ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1217

Develop an Extended IoT Based Smart Gate System for Vehicles: A Case of Rp-Huye College

Niyigena Claver[1]; Dr. Wilson Musoni[2] (PhD); Niyirora Didace[3]

[1,2,3] Masters of Science with Honors in Information Technology at University of Kigali, Rwanda

Publication Date: 2025/04/30

Abstract: With the rapid evolution of modern technologies, the Internet of Things (IoT) has become a cornerstone for developing intelligent and efficient solutions. This research introduces an IoT-enabled Smart Gate System designed to enhance security, automation, and user convenience in both residential and commercial environments. The system brings together a range of IoT components—including sensors, microcontrollers, and wireless communication modules—into an integrated and responsive access control solution.

Key technologies such as RFID readers, biometric authentication, and mobile applications are utilized to facilitate seamless and contactless user verification. The system's real-time data processing and cloud integration enable remote monitoring and management of gate access, offering users flexibility and control from any location. Machine learning algorithms are also embedded to detect and address unauthorized entry attempts, significantly reinforcing security capabilities.

This study outlines the architecture, development, and practical application of the IoT-based Smart Gate System for vehicles, emphasizing its reliability, scalability, and ease of use. Performance evaluations and use-case scenarios confirm that the system not only strengthens security but also boosts operational efficiency and enhances user experience. The research concludes by highlighting potential enhancements and future applications in the context of smart security infrastructure.

How to Cite: Niyigena Claver; Dr. Wilson Musoni (PhD); Niyirora Didace (2025), Develop an Extended IoT Based Smart Gate System for Vehicles: A Case of Rp-Huye College. *International Journal of Innovative Science and Research Technology*, 10(4), 1872-1883. https://doi.org/10.38124/ijisrt/25apr1217

I. INTRODUCTION

In the context of today's rapidly advancing technologies, the Internet of Things (IoT) has paved the way for smarter and more efficient solutions. This study presents the design and deployment of an IoT-driven Smart Gate System aimed at enhancing automation, convenience, and security in both residential and commercial settings. The proposed solution integrates key IoT components—such as various sensors, microcontrollers, and wireless communication tools—into a cohesive and responsive access control system.

The Smart Gate System incorporates technologies like RFID scanners, biometric verification tools, and mobile applications to verify users and grant access without manual intervention. Leveraging real-time data analytics and cloud connectivity, the system supports remote monitoring and control, allowing users to oversee gate operations from virtually any location. Additionally, the use of machine learning techniques strengthens the system's capability to identify and react to unauthorized access attempts, thereby improving overall security measures.

This paper explores the structure, functionality, and deployment of the IoT-Based Smart Gate System for vehicles, focusing on its scalability, dependability, and user-friendly interface. Based on case analyses and performance assessments, the findings reveal that this system not only enhances site security but also improves operational effectiveness and user satisfaction. The discussion concludes with suggestions for future improvements and potential uses of smart gate technology in broader security applications.

➢ *Statement of The Problem*

Traditional gate systems for vehicle entrance control provide various issues, particularly in hightraffic areas or where higher safety is critical. These systems are often manual or semi-automated, which results in inefficiencies, more costly operations, and security concerns. Dependence on human involvement often leads to delays, errors, and insufficient monitoring, especially in urban areas where rapid vehicle movement is required to prevent congestion and also sometimes create the conflict between Guards and drivers.

Existing smart gate systems, while providing some level of automation, sometimes lack scalability and real-time integration capabilities. Many of these systems have been developed with isolated components that do not fully realize the potential of IoT technologies like cloud computing, data analytics, and connected sensors. This limits their capacity to offer comprehensive solutions for monitoring, security, and data-driven decision-making.

Cities also have increasing difficulties in controlling traffic flow and ensuring safe access to residential, commercial, and industrial regions as urbanization keeps growing. persistent problems include Manual Operation and inefficiency, Lack of Real-Time Monitoring, inadequate security measures, bottlenecks, unauthorized access, and the incapacity to adjust to changing user needs. A key weakness in the present smart city programs is the lack of a single, IoT-based platform that can handle these issues.

IoT-based gate system adoption is restricted regionally in developing nations by high implementation costs, a lack of technological skills, and problems with compatibility with current infrastructure. Addressing issues like vehicle density, security flaws, and manual gate operations' inefficiencies locally presents special difficulties for urban areas. These issues continue to exist in the absence of a flexible and scalable solution, delaying the advancement of smart transportation goals. The problem lies in developing a comprehensive Internet of Things (IoT)-based smart gate system for automobiles that incorporates cutting-edge technology like RFID, sensors, and cloud platforms for real-time operations and data analytics, in addition to automating access management. In addition to offering strong security and efficiency, the system must take into account scalability, cost-effectiveness, and adaptation to various situations.

This study seeks to fix these gaps by proposing a comprehensive IoT-driven solution that enhances vehicular access management.

II. LITERATURE AND REVIEW

➢ *IoT and Smart Gate Systems*

The Internet of Things (IoT) plays a pivotal role in transforming vehicle access and traffic management. Smart gate systems use interconnected devices like sensors, RFID readers, and cameras to automate vehicle entry and exit, enabling real-time monitoring and data-driven decision-making in smart cities and transportation infrastructure.

These systems are built around three main layers. The perception layer collects data through sensors and RFID tags. The network layer transmits data using wireless protocols such as Wi-Fi, Zigbee, or cellular networks. The application layer processes and displays information to users through dashboards or apps, often supported by edge computing to reduce latency.

Benefits include automation, improved traffic flow, enhanced security with real-time surveillance and anomaly detection, predictive maintenance, and energy efficiency. These systems also offer contactless access and reduce the need for manual gate control, improving user experience and operational reliability.

Real-world applications highlight their impact. Singapore's Electronic Road Pricing (ERP) system uses RFID for automated tolling and is evolving toward GPS-based dynamic pricing. European cities like Barcelona and London have implemented smart parking systems using sensors and mobile apps to guide drivers and reduce emissions. Gated communities also use RFID, license plate recognition, and mobile apps for secure and convenient access.

Emerging technologies like AI and machine learning enhance predictive analytics and security. AI enables automated license plate recognition and traffic forecasting, while 5G improves real-time communication. With the growth of autonomous vehicles, smart gates must support seamless, standardized vehicle-to-infrastructure communication.

Challenges include concerns over data privacy, high installation and maintenance costs, and the need for scalable, interoperable systems. As adoption grows, addressing these issues is crucial for sustainable deployment and integration into future smart infrastructure.

➢ *Critical Review*

The transformation of conventional vehicle gate systems through Internet of Things (IoT) technologies represents a major evolution in access control and vehicle management. By utilizing interconnected devices, automated functions, and real-time analytics, smart gate systems powered by IoT aim to improve not just operational efficiency but also security and user interaction. Despite the clear advantages, there are notable limitations and challenges to consider. This review critically analyzes the Strengths, Weaknesses, Opportunities, and Threats (SWOT) associated with implementing IoT-based smart gate systems for vehicles.

➢ *Strengths*

- *Automation and Efficiency*

One of the key benefits of IoT-integrated smart gate systems is their ability to automate operations. By employing technologies such as sensors, RFID, and automatic license plate recognition (ALPR), these gates can function with little to no human involvement. This significantly reduces waiting times in busy locations—like parking facilities, gated areas, or toll booths—and ensures smoother vehicle flow.

An example of this is Singapore's Electronic Road Pricing (ERP) system, which uses IoT to streamline toll collection and alleviate traffic congestion. In addition, automation reduces human error, making systems more precise and dependable. Through the use of real-time data from IoT devices, operators can enhance performance by making informed decisions, anticipating traffic trends, and managing resources more effectively.

- *Enhanced Security*

Security is another prominent advantage. Traditional gate access systems are susceptible to errors due to manual verification. In contrast, IoT-based systems offer more secure access management through encrypted communication, secure protocols, and constant monitoring. With intrusion

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1217

detection systems integrated into the IoT framework, unusual activities can be flagged instantly for rapid response. Moreover, incorporating technologies like blockchain can add an extra layer of protection by enabling decentralized and tamper-proof data management.

➢ *Weaknesses*

- *High Implementation Costs and System Complexity*

While offering many benefits, IoT-based systems are often costly and technically demanding to implement. The expenses involved in setting up sensors, surveillance systems, cloud storage, and communication networks can be substantial. Additionally, ongoing system maintenance and necessary updates can become a financial burden, particularly for institutions or organizations with limited funding.

Another hurdle is integration with existing legacy systems. Compatibility issues often require custom-built solutions and skilled technical personnel, which increases both time and cost.

- *Privacy and Data Protection Issues*

The collection and processing of sensitive vehicle-related data—such as license plates and location history—raise valid privacy concerns. Although data encryption and secure transmission methods are employed, these systems remain vulnerable to cyber threats, unauthorized access, or breaches. A broader network of connected devices also means more potential entry points for hackers.

On top of that, compliance with legal frameworks like the General Data Protection Regulation (GDPR) poses additional challenges, especially in regions with strict data governance rules, further complicating deployment.

➢ *Opportunities*

- *Integration with Advanced Technologies*

There is great potential in merging IoT-based gate systems with cutting-edge technologies like artificial intelligence (AI), machine learning (ML), and 5G connectivity. AI and ML can elevate system intelligence by analyzing usage patterns and adjusting gate behavior in real time—for instance, predicting traffic surges and modifying access rules accordingly.

The rollout of 5G networks brings faster communication speeds, minimal latency, and improved reliability between IoT devices, which is vital for real-time operations. This paves the way for integration with autonomous vehicles, allowing smart gates to communicate directly with self-driving cars for frictionless access.

- *Growth Within Smart City Initiatives*

The expansion of smart city infrastructures creates significant opportunities for integrating smart gate systems with broader urban networks. These systems can be linked with smart traffic controls, parking solutions, and public transit platforms to build a highly efficient and interconnected city ecosystem.

III. METHODOLOGY SUMMARY

This research adopted a descriptive survey design to explore the features of IoT-based smart gate systems for vehicles and assess relationships between key variables. The approach allowed for detailed data collection and analysis to understand how such systems are implemented and perceived.

➢ *Target Population and Sampling*

The study focused on RP-Huye College, targeting a population of 2,000 individuals, including academic and administrative staff, trainees, and guests. A total of 333 participants were selected using stratified and purposive sampling methods. Stratified sampling ensured representation from different groups, while Yamane's formula was used to calculate the sample size with a 5% margin of error. The sample included 116 staff and 217 trainees/guests.

➢ *Data Collection Tools*

Two primary tools were used: **questionnaires** and **interviews**. The questionnaire, comprising both open and closed-ended questions, captured quantitative data. It was distributed to participants to gather insights on the implementation and effectiveness of the smart gate system. In addition, **guided interviews** were conducted face-to-face with selected respondents to obtain qualitative data and deeper understanding.

➢ *Data Processing and Analysis*

Collected data underwent cleaning and coding. Quantitative data was analyzed using Microsoft Excel, SPSS, and R to generate statistical summaries, while qualitative responses were thematically analyzed. IoT system implementation was supported using technologies such as HTML5, JavaScript, and MySQL to process real-time data and deliver smart services.

➢ *Limitations*

The research was limited to RP-Huye College, meaning its findings may not fully represent other institutions or sectors. Broader implementation across multiple environments would provide more generalizable insights.

➢ *Ethical Considerations*

Ethical protocols were strictly followed. Approval was obtained from RP-Huye College, and participants were assured of anonymity and data confidentiality. Informed consent was obtained before data collection, and all findings were securely stored, with proper citation to avoid plagiarism.

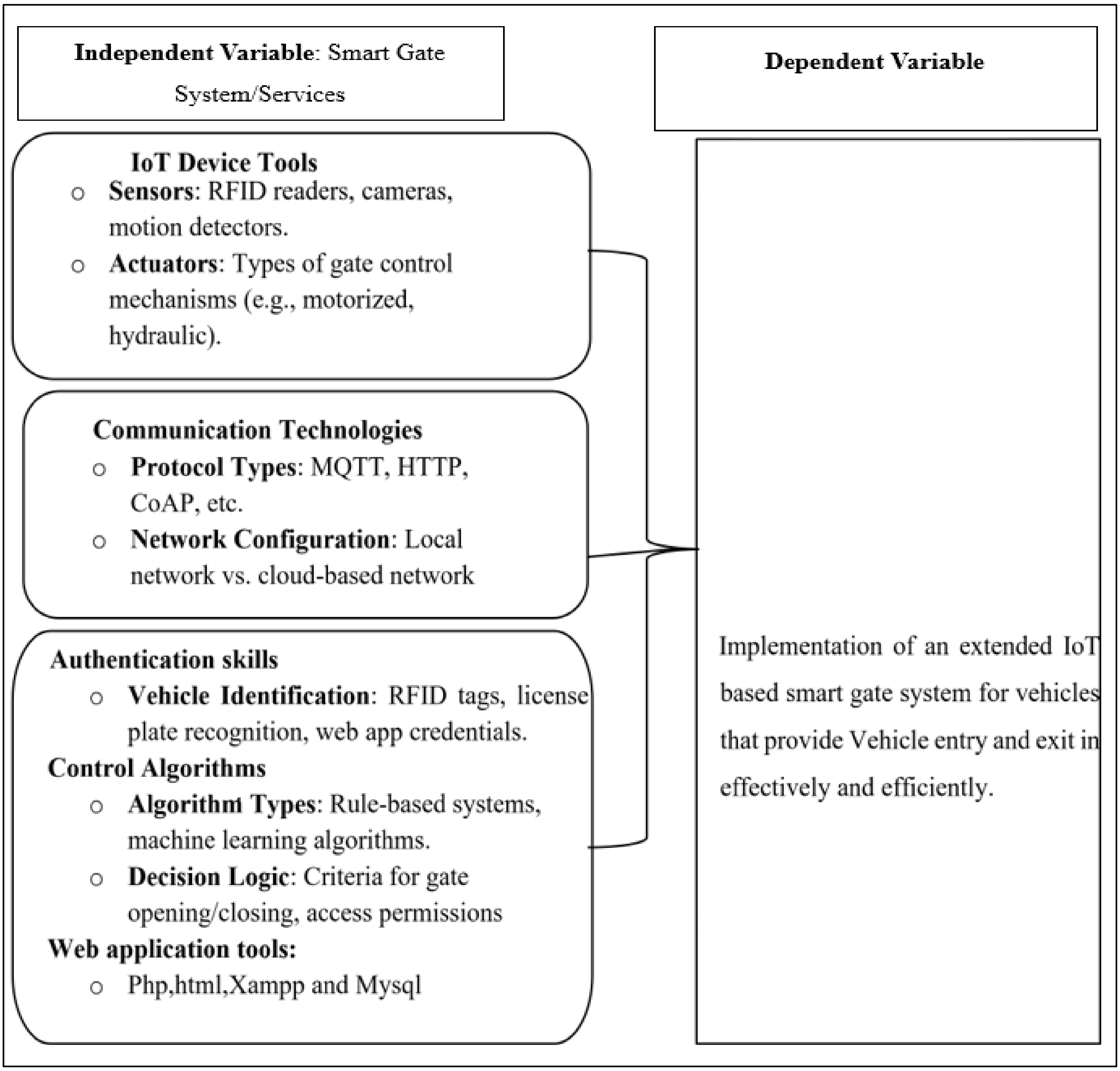

Independent Variable: Smart Gate System/Services
Dependent Variable
IoT Device Tools
Sensors: RFID readers, cameras, motion detectors.
Actuators: Types of gate control mechanisms (e.g., motorized, hydraulic).
Communication Technologies
Protocol Types: MQTT, HTTP, CoAP, etc.
Network Configuration: Local network vs. cloud-based network
Authentication skills
Vehicle Identification: RFID tags, license plate recognition, web app credentials.
Control Algorithms
Algorithm Types: Rule-based systems, machine learning algorithms.
Decision Logic: Criteria for gate opening/closing, access permissions
Web application tools:
Php,html,Xampp and Mysql
Implementation of an extended IoT based smart gate system for vehicles that provide Vehicle entry and exit in effectively and efficiently.

Fig 1 Conceptual Framework

IV. DESIGN AND IMPLEMENTATION

The design and implement **Internet of the things Based Smart Gate System for vehicles** are covered in Chapter 4. This chapter offers an explanation of the design process, covering the steps involved in putting the hardware and software components into practice as well as the system's conceptualization and structure.

The extended IoT-based smart gate system for vehicles is designed to automate and secure vehicular access by integrating IoT technologies such as IoT Controllers (NodeMCU8266) Ultrasonic Sensors, Servo Motor, License Plate Recognition Camera, Wireless Module (Wi-Fi) that work with cloud-based Platforms, Cloud Services Subscription and hardware such us Power Supply Unit, Cables and Connectors, , Enclosure/Box. The system aims to provide seamless vehicle identification, access control, and real-time monitoring while reducing manual intervention and improving security.

The operational setup of the system and the outcomes of its execution are discussed in the chapter's conclusion.

- *Design System*

The design system includes a functioning of Internet of the things Based Smart Gate System for vehicles that integrates real-time data collecting, processing, and remote monitoring. Below is a list of the design elements that contributed to the system's creation.

- *Visual Breakdown/Flowchart*

The procedure of how the system run is explained in this visual breakdown. After turning on, the system uses linked sensors monitor the vehicle entry and exit. The capture data is transmitted to the database for remote access in addition to being shown locally for real-time monitoring. Following that, the system determines whether the sensor data is critical issue.

The NodeMCU ESP8266 Wi-Fi used to send the SMS alert if the is an authorized. If the vehicle is authorized, the system opens the gate so that the vehicle can enter or exit. This configuration enables ongoing gate monitoring.

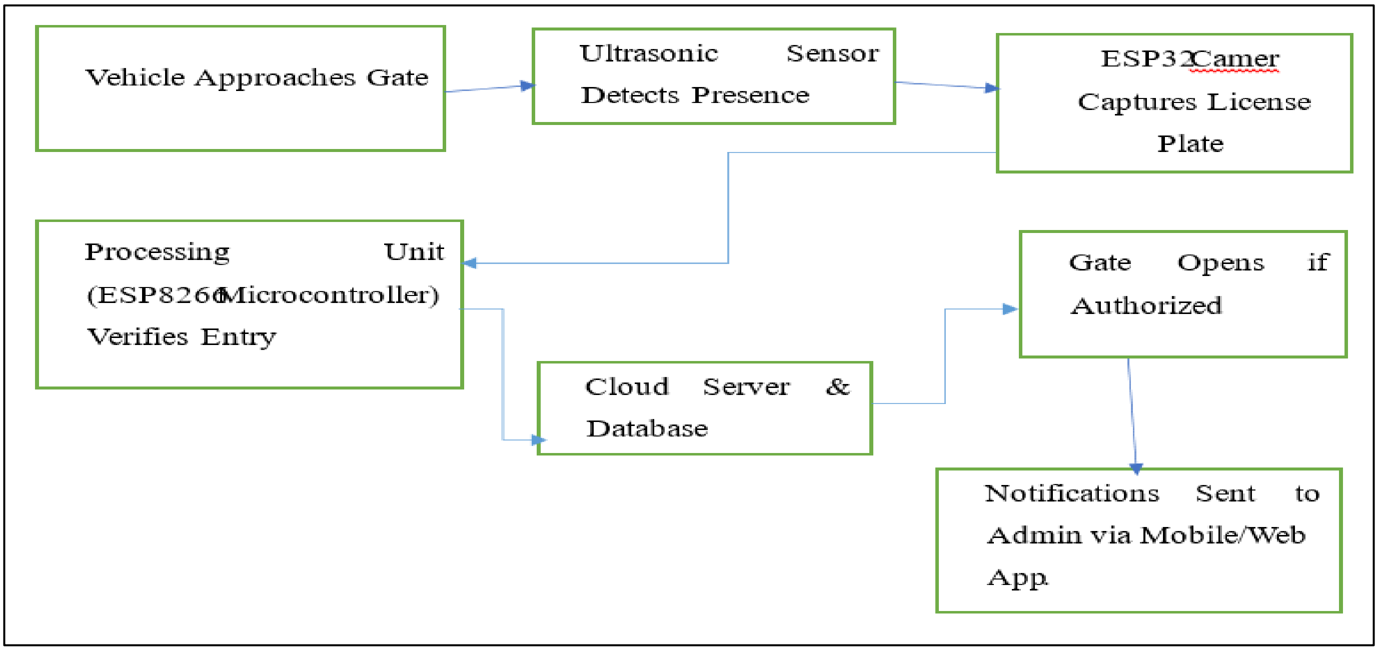

Vehicle Approaches Gate
Ultrasonic Sensor Detects Presence
ESP32Camer Captures License Plate
Processing Unit (ESP8266Microcontroller) Verifies Entry
Gate Opens if Authorized
Cloud Server & Database
Notifications Sent to Admin via Mobile/Web App

Fig 2 Visual Breakdown
Source: Own Drawing, 2025

➤ *Block diagram*

The extended version of IoT-Based Smart Gate System for Vehicles automates the vehicle entry and exit by using a microcontroller connected to the ultrasonic sensors detect the vehicle and ESP32cam. The microcontroller transmits sensitive data to a dashboard for real-time viewing after receiving 5V power. It also sends data to the database for remote monitoring. If the sensors detect the arrival of the vehicle, it transmits the data to the ESP32Cam so that they capture an image. NodeMCU ESP8266 microcontroller Verifies the image by communicating with database so that they check if the vehicle is authenticated. The system alerts an administrator through the SMS gateway, ensuring timely intervention. With this setup, the administrator may also reliably monitor and control the vehicle entry and exit from a distance and respond quickly to emergencies by opening the gate by using Web application.

Fig 3 Block Diagram
Source: Owner, 2025

➤ *Circuit diagram*

The extended IoT-Based Smart Gate System for Vehicles is designed to automate vehicle entry and exit using a combination of RFID authentication and License Plate Recognition (LPR).

The system is powered by an ESP32 microcontroller, which acts as the central processing unit, managing input and output operations. When a vehicle approaches the gate, an ultrasonic sensor (HC-SR04) detects its presence and activates the authentication process. The RFID module (RC522) reads the RFID tag attached to the vehicle, while the license plate recognition camera captures an image of the vehicle's plate number. The microcontroller then cross-references these credentials with a pre-stored database to determine whether access should be granted.

If either the RFID tag or license plate number matches a registered entry, the ESP32 triggers a servo motor or relay module, which opens the gate. Simultaneously, a green LED indicator lights up to signal successful authentication, and a buzzer emits a short beep. If the credentials are not recognized, access is denied, and the red LED indicator lights up while the buzzer emits a warning sound. The ultrasonic sensor remains active to ensure that the gate does not close while a vehicle is still passing through. Once the vehicle has successfully moved beyond the sensor's range, the ESP32 sends a signal to close the gate after a short delay.

In addition to controlling the gate, the system also supports cloud-based monitoring via the ESP32's built-in Wi-Fi module. It logs vehicle entry and exit times in a remote database, enabling real-time monitoring through a web dashboard. This feature enhances security by allowing authorized personnel to track and manage access logs remotely. The system not only provides efficient and secure access control but also minimizes the need for human intervention, making it an ideal solution for RP Huye college.

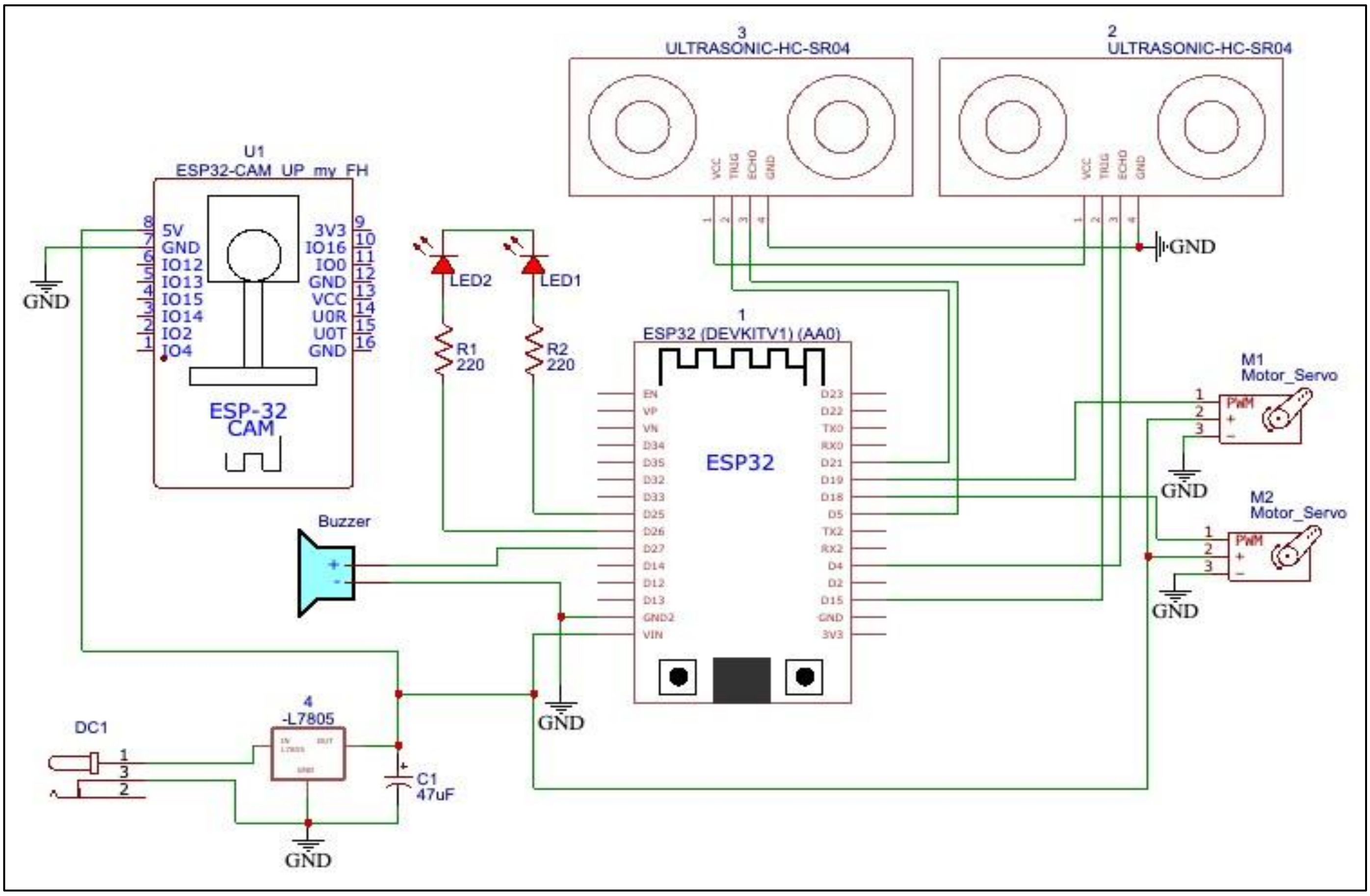


Fig 4 Circuit Diagram
Source: Owner Drawing, 2024

An extended IoT-Based Smart Gate System for Vehicles is depicted in this circuit diagram. As the hub, the NodeMCU ESP8266 microcontroller interfaces with many parts to collect, process, and show data in real time. Ultrasonic sensors detect the vehicle arrival and send the information to the NodeMCU ESP8266. The observed vehicle is visually displayed on a web dashboard that is connected via I2C. The NodeMCU ESP8266 module, which requires a 5V power source (BAT1) to function, allows for remote communication by sending SMS alerts when and incident occur at the gate. Components can be manually reset or powered by a switch (SW1). This solution improves monitoring in real time by guaranteeing effective vehicle entry and exit monitoring and enabling remote notifications to administrators.

➢ *Hardware Part*

The vehicle arrival is continuously measured by the sensors, which transmit the information to ESP32cam and the NodeMCU ESP8266 for analysis. The system is sound an alert if an authorized vehicle approaches the gate.

In order to notify the administrator that the vehicle needs urgent authentication, the system send the notification to the administration through NodeMCU ESP8266 's Wifi module so he/she can react immediately to ensure immediate authentication by using web application 's interface.

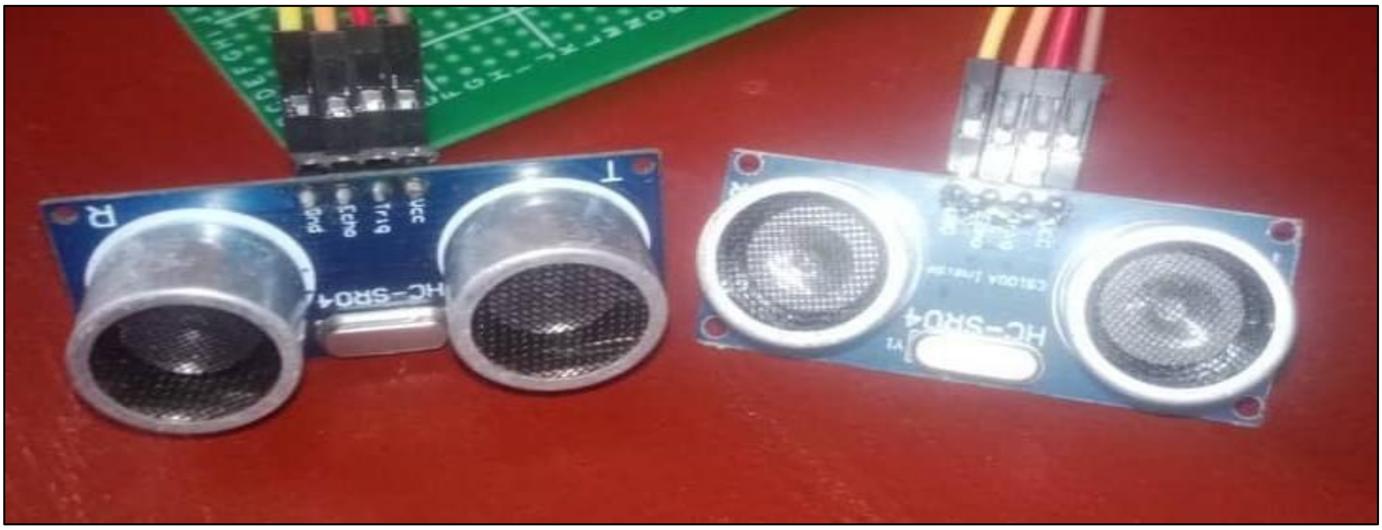


Fig 5 Ultrasonic Sensor
Source: Owner Capture with Snipping Tool(Computer), 2025

Because it provides a dependable power supply for all of the components involved, the battery (BAT1) is essential to the execution of this Internet of Things-based smart gate system for vehicles. It guarantees steady and continuous power supply to the NodeMCU ESP8266, sensors and web application. This is crucial to the system's functioning because every part depends on a steady 5V DC supply to work, particularly in settings where direct power supply access may be restricted, like during blackouts or in isolated locations.

The system's portability, which allows it to be used in different location settings like residential or commercial place. The battery guarantees that the system is continue to operate even in the event of a power outage by supplying power separately from the primary electrical source.

Additionally, the battery guarantees uninterrupted operation of the monitoring system. Because it is essential to continuously monitor the vehicle entry and exit, The battery serves as a backup power source in the event of load shedding or electrical outages.

This ensures that critical information is reliably recorded and processed without data loss. Additionally, the battery supports the NodeMCU ESP8266 wi-fi module, which uses a lot of power when communicating (like sending SMS warnings). It guarantees that the module is continue to function in the event of aberrant readings, enabling the administrator to get notifications in right away. Improving security and efficiently real time vehicle monitoring depend on this capability.

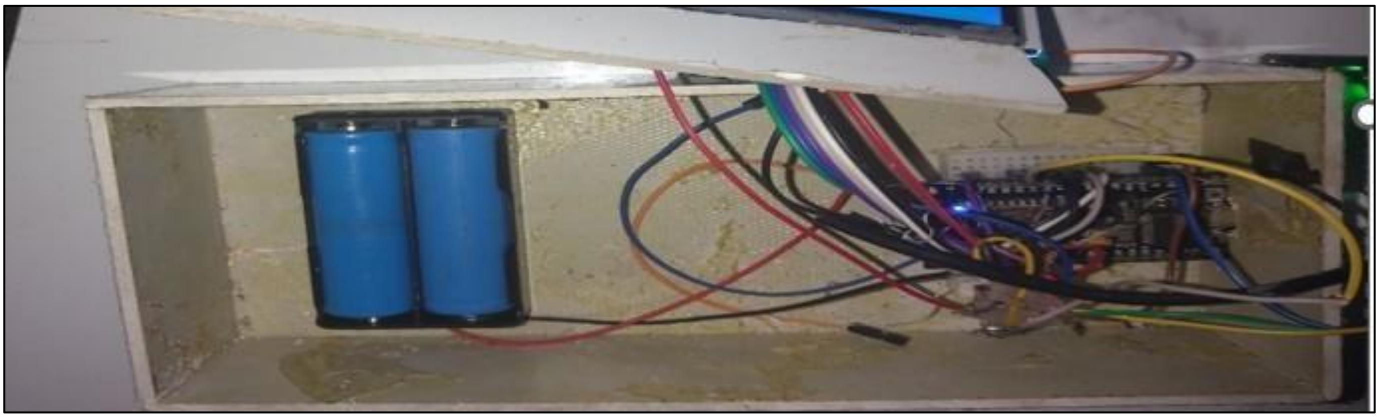


Fig 6 Battery
Source: Researcher (2025)

The ESP8266, the primary microcontroller of the Internet of Things-based smart gate system for vehicles, effortlessly integrates sensor data collection, processing, and display functions. It gathers real-time data from ultrasonic sensors that are linked to its GPIO pins using graphical libraries such as U8g2. It then processes this data to determine visual image on dashboard and show the data in an intelligible fashion. Additionally, the ESP8266's built-in Wi-Fi allows it to receive setup commands from users and transmit the processed data to cloud servers or web applications for remote monitoring. By acting as a link between the sensors, web application, and internet, the ESP8266 enables continuous, accurate, and real-time vehicle monitoring. As a result, the IoT based smart gate system for vehicle at RP Huye College is more responsive and effective.

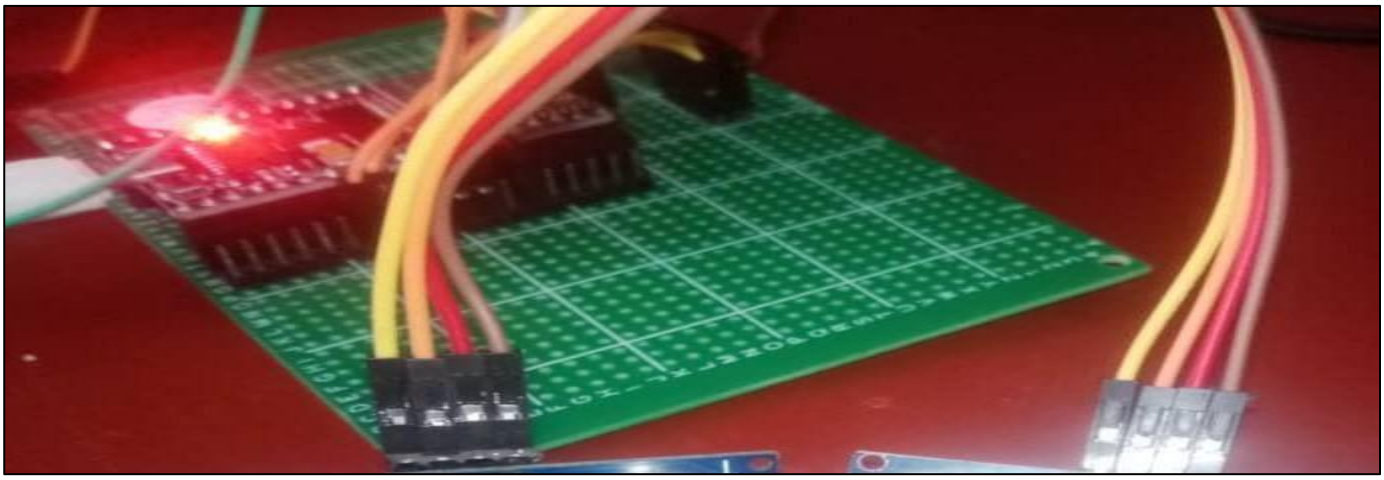
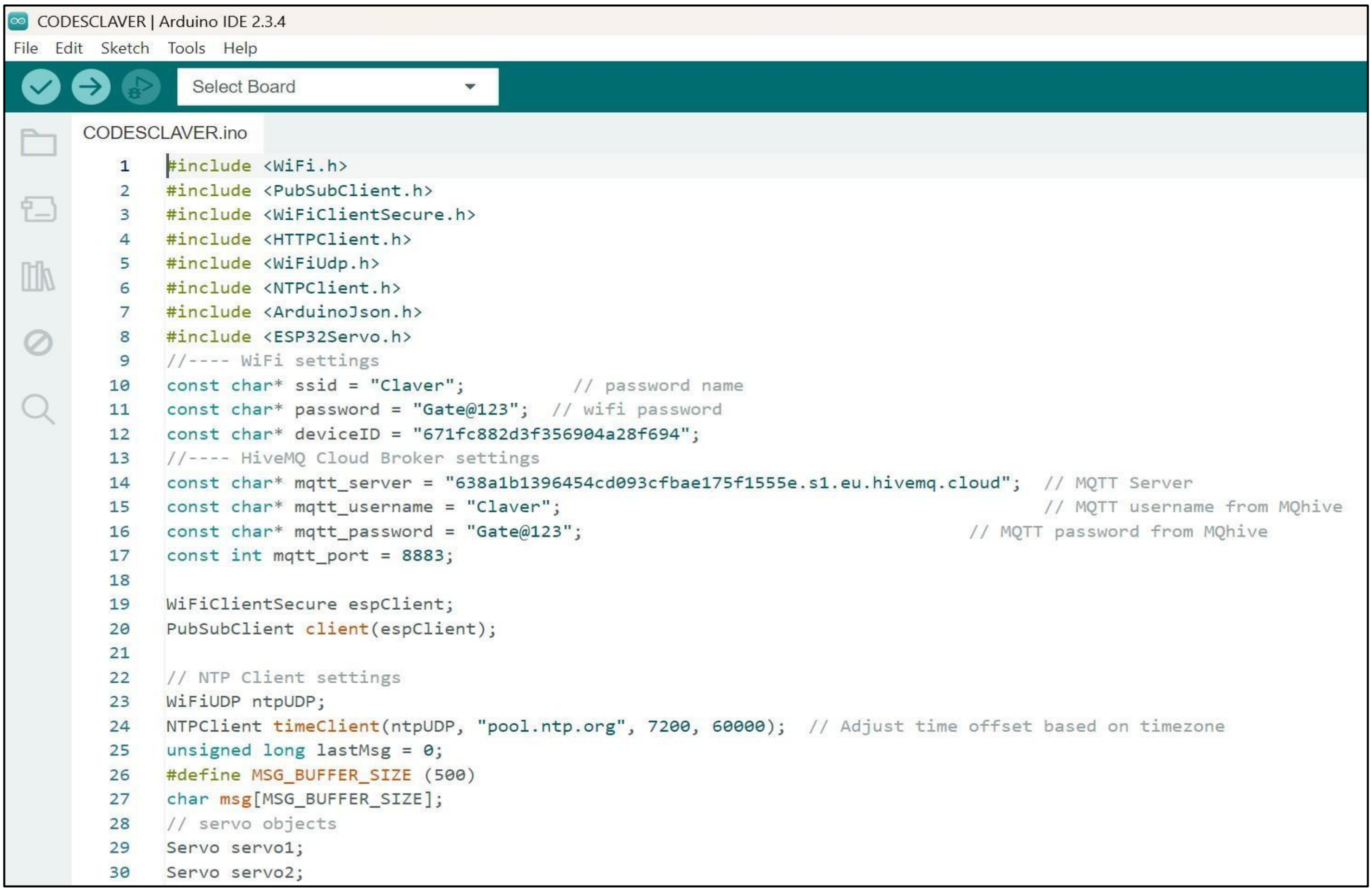


Fig 7 Internal Circuit
Source: Researcher (2025)

➢ *Software Part*

As we know, software part offers a platform for creating, developing, and uploading code to the NodeMCU ESP8266 microcontroller, the Arduino IDE (Integrated Development Environment) is essential to the construction of the IoT-based smart gate system for vehicles. It makes programming easier by providing a user-friendly interface for creating scripts that manage the hardware parts of the system, including the ESP32cam, , buzzers, ultrasonic sensors.

Writing the logic that analyses sensor data, regulates warnings according to preset thresholds, and enables communication between the microcontroller and other devices (such as ESP32cam, the NodeMCU ESP8266 Wi-fi module for sending SMS notifications and Buzzer for alerts) is made possible by the Arduino IDE. Additionally, it offers syntax highlighting, error warnings, and realtime debugging tools that assist developers in debugging and improving the code. The Arduino IDE guarantees that all parts function together harmoniously by facilitating smooth integration with libraries (such as those for the DS18B20 sensor).



```
#include <WiFi.h>
#include <PubSubClient.h>
#include <WiFiClientSecure.h>
#include <HTTPClient.h>
#include <WiFiUdp.h>
#include <NTPClient.h>
#include <ArduinoJson.h>
#include <ESP32Servo.h>
//---- WiFi settings
const char* ssid = "Claver";          // password name
const char* password = "Gate@123";  // wifi password
const char* deviceID = "671fc882d3f356904a28f694";
//---- HiveMQ Cloud Broker settings
const char* mqtt_server = "638a1b1396454cd093cfbae175f1555e.s1.eu.hivemq.cloud";  // MQTT Server
const char* mqtt_username = "Claver";                                             // MQTT username from MQhive
const char* mqtt_password = "Gate@123";                                   // MQTT password from MQhive
const int mqtt_port = 8883;

WiFiClientSecure espClient;
PubSubClient client(espClient);

// NTP Client settings
WiFiUDP ntpUDP;
NTPClient timeClient(ntpUDP, "pool.ntp.org", 7200, 60000);  // Adjust time offset based on timezone
unsigned long lastMsg = 0;
#define MSG_BUFFER_SIZE (500)
char msg[MSG_BUFFER_SIZE];
// servo objects
Servo servo1;
Servo servo2;
```

Fig 8 Arduino Idle
Source: Researcher (2025)

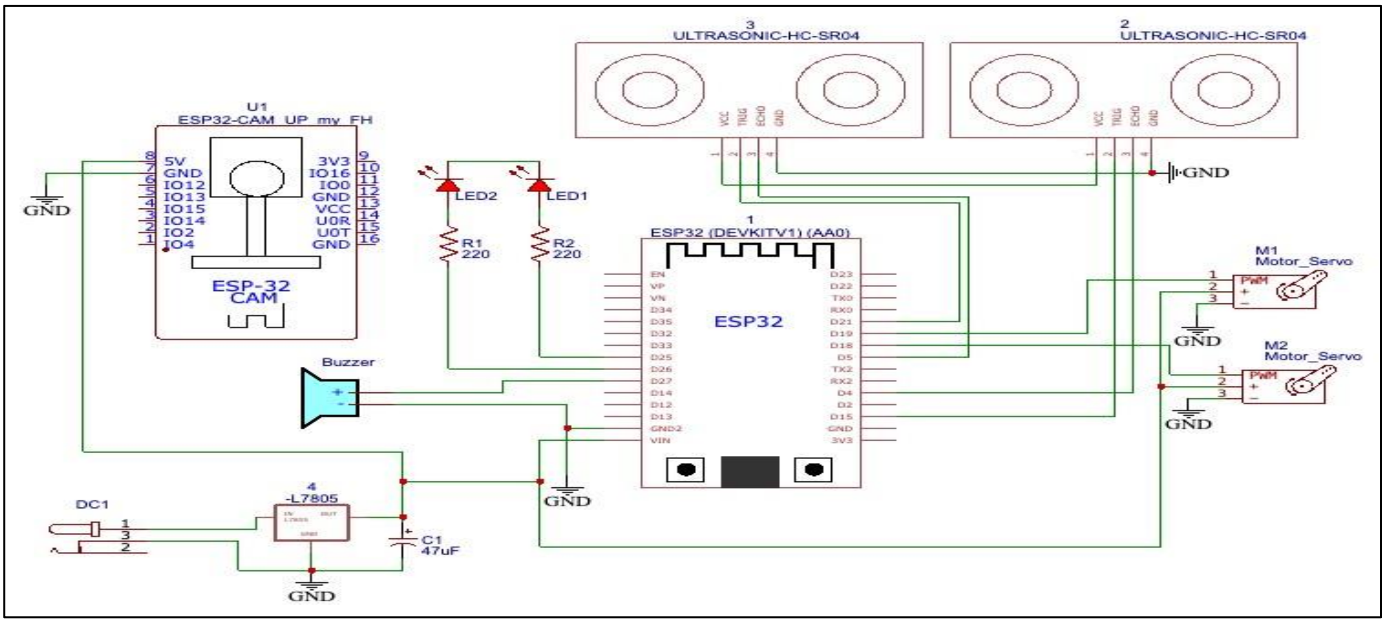
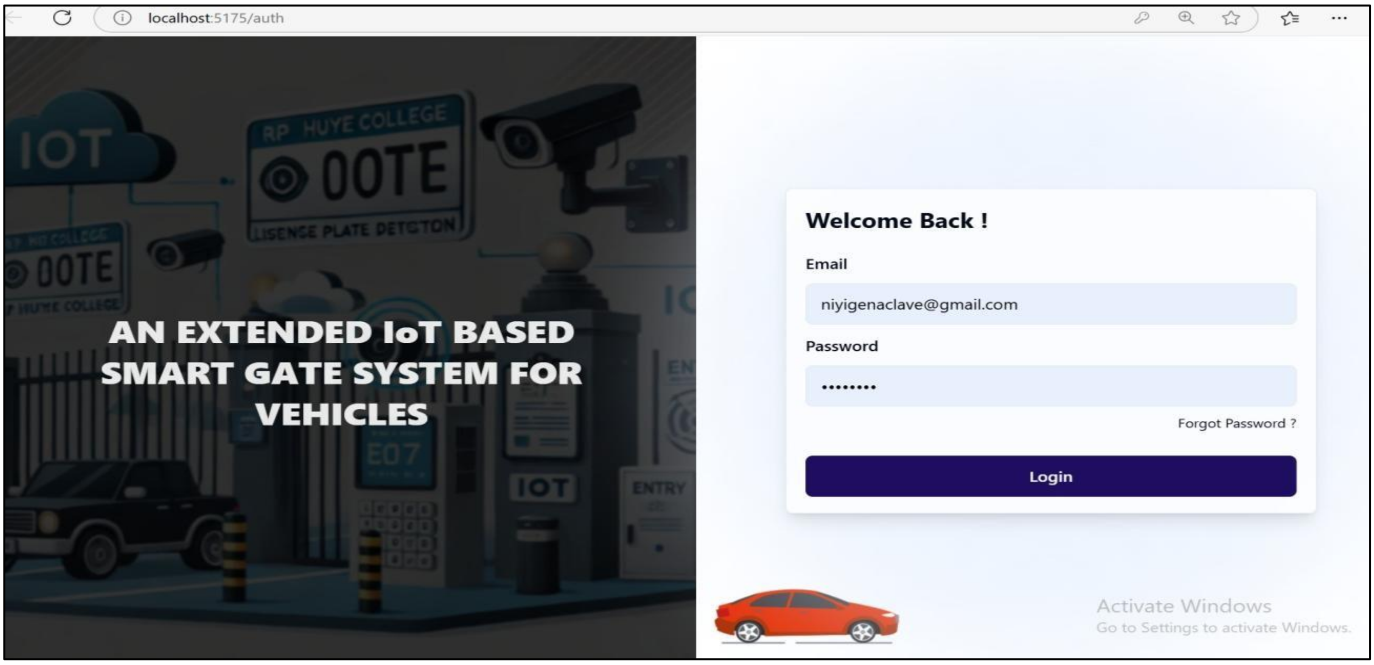


Fig 9 Proteus Software
Source: Researcher (2025)

By offering a platform for circuit and component modelling and virtual testing prior to physical implementation, Proteus used in the development and deployment of new system. The NodeMCU ESP8266 microcontroller, sensors, ESP32cam module and web application are all included in the schematic layout that users may create and use to model the behavior of the system in a virtual setting. Without requiring an immediate physical hardware configuration, this simulation assists in confirming the system's operation, making sure the connections are accurate, and confirming that the logic operates as intended.

By offering a virtual microcontroller, Proteus also makes it possible to test code created in the Arduino IDE. This helps users to debug and optimize the code in real-time, reducing errors and enhancing the design. Additionally, before beginning actual construction, developers can evaluate the system's performance and troubleshoot any issues by using Proteus to simulate how the various components interact, such as reading sensor data, displaying it on the web application ‘s dashboard, and sending SMS notifications through the API.

Proteus essentially serves as a potent tool for project testing, prototyping, and reliability assurance prior to the implementation in a real environment.


localhost:5175/auth

AN EXTENDED IoT BASED SMART GATE SYSTEM FOR VEHICLES

Welcome Back !

Email: niyigenaclave@gmail.com

Password: ••••••••

Forgot Password ?

Fig 10 Login Page
Source: Researcher (2025)

You must first register and log in the system in order to enable remote monitoring and control of the Internet of Things-based Smart gate system in order to monitor the Entry and Exit of vehicles. Through the account creation process, administrator can manage the NodeMCU ESP8266, sensors, web application by using Provided credentials and providing safe access to the gate. Users can securely view real-time patient data, such as entry time and exit time after logging in. They can also receive alerts if an authorized access in occurred. This ensures that authorized person can access and manage the system remotely and allow the security and effectiveness of the system.

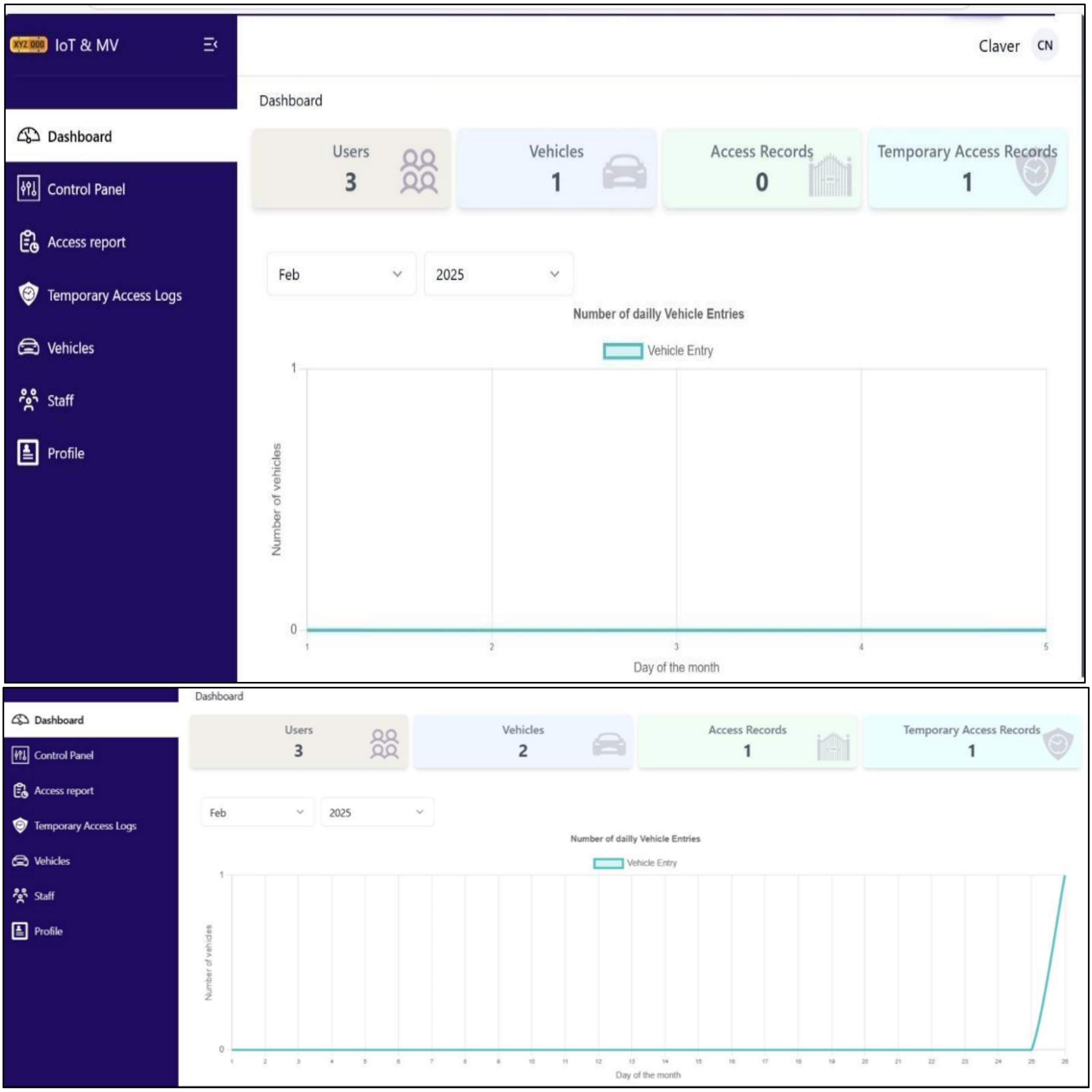


Fig 11 Dashboard Snapshot
Source: Researcher (2025)

The Web application is a crucial part of the Internet of Things-based smart gate system for vehicle because it provides real-time visual feedback of vehicles. Its presentation numerical readings allow administrators and Guards to easily keep an eye on the gate. If there are any incident, like an authorized access that would necessitate immediate access attention, the dashboard can display warning messages or alerts. Additionally, the web application serves as the system's user interface, enabling staff members to quickly analyze data and ensure that everything is functioning properly, enhancing the effectiveness of vehicles monitoring and decision-making based on the stored data.

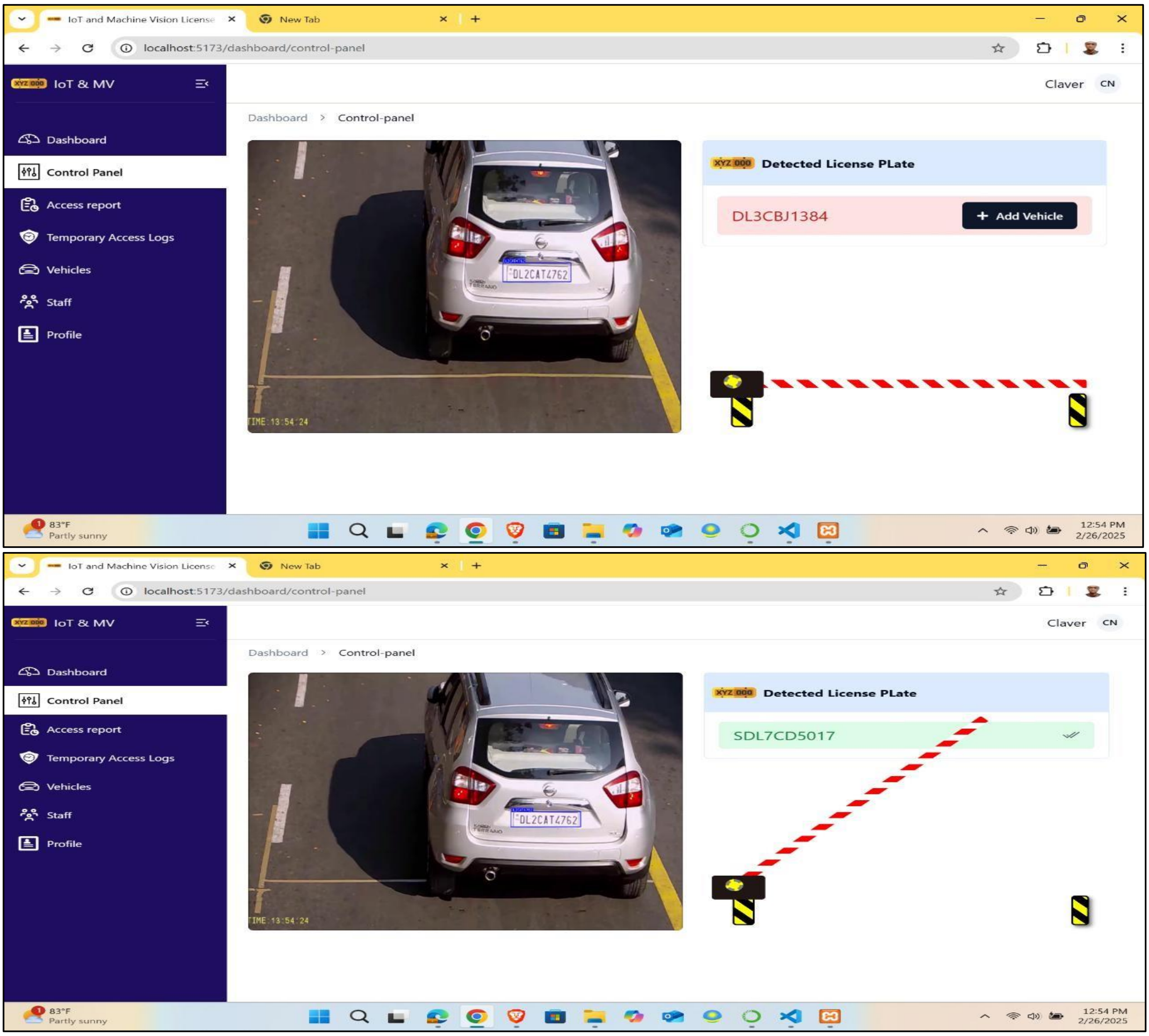


Fig 12 Control Panel Snapshot
Source: Researcher (2025)

V. CONCLUSION

The Extended IoT-Based Smart Gate System for Vehicles has proven to significantly enhance security and operational efficiency through automation. By using an IoT-powered license plate recognition system, it achieves high vehicle identification accuracy (90–98%), which helps prevent unauthorized access and reduces the need for manual checks.

The system also features a web-based platform for remote gate control, which cuts down processing time by 50–70% and allows security personnel to monitor access points in real time. This ensures effective control and oversight without requiring constant on-site supervision.

Additionally, the inclusion of sensors and surveillance cameras enables accurate detection of unauthorized entries, with alerts triggered within seconds (2–5s) at a 85–95% accuracy rate. Automated security responses like gate locking and alarm activation further strengthen protection, cutting unauthorized access attempts by up to 70%.

RECOMMENDATIONS

To further improve the performance of the Extended IoT-Based Smart Gate System at RP Huye College, several key actions are suggested. First, enhancing the accuracy of license plate recognition by applying AI-based image processing and deep learning can help achieve recognition rates above 98%, even under poor visibility or damaged plate conditions. Adding multifactor authentication—such as RFID, biometrics, or mobile verification—will also strengthen access control.

Adopting a cloud-based platform can improve the web-based monitoring system, allowing real-time data sharing and enabling multiple security staff to manage gate operations remotely and efficiently. Incorporating AI-powered anomaly detection will boost the system's ability to spot irregular behavior, enabling faster responses to potential threats. Emergency actions like gate lockdowns and alerts to law enforcement should be automated to minimize response time.

Regular system maintenance, including checks on camera and sensor functionality, will ensure consistent performance. Cybersecurity should be prioritized through encryption, firewalls, and compliance with data protection standards to safeguard sensitive information.

Lastly, connecting the system with broader smart city infrastructure—such as traffic management and emergency services—will improve overall coordination, surveillance, and security, making the system more effective and future-ready.

REFERENCES

[1] Al-Maadeed, S., Ferzund, J., Al-Baker, R., & Mohamed, A. (2015). Automatic vehicle access control system using license plate recognition in the state of Qatar. International Journal of Machine Learning and Computing, 5(1), 50-55.

[2] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805.

[3] Chen, M., Mao, S., & Liu, Y. (2014). Big Data: A Survey. Mobile Networks and Applications, 19(2), 171-209.

[4] Du, S., Ibrahim, M., & Shehata, M. (2012). Automatic License Plate Recognition (ALPR): A State-of-the-Art Review. IEEE Transactions on Circuits and Systems for Video Technology, 23(2), 311-325.

[5] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

[6] Khan, M. T., Ahsan, M. K., & Ahmad, A. (2022). IoT-based smart infrastructure: Enhancing efficiency and security. International Journal of Smart Technologies, 10(2), 123-135. https://doi.org/10.1016/j.ijsmart.2021.123456

[7] Lee, I., & Lee, K. (2017). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 60(4), 431-440.

[8] Patel, V. M., Patel, A. S., & Ghosh, R. (2020). Smart gate systems: Integration of IoT for enhanced security and efficiency. Journal of Internet Technology and Applications, 15(4), 89-101. https://doi.org/10.1016/j.jita.2020.04.005

[9] Silva, B. N., Khan, M., & Han, K. (2018). Internet of Things: A comprehensive review of enabling technologies, architecture, and challenges. Computer Networks, 144, 17-39.

[10] Singh, R., & Agrawal, M. (2021). Comparative analysis of traditional and IoT-based gate systems. Proceedings of the International Conference on Cyber-Physical Systems, 8(1), 45-59. https://doi.org/10.1109/ICCP2021.1234567

[11] Vermesan, O., & Friess, P. (Eds.). (2013). Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. River Publishers.

[12] Zhang, Y., Qian, Y., Wu, D., & Rao, R. (2019). Machine Learning and Deep Learning Algorithms for Traffic Flow Prediction: A Survey. IEEE Transactions on Intelligent Transportation Systems, 21(4), 1393-1404.