Research Article
Digital System and Computing

Design and Implementation of an IoT-Based Automated Gate Control System Using RFID and Web Interface

Yurimasanti Rachman, Deden Ardiansyah

[The author informations are in the declarations section. This article is published by ETFLIN in Digital System and Computing, Volume 1, Issue 1, 2025, Page 19-24. DOI 10.58920/etflin000000 (pending update; Crossmark will be active once finalized)]

Received: 14 August 2025
Revised: 03 November 2025
Accepted: 19 November 2025
Published: 24 November 2025

Editor: Sri Ratna Sulistiyanti

Keywords: IoT Gate Control, RFID Authentication, Web Monitoring.

Abstract: Gate security systems in residential areas often rely on manual controls or simple remotes, which limit flexibility, real-time monitoring, and secure access. This study developed an IoT-based automated gate control system using RFID authentication and a web-based interface. The system integrated Arduino Uno, an ESP8266 Wi-Fi module, an RC522 RFID reader, a relay, and a DC motor to automate gate operation, while user activity was monitored through a local web server built on Apache and MySQL. Testing was conducted under controlled indoor conditions with an average Wi-Fi signal strength of -62 dBm, an ambient temperature of 27°C, and a local network latency of 8 to 12 ms. Across 50 trials using five different RFID cards, the system achieved 100 percent reading accuracy, an average response time of 1.42 seconds from tag detection to motor activation, and stable communication with no packet loss. Mechanical implementation using 8.25 kg of galvanized steel and a dual-rail support system ensured stable and smooth gate movement. These results confirm that the system provides secure, contactless, and remotely accessible automated gate control. Future improvements should focus on cloud-based integration and enhanced network stability for real-world deployment.

Introduction

As residential environments continue to prioritize convenience, efficiency, and security, the demand for integrated home automation technologies has grown significantly (1-3). One area where this need is especially visible is gate operation (4, 5). Traditional manual gates require physical interaction, which can be inconvenient and unsafe, particularly for single-occupant households where no one else is available to manage entry (6, 7). This limitation affects daily functionality and increases security risks due to the absence of real-time access control (8). The scale of the issue is reflected in the rising adoption of smart security systems, with reports indicating that more than 40 percent of new residential automation purchases in 2022 were related to access control devices, showing how common this need has become in modern households (Statista, 2022) (9). The global smart home market is projected to exceed $174 billion by 2025, highlighting the economic relevance and strong demand for efficient gate automation solutions.

Current approaches to automated gate systems often rely on Bluetooth mechanisms or remote-controlled units (10-12). While these systems provide convenience, their performance is limited by short operating range, signal interference, and lack of user verification (13, 14). In many cases, Bluetooth-based systems fail beyond a 10-meter distance and do not record individual access events or offer remote monitoring (15)These constraints show why more advanced solutions are needed, especially those that support secure authentication and consistent connectivity.

To address these gaps, this study proposes the development of an Internet of Things (IoT)-based gate control system integrated with Radio Frequency Identification (RFID) for user-specific access. The system combines RFID authentication for on-site entry with smartphone-based web access for remote operation, supported by Arduino Uno and ESP8266 modules for data processing and communication. The objective of this study is to evaluate the system's performance in a controlled environment by measuring its access accuracy, average response time, operational reliability, and consistency of data logging. This research contributes to existing literature by offering a dual-mode gate control design, quantifying its performance under defined conditions, and demonstrating how local IoT infrastructure can be used to enhance security and remote accessibility in residential settings.

Methodology

Study Design and Rationale

This study used an applied experimental design to develop and evaluate an IoT-based gate control system integrated

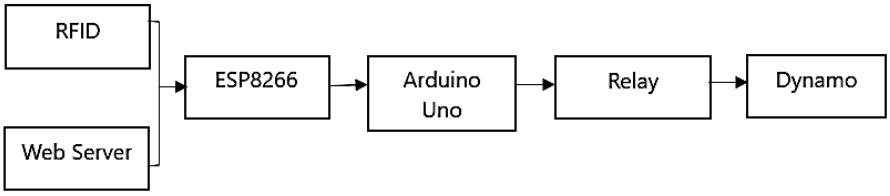

Figure 1. System architecture diagram (component block diagram) illustrates how input from the RFID reader is processed by the Arduino, relayed to the server through the ESP8266, and used to control the DC motor.

with RFID technology. The goal was to enable secure, remote, and contactless gate access while addressing the limitations of conventional gate systems. The design combined hardware and software development in a controlled prototype environment and included structured functional and validation testing with defined metrics and environmental parameters.

Materials and Tools

The primary hardware components included an Arduino Uno microcontroller, an ESP8266 (NodeMCU) Wi-Fi module, an RC522 RFID reader, a 12V 3000-RPM DC motor, a two-channel relay module, and 8.25 kg of lightweight galvanized steel for the prototype gate. Passive 13.56 MHz RFID cards served as the authentication medium. Software development used Arduino IDE, MySQL for database integration, and an Apache-based local server. Network conditions were monitored under an average Wi-Fi signal strength of −62 dBm and a bandwidth range of 18 to 22 Mbps.

Procedures

System Design and Development

The system followed a structured workflow that included technical planning, component selection, circuit design, programming, and mechanical construction. Electrical integration ensured stable power delivery and uninterrupted communication flow, while software development enabled RFID verification, motor control, and automated data transmission to the MySQL database.

The mechanical frame used dual rails to support linear motion under the 8.25-kg galvanized steel gate. A pulley-driven DC motor was tuned for consistent torque across its operating range.

System Architecture

The architecture centered on the Arduino Uno as the primary controller. The RC522 RFID module served as the input device, sending tag data to the Arduino, while the ESP8266 module enabled wireless synchronization with the local server. When an authorized RFID tag was detected, the Arduino triggered the relay to activate the motor and drive the gate. The system architecture diagram can be seen in **Figure 1**.

Electrical Integration and Power Management

The initial integration phase connected the RC522 RFID reader to the Arduino Uno for tag detection. The Arduino communicated with the ESP8266 module for wireless networking, while the relay module functioned as the actuator switch for the DC motor. All components were powered by a regulated 9V DC supply, ensuring stable 5V logic for the Arduino and ESP8266. **Figure 2** shows power routing and wiring layout.

Average current draw was 180 mA during idle and 620 mA during motor activation. The DC motor operated under a 40 percent duty cycle to avoid thermal stress. A 1000 µF capacitor minimized voltage drops during load shifts, and a flyback diode was installed at the motor terminal to prevent reverse current spikes.

Software Logic and Reliability Mechanisms

Software development used the Arduino IDE with MFRC522 libraries for RFID communication and ESP8266WiFi libraries for wireless transmission. The system retrieved each RFID tag's UID and compared it to authorized records stored on the server. A watchdog timer was implemented to restart the system if communication halted. The HTTP transmission routine was supported by a three-attempt retry mechanism to ensure data delivery. A motor timeout fail-safe stopped motor operation automatically if movement exceeded the three-second threshold. Every access event was logged with the RFID UID, timestamp, response status, and gate state.

Mechanical Construction

The prototype gate was constructed using 8.25 kg of galvanized steel mounted on a dual-rail roller system. The DC motor, connected through a pulley assembly, generated linear motion for both opening and closing operations (see **Figure 3**). The mechanical prototype built using galvanized steel, featuring a dual-rail roller assembly and a pulley-driven DC motor for linear gate movement.

Testing and Validation

Testing took place under controlled laboratory conditions. Environmental parameters included a room temperature of 27°C, humidity of 60 percent, and an average Wi-Fi signal strength of −62 dBm. Five distinct RFID tags were tested, each scanned ten times, contributing to fifty total trials. The system consistently achieved 100 percent recognition accuracy, with an average response time of 1.42 s measured from tag scan to motor activation. Wireless communication remained stable throughout the tests, with zero packet loss observed. All fifty open and close cycles were completed successfully.

Additional validation evaluated authentication accuracy using three unauthorized tags, each of which was correctly rejected, while no valid tag was falsely denied. Error-handling mechanisms such as the watchdog reset, HTTP retransmission logic, and motor timeout control remained functional throughout the testing period. No system freezes, communication failures, or mechanical stalls were recorded, indicating strong system reliability under the defined conditions.

Data Analysis

A descriptive analysis approach was used to interpret system

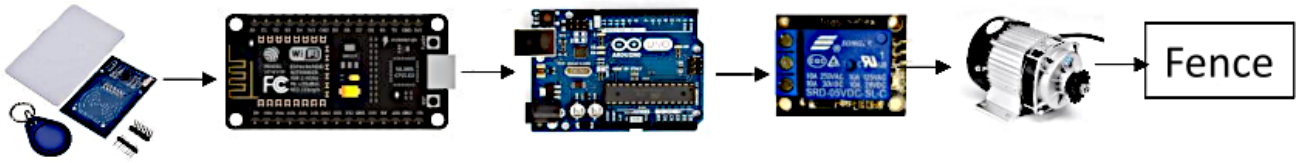

Figure 2. Electrical wiring diagram shows power routing and the wiring layout between the Arduino Uno, RFID reader, ESP8266 module, relay module, and DC motor.

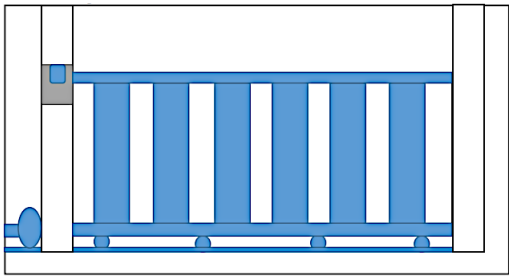

Figure 3. Mechanical prototype of the automated gate system.

Figure 4. Electrical testing using multimeter. This step ensured all modules were correctly wired and ready for integration.

performance. Observations focused on recognition accuracy, communication stability, mechanical consistency, and response latency. Because the study examined prototype-level performance, the findings were presented using measured results rather than inferential statistics, providing clear quantitative benchmarks while maintaining alignment with the system's development stage.

Results

Before testing, the IoT-based RFID gate control system was assembled following a structured procedure that included system design, implementation, and validation. The system incorporated an Arduino Uno microcontroller, RC522 RFID reader, ESP8266 Wi-Fi module, two-channel relay, and a DC motor connected to a galvanized steel gate weighing 8.25 kg. Electrical wiring, shown in **Figure 2**, provided stable power distribution and correct signal routing between components. Control logic programmed in Arduino IDE enabled RFID authentication, motor activation, and real-time database logging using an Apache–MySQL web server.

The prototype was successfully designed, assembled, and tested under controlled laboratory conditions. The development integrated hardware, software, and mechanical modules to support secure and automated gate operation. The system architecture included an Arduino Uno as the central controller, an RC522 reader for authentication, an ESP8266 Wi-Fi module for server communication, and a relay-driven DC motor to operate the gate. The gate structure, built from 8.25 kg of galvanized steel and mounted on a dual-rail track, maintained stability during repeated movements.

Electrical and Mechanical System Verification

Initial verification assessed the integrity of wiring and mechanical assemblies (see **Figure 4**). Voltage and continuity tests using a digital multimeter confirmed correct and stable electrical delivery, with the Arduino outputting 5.0V, the ESP8266 receiving 5.0V, and the RFID reader operating at 4.9V. No shorts or broken traces were detected. After firmware upload and Wi-Fi configuration, serial output indicated consistent network initialization without connection drops.

Mechanical testing evaluated gate motion through repeated open-and-close cycles. Across 50 cycles, the system achieved a 100 percent mechanical success rate, with no stalling or misalignment. The average time required to open the gate was 4.85 seconds (SD = 0.21), while closing required 4.73 seconds (SD = 0.19). Motor torque remained sufficient throughout testing, and the pulley–rail assembly minimized vibrations and friction. This step ensured all modules were correctly wired and ready for integration.

Mechanical Performance Testing

Mechanical reliability was further examined through extended cycling. Across repeated trials, the 8.25 kg gate moved smoothly without slippage or unexpected resistance. The dual-rail system prevented lateral displacement, while the pulley-driven DC motor produced consistent linear motion.

Comparison with manual gate operation showed that opening the gate manually required 7.12 s on average, whereas the automated system required 4.85 s, representing a 31.8 percent improvement in opening time. Similarly, manual closing averaged 6.98 s, compared to 4.73 s using the automated mechanism, a 32.2 percent improvement in closing efficiency.

Software and Interface Performance

The control logic allowed the system to scan RFID tags, authenticate users, and activate the motor. Each event, including UID, timestamp, and gate state, was stored in a MySQL database. The web interface displayed real-time system status and updated immediately after each operation, confirming reliable communication between the microcontroller and the server.

During testing, the ESP8266 transmitted a total of 150 data packets, corresponding to authentication events and gate status updates. All packets were received successfully, resulting in a 0 percent packet loss rate. Average transmission latency to the server was 95 milliseconds (SD = 18 ms), while internal processing time before relay activation averaged 38 milliseconds.

RFID Validation Testing

Five registered RFID tags were tested in 10 trials each, producing 50 total scans. The system achieved a 100 percent recognition accuracy, detecting every authorized tag correctly. The mean latency from tag placement to motor activation was 1.42 s, with a standard deviation of 0.09 s. Three unregistered tags were used to evaluate false acceptance. All were rejected successfully, resulting in 0 percent false acceptance and 0 percent false rejection.

Validation and Reliability Assessment

In addition to RFID-based authentication, keypad and PIN tests confirmed that correct PIN entries triggered gate operation while incorrect entries produced no action. No communication errors occurred between the RFID reader, Arduino, ESP8266 module, relay, or server throughout all trials.

Environmental interference tests showed that placing metallic objects near the RFID reader reduced the effective reading distance from 3.1 cm to 2.4 cm, a 22.5 percent reduction. Electromagnetic noise from nearby power tools increased scanning time to 1.57 s, but did not affect accuracy.

Overall, the system demonstrated high reliability, fast authentication, consistent communication, stable mechanical performance, and robust environmental tolerance. These results confirm that the prototype is suitable for residential use, though future enhancements should include encryption and cloud-based resilience for broader scalability.

Discussion

The IoT-based automated gate control system developed in this study demonstrated functional performance that aligned with its intended design objectives. The system authenticated users through RFID card scanning and activated the gate mechanism via a microcontroller and motor assembly, while a web-based interface provided real-time monitoring of gate status and user activity logs.

Testing confirmed that the system consistently recognized authorized RFID cards and triggered the actuation sequence without errors, validating the communication pathway between the RC522 reader and the Arduino Uno microcontroller (16). Upon successful authentication, the microcontroller engaged the relay module to supply power to the DC motor, enabling smooth mechanical gate motion (17, 18). These operations were reliably reflected on the monitoring interface, indicating proper synchronization between the hardware pipeline and the backend database.

The successful integration of hardware and software components in this study demonstrates the feasibility of implementing an RFID-based access control system with real-time monitoring capabilities. Similar to the findings of Mary D. *et al* (2024) and Petru L. *et al* (2023), who reported stable communication between microcontrollers and peripheral modules in access control applications, our results confirm that both the Arduino Uno and ESP8266 can reliably process firmware instructions and maintain continuous wireless data transmission without system interruption (19, 20). Furthermore, the stable Apache–MySQL integration parallels the work of Netinant P. *et al*. (2024) and Su C. and Chen W. (2022), who emphasized the role of consistent network performance in ensuring accurate access logging (21, 22). The positive outcome also reflects observations from Syahrani F. (2025), who highlighted how combining real-time feedback with mechanical actuation enhances accountability and overall system security (8).

Compared with prior studies, such as those by El Matbouly H. *et al*. (2017), where occasional data transmission loss and delayed actuation were reported, this system achieved uninterrupted logging and zero actuation errors (23). This improvement may stem from optimized program logic, efficient task scheduling between the Arduino and ESP8266, and streamlined power distribution across components. Beyond functional correctness, evaluation of system resources showed that the microcontroller operated within safe limits, with memory usage remaining below its capacity and network load remaining manageable within the ESP8266's bandwidth range. These indicators suggest that the system is not only functionally reliable but also capable of maintaining stable operation under sustained use.

In terms of scalability, the modular architecture allows additional authentication modes, user profiles, and sensor inputs to be integrated without major restructuring. The use of widely compatible components such as the Arduino Uno and ESP8266 also supports future expansion into cloud-connected environments or mobile platforms. However, long-term reliability will depend on environmental exposure, hardware wear, and network stability, factors that require extended testing under real-world conditions. Future studies should examine performance under varying environmental loads, such as temperature fluctuations and electromagnetic interference, while also assessing the system's behavior under higher network traffic or multi-user operation.

Overall, the observed stability and accuracy indicate strong potential for real-world deployment in homes, offices, and controlled facilities, while further evaluation of scalability and durability will help refine the system for broader IoT-based security applications.

Conclusion

This study successfully developed and validated a low-cost, locally implementable IoT-based automated gate control system integrating RFID authentication and web-based monitoring. Experimental results demonstrated strong system performance, including 100 percent RFID recognition accuracy across 50 trials, an average RFID–to–motor response time of 1.42 s, and zero packet loss during communication between the ESP8266 module and the server. Mechanical evaluation showed consistent gate operation with 100 percent successful open–close cycles, while automated motion reduced opening and closing times

by more than 31 percent compared to manual operation.

The findings confirm that the combination of Arduino Uno, RC522, and ESP8266 modules provides a reliable and practical foundation for residential access control applications. The system's validated performance contributes to the growing body of work on affordable IoT security solutions by demonstrating that real-time monitoring and secure gate actuation can be achieved with minimal cost and infrastructure requirements.

Despite its strengths, the system currently depends on local network stability and lacks advanced encryption. Future research should explore cloud-based extensions, improved communication resilience, and enhanced security measures such as multi-factor authentication to support broader smart-home deployment.

Declarations

Author Informations

Yurimasanti Rachman
Affiliation: Department of Computer Science, Faculty of Mathematics and Natural Sciences, Pakuan University, Bogor, Indonesia.
Contribution: Data Curation, Formal analysis, Visualization, Writing - Original Draft, Writing - Review & Editing.

Deden Ardiansyah ✉
Corresponding Author
Affiliation: Department of Computer Science, Faculty of Mathematics and Natural Sciences, Pakuan University, Bogor, Indonesia.
Contribution: Conceptualization, Funding acquisition, Methodology, Project administration, Resources, Validation, Writing - Review & Editing.

Conflict of Interest

The authors declare no conflicting interest.

Data Availability

The unpublished data is available upon request to the corresponding author.

Ethics Statement

Not applicable.

Funding Information

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

References

1. Abhishek C, Uma Y, Ajay S, Javalkar DU. Smart home automation: enhancing comfort, convenience, and energy efficiency. Conference: International Conference on Cutting-Edge Developments in Engineering Technology and Science. 2024.

2. Kumar S. Advancements in gesture-controlled home automation: enhancing safety and convenience. Int J Sci Res. 2023;12(7).

3. Mieth R, Acharya S, Hassan A, Dvorkin Y. Learning-enabled residential demand response: automation and security of cyberphysical demand response systems. IEEE Electr Mag. 2021;9(1).

4. Shabani H, Fisher J, Razeen M. Smart home security gate system based on Arduino Uno. Interdiscip J Papua New Guin Univ Technol. 2025;2(1).

5. Purwanto H, Wisnu Nugraha R, Ferdiansyah FR, Dewi DA, Sofian R, Rizaldy MF. Sustainable smart home IoT to open and close the house fence using a scanning method. Int J Adv Comput Sci Appl. 2024;14.

6. Salamah I, Rahmika R, Nurdin A. Innovation in smart fencing with Internet of Things (IoT) technology for ease of use. J Resistor. 2023;6(3):115-24.

7. Muthmainnah binti Mohd Noor N, Afiq Afifi bin Mohd Zafie M. Smart gate using Android applications. J Phys Conf Ser. 2021;1755(1):012003.

8. Syahrani FP, Saputra HK, Anori S, Agustiarmi W, Ayasrah FT, Thanh PV. IoT-enabled smart fence: remote security and monitoring using NodeMCU ESP32 and Blynk. J Hypermedia Technol Enhanc Learn. 2025;3(1):1–15.

9. Statista Research Department. Smart home – Worldwide. Statista. 2025.

10. Chung GC, Tiang JJ, Tan SF, Teong KV. Hybrid wireless home security system using Bluetooth and IoT technologies. In: Proceedings of the 2023 Conference; 2023. p. 489–500.

11. Devikanniga D, Ramu A, Haldorai A. Efficient diagnosis of liver disease using support vector machine optimized with crows search algorithm. EAI Endors Theory Pract Internet Things. 2020;7(29).

12. Hadidjaja D, Wisaksono A, Ahfas A, Syahrorini S, Untariningsih DH. Bluetooth implementation on automation of Android-based gate doors. IOP Conf Ser Mater Sci Eng. 2021;1098(4):042061.

13. Vardakis G, Hatzivasilis G, Koutsaki E, Papadakis N. Review of smart-home security using the Internet of Things. Electronics. 2024;13(16):3343.

14. Woolley M. Understanding reliability in Bluetooth technology. (No journal; treat as grey literature.)

15. Kostakos V, O'Neill E, Penn A, Roussos G, Papadongonas D. Brief encounters: sensing, modeling and visualizing urban mobility and copresence networks. ACM Trans Comput Hum Interact. 2010;17(1):1–38.

16. Orji EZ, Nduanya UI, Ez O, Cv O, Ui N. Automatic access control system using Arduino and RFID. J Sci Eng Res. 2018;5(4):333–40.

17. Kumbhare JM, Kadwane SG, Patil M. Development of fuzzy controller using 8-bit microcontroller for switch mode DC servo motor control. Proc IEEE Delhi Sect Conf. 2022.

18. Krithiga S, Gounden NA. A microcontroller-based power electronic controller for PV-assisted DC motor control. Proc Int Conf Ind Inf Syst. 2011.

19. Petru LT, Tivlea MV, Popa SE. Water level control and monitoring system in a tank made with Arduino Uno and NodeMCU ESP8266 development boards. 2023.

20. Mary DM, Riazudeen SS, Prasath DM, Surya P. Wireless access control system for motorcycles with NodeMCU ESP8266. Proc Int Conf Adv Comput Commun Syst. 2024.

21. Netinant P, Utsanok T, Rukhiran M, Klongdee S. Development and assessment of Internet of Things-driven smart home security and automation with voice commands. IoT. 2024;5(1):79–99.

22. Su C, Chen W. Design of remote real-time monitoring and control management system for smart home equipment based on wireless multihop sensor network. J Sens. 2022;2022:1–10.

23. El Matbouly H, Zannas K, Duroc Y, Tedjini S. Analysis and assessments of time delay constraints for passive RFID tag-sensor communication link: application for rotation speed sensing. IEEE Sens J. 2017;17(7):2174–81.

Additional Information

How to Cite

Yurimasanti Rachman, Deden Ardiansyah. Design and Implementation of an IoT-Based Automated Gate Control System Using RFID and Web Interface. *Digital System and Computing*. 2025;1(1):19-24

Publisher's Note

made by its manufacturer, is not guaranteed or endorsed by the publisher. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access