeri Padang (2009) and a master's degree in Computer Science from Universitas Putra Indonesia (2015). His research focuses include information technology and computer networks, with extensive experience in these areas.

Sartika Anori is a lecturer at Universitas Negeri Padang with six years of experience in vocational education, specializing in electronics. She has published widely in vocational and electronics education, and her current research focuses on advancements in electronics engineering.

Winda Agustiarmi is a Department of Electronics Engineering lecturer at Universitas Negeri Padang. She specializes in vocational education (electronics) and control systems, with interests in electronics systems engineering technology. Her research focuses on developing effective teaching methods in electronics education and advancing control systems applications.

Firas Tayseer Ayasrah is an assistant professor at Al Ain University, UAE, specializing in artificial intelligence (AI) and educational technology. Holding a Ph.D. in educational technologies, Ayasrah's research focuses on AI integration in educational platforms, digital learning environments, and AR/VR, with numerous publications in reputable journals. His work aims to advance AI-powered educational technologies to enhance learning experiences in higher education.

Pham Van Thanh is a lecturer at Dong Nai Technology University, Faculty of Engineering, in Bien Hoa City, Vietnam. He has six years of experience in vocational education and specializes in electronics and automotive engineering. His academic focus has been on IoT applications and automation systems, with a particular interest in developing practical solutions for enhanced security and remote monitoring.