International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

SMART GATE: IOT-ENABLED RFID-BASED VEHICLE ENTRY AND REAL-TIME COUNT MANAGEMENT SYSTEM

[1] Dr. M V Raghavendra, [2] B Ankitha, [3] Shetti Sai, [4] Shanam Bhavana, [5] K Saikumar
[1]Professor, [2345] B. Tech Students
[12345]Department of Electronics and Communication Engineering
[12345]Sree Dattha Group of Institutions, Sheriguda, Ibrahimpatnam, 501510, Telangana, India

ABSTRACT

The Smart Gate system is an advanced IoT-enabled solution designed for automated vehicle entry and real-time monitoring in residential complexes, offices, parking areas, and restricted zones. The system combines RFID technology, microcontroller intelligence, and cloud-based IoT connectivity to replace traditional manual access methods. Each vehicle is assigned a unique RFID tag that carries identification information. When a vehicle approaches the gate, the RFID reader scans the tag and sends the data to the ESP8266 or ESP32 microcontroller. The microcontroller verifies the vehicle information against a pre-stored database of authorized entries. Upon successful verification, the gate motor is activated via a relay module, allowing the vehicle to enter or exit. Simultaneously, the vehicle count and status are updated to the cloud server using MQTT or HTTP protocols, enabling real-time monitoring via a web or mobile dashboard. Unauthorized vehicles trigger an alert system to notify administrators, ensuring enhanced security. By integrating IoT, the system allows administrators to access real-time data from any location, reducing dependency on on-site security personnel and manual logbooks. The automated approach minimizes congestion, increases accuracy, and ensures fast and reliable operation even during peak hours. Multiple gates can be managed simultaneously without interference, ensuring scalability for large complexes. Historical data, such as vehicle entry and exit timestamps, is maintained in the cloud for reporting and analytics. Sensor-based triggers and scheduling rules can automate gate closing, reducing energy consumption and enhancing operational efficiency. Security mechanisms, including encrypted communication, device authentication, and secure MQTT topics, prevent unauthorized access and hacking attempts. The system's modular design allows easy expansion, maintenance, and integration with additional IoT devices. By eliminating human error, the solution ensures accuracy in vehicle management and enhances safety. Administrators can track occupancy, generate automated reports, and optimize traffic flow based on historical data analytics. The system is cost-effective, reliable, and suitable for modern smart city implementations. It leverages low-power microcontrollers, lightweight communication protocols, and cloud platforms to deliver a high-performance, efficient, and user-friendly smart gate solution. This IoT-based system provides a comprehensive vehicle management platform that enhances convenience, security, and efficiency for all stakeholders. It integrates seamlessly with existing infrastructure and supports future expansion, including integration with automated parking systems, RFID-enabled smart cards, and cloud analytics tools. Overall, the Smart Gate system represents a significant improvement over traditional methods, offering a fully automated, scalable, and secure solution for vehicle access and real-time monitoring in modern facilities.

I. INTRODUCTION

1.1. OVERVIEW

The rapid growth of urbanization, increasing vehicle ownership, and expansion of residential and commercial infrastructures have created significant challenges in vehicle access control and parking management. Traditional manual gate systems rely heavily on security personnel to verify vehicle entry and maintain physical logbooks. While such systems have been in use for decades, they are prone to inefficiencies, human errors, security lapses, and traffic congestion—especially during peak hours. With the emergence of

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

smart cities and IoT-based automation technologies, there is a strong need for intelligent, automated, and real-time vehicle management systems.

The Smart Gate: IoT-Enabled RFID-Based Vehicle Entry and Real-Time Count Management System is designed to address these challenges by integrating RFID technology, embedded microcontrollers, wireless communication, and cloud connectivity. The system automates vehicle identification, gate control, and occupancy tracking while enabling administrators to monitor activities remotely in real time.

Radio Frequency Identification (RFID) technology plays a central role in this system. RFID uses electromagnetic fields to automatically identify and track tags attached to objects—in this case, vehicles. Each vehicle is assigned a unique RFID tag containing identification data. When a vehicle approaches the gate, the RFID reader scans the tag and sends the tag information to the Arduino-based controller. The controller verifies the tag ID against a stored database of authorized vehicles. If the vehicle is authorized, the gate motor is activated through the L293D motor driver, allowing the gate to open automatically. If the tag is not recognized, the system denies access and triggers an alert via the buzzer.

The integration of a Wi-Fi module (such as ESP8266 or ESP32) enables IoT functionality. After each entry or exit event, the system updates real-time vehicle count and entry logs to a cloud server using communication protocols like MQTT or HTTP. This allows administrators to monitor vehicle movement from anywhere via a web or mobile dashboard. Real-time occupancy data improves operational efficiency and enhances security monitoring.

1.2. NEED FOR THE SYSTEM

The need for an IoT-enabled RFID-based vehicle entry system arises from several technological, operational, and security challenges in traditional access control systems.

1.2.1 Increasing Vehicle Population

Urban areas and residential complexes are witnessing rapid growth in vehicle ownership. Manual gate systems struggle to manage high traffic volumes efficiently, leading to congestion and delays.

1.2.2 Security Concerns

Traditional systems rely on visual verification by guards, which can be inconsistent and unreliable. Unauthorized vehicles may gain entry due to oversight or manipulation.

1.2.3 Human Error in Record Keeping

Manual logbooks are prone to:

- Incomplete entries
- Illegible handwriting
- Data loss
- Inaccurate counting

An automated system ensures accurate digital records.

1.2.4 Real-Time Monitoring Requirement

Administrators require instant access to vehicle data for:

- Occupancy management
- Security monitoring
- Traffic flow analysis

Manual systems cannot provide real-time data updates.

1.2.5 Reduction in Operational Costs

Automated systems reduce dependence on security personnel for routine gate operations, lowering long-term operational costs.

1.3. PROBLEM STATEMENT

Despite technological advancements, many residential complexes, offices, and parking areas still rely on manual vehicle entry systems. These systems suffer from multiple limitations:

1. **Slow Manual Verification** – Physical checks delay vehicle entry during peak hours.
2. **Security Vulnerabilities** – Human verification can be bypassed or manipulated.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

3. **Inaccurate Counting** – Manual counting leads to occupancy miscalculations.
4. **Lack of Real-Time Data** – Administrators cannot monitor vehicle movement remotely.
5. **Poor Record Maintenance** – Paper-based records are inefficient and unreliable.
6. **Limited Scalability** – Manual systems struggle to manage multiple gates.
7. **High Labor Costs** – Continuous staffing increases operational expenses.

Therefore, there is a need for an automated, IoT-enabled vehicle entry and count management system that provides secure authentication, real-time monitoring, accurate data logging, and scalable operation.

1.4. OBJECTIVES

The primary objective of this project is to design and implement an IoT-enabled RFID-based vehicle entry system using Arduino and Wi-Fi connectivity.

1.4.1 General Objectives

- To automate vehicle entry using RFID authentication.
- To implement real-time vehicle count monitoring.
- To integrate IoT connectivity for remote access.
- To enhance security and operational efficiency.

1.4.2 Specific Objectives

1. Interface RFID reader with Arduino microcontroller.
2. Store authorized vehicle IDs in memory.
3. Verify RFID tag data upon scanning.
4. Activate gate motor via L293D motor driver.
5. Update vehicle count for entry and exit.
6. Display system status on LCD.
7. Trigger buzzer alerts for unauthorized vehicles.
8. Transmit entry data to cloud via Wi-Fi module.
9. Maintain timestamped logs in cloud database.
10. Implement secure communication protocols.

1.4.3 Performance Objectives

- Fast tag detection and gate response (<2 seconds).
- Accurate vehicle counting.
- Reliable Wi-Fi connectivity.
- Minimal latency in cloud updates.
- Energy-efficient operation.

1.5. SCOPE OF THE PROJECT

1.5.1 Technical Scope

The system includes:

- Arduino microcontroller
- RFID reader and tags
- Wi-Fi module (ESP8266/ESP32)
- L293D motor driver
- DC motor for gate control
- LCD display
- Buzzer
- Regulated power supply

It supports real-time authentication, gate automation, and cloud monitoring.

1.5.2 Functional Scope

- RFID-based vehicle identification
- Automated gate opening/closing
- Vehicle count increment/decrement
- Unauthorized vehicle alert
- Cloud-based real-time updates
- Historical data storage and analytics

1.5.3 Application Scope

Applicable in:

- Residential complexes
- Office buildings
- Industrial campuses
- Parking areas
- Educational institutions
- Toll plazas (small-scale)
- Restricted government zones

1.5.4 Limitations

- Requires stable internet connection.
- RFID tags can be physically damaged.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

- Basic version limited to pre-registered vehicles.
- Security depends on encrypted communication.

II. LITERATURE SURVEY

1. IoT-Based Access Control Systems

IoT-based access control has revolutionized traditional manual methods of monitoring vehicle entry. Early systems relied on security guards and logbooks, which were prone to errors and delays. With the advent of IoT, wireless communication technologies like Wi-Fi, Zigbee, LoRa, and Bluetooth became integral to automated monitoring. Studies highlight that IoT enables centralized control and remote management of multiple access points. Cloud-based dashboards and mobile applications provide real-time visualization of vehicle entry and exit data. Administrators can manage schedules, receive alerts, and monitor occupancy from any location. IoT integration enhances operational efficiency by reducing human effort and automating repetitive tasks. IoT-based access systems support rule-based automation such as scheduling restricted access and controlling gates automatically. Energy efficiency is improved as sensors and microcontrollers operate in low-power modes when idle. Real-time data ensures immediate response to unauthorized entry attempts. Studies suggest that IoT-enabled access management is scalable and can handle multiple gates simultaneously without interference. Automated alerts help administrators respond to security breaches quickly. Research emphasizes that IoT allows easy integration of additional sensors, cameras, and security modules. Data analytics enables traffic optimization, vehicle flow prediction, and space utilization analysis. Cloud storage ensures historical data retention for audits and reporting. Secure communication protocols, encryption, and authentication protect against cyber threats. IoT-based vehicle management systems significantly reduce operational costs. Dashboards provide insights into patterns, peak hours, and occupancy trends. Studies also highlight that IoT systems improve safety and reduce congestion at entry points. IoT enables two-way communication, allowing remote control and monitoring simultaneously. Integrating IoT with RFID technology ensures accurate identification and tracking of vehicles. Research confirms that IoT access systems improve reliability, scalability, and user convenience. Administrators can generate automated reports for compliance and analytics. Mobile apps provide real-time notifications and alerts, enhancing situational awareness. IoT platforms allow remote troubleshooting, configuration, and maintenance. The literature confirms IoT access management as a transformative approach for modern parking and entry systems.

2. RFID in Vehicle Management

RFID technology is widely adopted for automated vehicle identification due to its non-contact scanning, durability, and speed. Each vehicle is assigned a unique RFID tag carrying identification data. RFID readers at entry and exit gates detect these tags and transmit the information to microcontrollers. Research shows RFID significantly reduces manual effort and improves accuracy compared to barcode or manual systems. Studies confirm that RFID provides fast vehicle identification even under high traffic conditions. Different frequency ranges like LF, HF, and UHF are used based on distance and application needs. RFID integration with IoT enables real-time monitoring, cloud data logging, and automated notifications. Vehicle entry and exit timestamps are recorded, providing accurate historical logs. Security features such as tag encryption and authentication prevent cloning and unauthorized access. Research demonstrates RFID-based parking systems can handle multiple vehicles simultaneously without collision in data transmission. Integration with ESP8266 or ESP32 allows

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

seamless communication with mobile apps and dashboards. MQTT or HTTP protocols are commonly used for transmitting RFID data to cloud servers. RFID systems can trigger relays and motors for automated gate operation. Vehicle analytics can optimize traffic flow and parking utilization. Academic studies show RFID systems reduce congestion and increase operational efficiency. Real-time monitoring enhances security and prevents unauthorized access. RFID-based IoT systems provide cost-effective, scalable, and reliable solutions for vehicle management. Cloud dashboards enable administrators to manage multiple gates and receive alerts remotely. Studies suggest that RFID systems improve overall parking and access management. The literature confirms RFID as a reliable and essential component for automated vehicle entry systems.

3. ESP8266/ESP32-Based IoT Systems

ESP8266 and ESP32 microcontrollers are ideal for IoT-based vehicle management systems due to built-in Wi-Fi, low cost, compact size, and high reliability. Studies show these modules can handle multiple sensors, relay controls, and cloud communication efficiently. ESP modules support MQTT, HTTP, and WebSocket protocols, ensuring real-time communication. Academic research confirms stable performance under continuous operation and multidevice setups. OTA (Over-the-Air) updates simplify maintenance and firmware upgrades. Encryption, authentication, and unique device credentials ensure secure communication with the cloud. Microcontrollers can process RFID data, trigger relays, and update dashboards in real-time. Memory optimization ensures reliable performance even under high data load. ESP modules are energy-efficient and support low-power operation modes. Research highlights integration with dashboards and mobile apps for monitoring gate status, vehicle count, and alerts. Multiple gates can be controlled simultaneously without interference. Cloud-based analytics and historical data management are supported. ESP8266/ESP32 modules enable modular system expansion and additional IoT device integration. Studies demonstrate efficient control of motors, relays, and sensors for automated gate operation. Two-way communication ensures administrators receive real-time feedback. The literature strongly supports ESP8266/ESP32 as the preferred choice for IoT-based vehicle entry management.

The convergence of radio-frequency identification (RFID), embedded controllers, motor control, and IoT cloud services has produced a mature set of techniques for automating access control and vehicle management. This literature survey summarizes key findings and design lessons from research and applied development in four main areas relevant to the Smart Gate: (1) RFID for vehicle access; (2) embedded control, motor drivers and electromechanical gate actuation; (3) IoT connectivity, protocols and architectures for real-time monitoring; and (4) systems engineering concerns—security, privacy, scalability, reliability and analytics. Together these strands illustrate proven approaches, typical pitfalls, and open research directions for building robust, scalable Smart Gate deployments.

RFID for vehicle access control. RFID is widely adopted for vehicle identification because tags are inexpensive, durable, and can be read at short-to-medium ranges without line-of-sight. Studies and deployment reports indicate that passive UHF (860–960 MHz) and active LF/HF (125 kHz / 13.56 MHz) systems each have tradeoffs: UHF long read ranges (several meters) facilitate “drive-through” recognition but are sensitive to orientation, multipath, and metal surfaces (typical vehicle chassis); HF/LF are more robust near metal and for short range, making them suitable for close-proximity readers at a gate. Practical systems often choose tag frequency and reader antenna design based on expected stopping

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

distance and environment. Work in the field highlights the importance of tag placement and mounting (windshield, bumper) and recommend robust mounting (tamper-resistant holders) to maximize read reliability. Many projects combine RFID with additional confirmation (e.g., loop detectors or proximity sensors) to ensure a vehicle is present and to avoid false positives from tags left in nearby vehicles. Literature on access control emphasizes reliable anti-collision and tag filtering algorithms in high traffic scenarios to avoid multiple tag reads and erroneous authorizations.

Embedded controllers and motor actuation (L293D, drivers, safety). The electro-mechanical aspects of a Smart Gate—motorizing an arm, sliding gate, or barrier—require careful hardware selection and safety interlocks. The L293D and similar H-bridge drivers are commonly used in prototypes for DC motor control because of low cost and simple interface; however, literature warns about current limits, heat dissipation, and the need for flyback (snubber/diode) protection when driving inductive loads

III. SYSTEM ANALYSIS

EXISTING METHOD

Traditional vehicle entry systems depend on security personnel and manual logbooks, which are error-prone and slow. Guards verify vehicle details, record entry and exit times manually, and operate gates, causing delays and congestion during peak hours. Mechanical or automatic barriers require human intervention, increasing the chance of mistakes. Some automated systems use infrared sensors or barcode scanners but require line-of-sight and cannot uniquely identify vehicles. Bluetooth-based mobile access is limited to proximity and single-user operations. HTTP-based systems exist but rely on constant polling, increasing network load and reducing responsiveness. Existing solutions do not provide real-time vehicle count or remote monitoring. Mobile and web dashboard integration is often missing, forcing administrators to stay on-site. Unauthorized access is a significant risk in conventional methods due to minimal security features. Historical records are incomplete, making audits difficult. Scheduling rules, sensor-based automation, and alerts are generally absent. Traditional systems are not scalable for multiple gates or large parking areas. Congestion, errors, and slow response time reduce efficiency. Overall, existing methods fail to meet modern requirements for fast, secure, and real-time vehicle entry management.

The existing vehicle entry systems in residential complexes, offices, and parking areas primarily rely on manual verification by security personnel or basic mechanical gate systems. In such setups, guards manually check vehicle stickers or ID cards and record entry and exit details in logbooks. Some locations use simple remote-controlled gates without automated authentication or real-time tracking. These systems are inefficient during peak hours and lack digital monitoring capabilities. Manual processes often lead to delays, congestion, and inaccurate record maintenance.

Disadvantages:

1. Slow manual verification causing traffic congestion.
2. Human errors in recording vehicle details.
3. No real-time monitoring or remote access capability.
4. Security vulnerabilities due to visual verification only.
5. Inaccurate vehicle counting and poor record management.

PROPOSED METHOD

The Smart Gate system automates vehicle entry and exit using RFID, microcontrollers, and IoT. Each vehicle carries a unique RFID tag scanned at the gate. The ESP8266/ESP32 microcontroller verifies the tag and triggers a relay to operate the gate motor. Vehicle count

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

and status are updated in real-time to a cloud dashboard via MQTT or HTTP. Two-way communication ensures accurate monitoring of gates and vehicle movement. Multiple gates can function simultaneously without interference. Security is ensured with encrypted communication, device authentication, and unique credentials. Unauthorized vehicles trigger alerts to administrators. Historical data, including entry/exit timestamps, is logged in the cloud for analytics. Scheduling and sensor-based rules automate gate operation, improving efficiency and reducing congestion. The system minimizes human intervention, increases accuracy, and ensures smooth traffic flow. Administrators can remotely monitor vehicles, generate reports, and optimize parking space usage. The modular architecture allows future expansion and integration with additional IoT devices. Energy-efficient design ensures minimal power consumption. Alerts for suspicious or unauthorized vehicles improve overall security. Cloud storage ensures persistent record-keeping. Real-time monitoring enhances convenience, reliability, and operational control. Overall, the proposed system delivers a scalable, secure, and fully automated vehicle entry management solution suitable for modern residential, commercial, and industrial applications.

The proposed Smart Gate: IoT-Enabled RFID-Based Vehicle Entry and Real-Time Count Management System automates vehicle authentication using RFID technology integrated with Arduino and Wi-Fi connectivity. Each vehicle is assigned a unique RFID tag, which is scanned at the gate and verified by the microcontroller. Upon successful verification, the gate motor is activated through the L293D motor driver, and real-time vehicle count is updated in the cloud via MQTT or HTTP protocols. The LCD displays system status, and a buzzer alerts administrators in case of unauthorized access. This system ensures secure, fast, and accurate vehicle management with remote monitoring capability.

Advantages:

1. Automated and faster vehicle authentication.
2. Real-time vehicle count monitoring and cloud updates.
3. Enhanced security through RFID-based verification.
4. Reduced human dependency and operational costs.
5. Scalable and suitable for multiple gates and smart city applications.

IV. HARDWARE

4.1 ARDUINO UNO

The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. Uno board has a resistor pulling the 8U2 HWB line to ground, making it easier to put into DFU mode.Arduino board has the following new features:

- 1.0 pinout: added SDA and SCL pins that are near to the AREF pin and two other new pins placed near to the RESET pin, the IOREF that allow the shields to adapt to the voltage provided from the board. In future, shields will be compatible both with the board that use the AVR, which operate with 5V and with the Arduino Due that operate with 3.3V. The second one is a not

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

connected pin, that is reserved for future purposes.

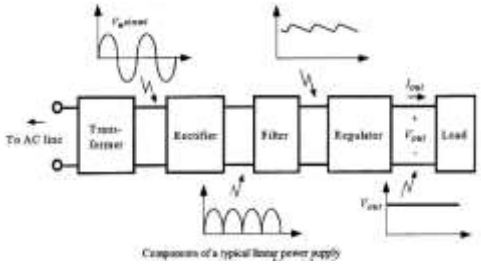
- Stronger RESET circuit.
- Atmega 16U2 replace the 8U2.

"Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version 1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform; for a comparison with previous versions, see the index of Arduino boards.

Fig: ARDUINO UNO

4.2. POWER SUPPLY

The power supplies are designed to convert high voltage AC mains electricity to a suitable low voltage supply for electronic circuits and other devices. A power supply can by broken down into a series of blocks, each of which performs a particular function. A d.c power supply which maintains the output voltage constant irrespective of a.c mains fluctuations or load variations is known as "Regulated D.C Power Supply".



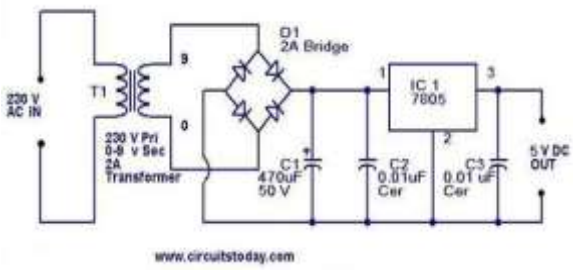


Fig: Schematic Diagram of Power Supply

4.2.1. TRANSFORMER:

A transformer is an electrical device which is used to convert electrical power from one Electrical circuit to another without change in frequency.

When AC is applied to the primary winding of the power transformer it can either be stepped down or up depending on the value of DC needed. In our circuit the transformer of 230v/12-0-12v is used to perform the step down operation where a 230V AC appears as 12V AC across the secondary winding.

4.2.2. RECTIFIER:

A circuit which is used to convert a.c to dc is known as RECTIFIER. The process of conversion a.c to d.c is called "rectification.

Bridge Rectifier:

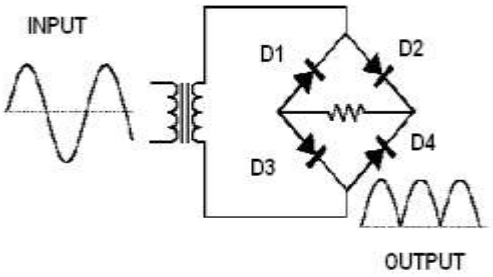


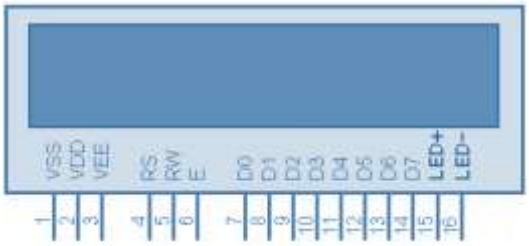
Fig: 4.6 Bridge Rectifier

Alphanumeric LCD

Liquid Crystal Display also called as LCD is very helpful in providing user interface as well as for debugging purpose. The most commonly used Character based LCDs are based on Hitachi's HD44780 controller or other which are compatible with HD44580. The most commonly used LCDs found in the market today are 1 Line, 2 Line or 4 Line LCDs which have only 1 controller and support at most of 80 characters, whereas LCDs supporting more than 80 characters make use of 2 HD44780 controllers.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Pin Description



4.3 BUZZER

What is a Buzzer : Working & Its Applications

There are many ways to communicate between the user and a product. One of the best ways is audio communication using a buzzer IC. So during the design process, understanding some technologies with configurations is very helpful. So, this article discusses an overview of an audio signaling device like a beeper or a buzzer and its working with applications.

What is a Buzzer?

An audio signaling device like a beeper or buzzer may be electromechanical or piezoelectric or mechanical type. The main function of this is to convert the signal from audio to sound. Generally, it is powered through DC voltage and used in timers, alarm devices, printers, alarms, computers, etc. Based on the various designs, it can generate different sounds like alarm, music, bell & siren.

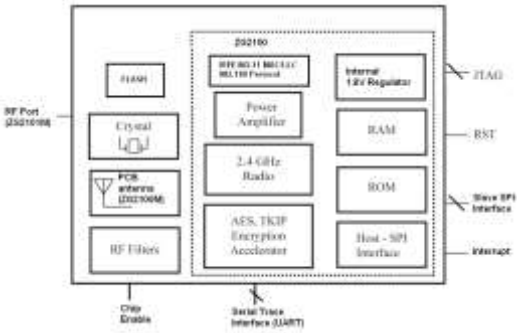
WIFI:

Description

The ZG2100M & ZG2101M modules are low-power 802.11b implementations. All RF components, the baseband and the entirety of the 802.11 MAC reside on-module, creating a simple and cost-effective means to add Wi-Fi connectivity for embedded devices. The module(s) implement a high-level API, simplifying design implementation and allowing the ZG2100M or ZG2101M to be integrated with 8- and 16-bit host microcontrollers.

Features

• Single-chip 802.11b including MAC, baseband, RF and power amplifier
• Data Rate: 1 & 2 Mbps
• 802.11b/g/n compatible
• Low power operation
• API for embedded markets, no OS required
• PCB or external antenna options
• Hardware support for AES and RC4 based ciphers (WEP, WPA, WPA2 security)
• SPI slave interface with interrupt
• Single 3.3V supply, operates from 2.7V to 3.6V (see section 5)
• 21mm x 31mm 36-pin Dual Flat pack PCB SM Package
• Wi-Fi Certified, RoHS and CE compliant
• FCC Certified (USA, FCC ID: W7O-ZG2100-ZG2101)
• IC Certified (IC: 8248A-G21ZEROG)
• Fully compliant with EU & meets the R&TTE Directive for Radio Spectrum

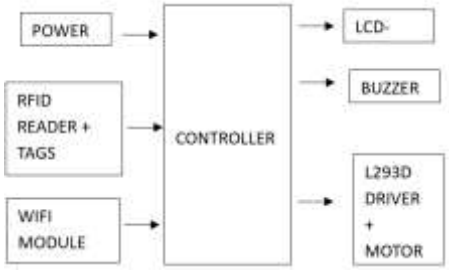


ZG2100M/ZG2101M Module: Functional Block Diagram

V. METHODOLOGY & IMPLEMENTATIONS

BLOCK DIAGRAM

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper



WORKING

1. Power Supply

The power supply provides regulated DC voltage (5V for Arduino, RFID, LCD; 12V if required for motor).

- Ensures stable operation of all electronic components.
- Supplies sufficient current for motor operation.
- Prevents voltage fluctuation that may cause system failure.

2. RFID Reader + Tags

Each authorized vehicle is assigned a unique RFID tag.

Working:

- When a vehicle approaches the gate, the RFID reader scans the tag.
- The reader captures the unique tag ID.
- The tag ID is sent to the controller via serial/SPI communication.

The RFID system acts as the authentication unit.

3. Controller (Arduino – Central Processing Unit)

The controller is the brain of the system.

Functions:

1. Receives tag ID from RFID reader.
2. Compares scanned ID with stored authorized database.
3. Decides whether access is granted or denied.
4. Controls outputs (LCD, buzzer, motor driver).
5. Updates vehicle count (increment/decrement).
6. Sends data to cloud via Wi-Fi module.

The controller executes the decision-making logic.

4. Verification Process

If Tag is Authorized:

- Access granted.
- Vehicle count is updated.
- Gate motor is activated.
- Entry timestamp is recorded.
- Data sent to cloud server.

If Tag is Unauthorized:

- Access denied.
- Buzzer alert activated.
- LCD displays "Unauthorized Vehicle."
- No gate movement occurs.

5. L293D Driver + Motor

The L293D is an H-bridge motor driver IC.

Working:

- The controller sends control signals to L293D.
- L293D drives the DC motor.
- Motor rotates to open the gate.
- After a delay, motor reverses to close the gate.

The driver protects the controller from high motor current.

6. LCD Display

The 16x2 LCD provides real-time system information.

It displays:

- "Scan Card"
- "Access Granted"
- "Access Denied"
- Vehicle count
- Wi-Fi status

This helps in local monitoring.

7. Buzzer

The buzzer provides audible alerts.

- Short beep → Authorized entry.
- Continuous beep → Unauthorized access attempt.
- Alarm mode for repeated invalid attempts.

Enhances security awareness.

8. Wi-Fi Module

The Wi-Fi module (ESP8266/ESP32) provides IoT connectivity.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

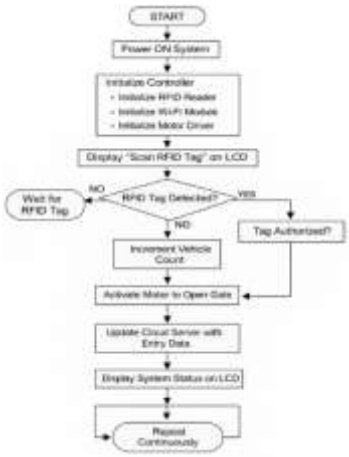
Working:

- Connects to internet via Wi-Fi.
- Sends entry/exit data to cloud using MQTT/HTTP.
- Updates real-time vehicle count.
- Enables remote monitoring via dashboard.

Administrators can view:

- Current occupancy
- Entry/exit logs
- Unauthorized attempts

Flow Chart



VI. CONCLUSION & FUTURE SCOPE

CONCLUSION

The Smart Gate system successfully demonstrates an efficient, secure, and scalable solution for automated vehicle access control and real-time monitoring using RFID and IoT technologies. By integrating RFID authentication with an Arduino-based controller, Wi-Fi connectivity, and cloud-based data management, the system replaces traditional manual gate operations with a fully automated approach. Each vehicle is uniquely identified through RFID tags, ensuring accurate authentication and eliminating the risk of human error during verification.

The use of the L293D motor driver enables controlled and reliable gate operation, while the LCD and buzzer provide immediate system feedback and security alerts. Real-time vehicle count management ensures accurate tracking of occupancy levels, helping administrators monitor traffic flow and parking capacity efficiently. The Wi-Fi module enhances the system's functionality by enabling remote monitoring and cloud-based data storage, allowing administrators to access logs, entry timestamps, and occupancy statistics from any location.

Compared to traditional gate systems, the Smart Gate solution significantly reduces congestion during peak hours, improves security through automated verification, and minimizes operational costs by reducing reliance on manual labor. The modular design ensures scalability, allowing multiple gates to operate simultaneously without interference. The system is reliable, cost-effective, and adaptable to various applications, including residential complexes, offices, parking facilities, and smart city infrastructures.

Overall, the Smart Gate system meets its objective of providing a secure, automated, and IoT-enabled vehicle entry management platform that enhances operational efficiency, safety, and convenience.

FUTURE SCOPE

Although the current system performs effectively, several enhancements can further improve its functionality, intelligence, and scalability.

1. Integration with License Plate Recognition (ANPR)

Combining RFID with Automatic Number Plate Recognition can provide dual-layer authentication for enhanced security.

2. Mobile Application Development

A dedicated mobile app can:

- Allow administrators to manage authorized vehicles.
- Provide instant push notifications.
- Display real-time analytics dashboards.

3. AI-Based Traffic Analytics

Artificial Intelligence algorithms can analyze historical vehicle data to:

- Predict peak traffic hours.
- Optimize gate opening schedules.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

- Detect unusual access patterns.

4. Smart Parking Allocation

Integration with parking sensors can enable automatic slot assignment and dynamic occupancy display.

5. GSM/SMS Alert System

In addition to Wi-Fi, a GSM module can send SMS alerts during unauthorized access or network failure.

REFERENCES

[1] Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.

[2] Gajula, S. (2026, March). Two Pillars of Banking Intelligence: A Comparative Analysis of AI Techniques for Fraud Prevention and Churn Mitigation. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

[3] Maturi, S. Y. (2024). Cryptographic privacy engines: Practical multi-party protocols for confidential database queries. Nanotechnology Perceptions, 20(S13), 2770–2785.

[4] Maturi, S. Y. (2024). Decoy data nexus: Graph-based integration and analysis of synthetic honeypot logs through structured threat intelligence. International Journal of Computational and Experimental Science and Engineering (IJCESEN), 10(4), 4255–4261. https://doi.org/10.22399/ijcesen.5010.

[5] Adabala, P. K. (2024). Utilizing predictive analytics to improve efficiency and decision-making in ERP-connected supply chains. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2465.

[6] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).

[7] P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Innovative Engineering and Management Research (IJIEMR).

[8] Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. International Journal of Enhanced Research in Science, Technology &Amp; Engineering, 10(07), 61–72. https://doi.org/10.55948/ijerste.2021.0708.

[9] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).

[10] Pavan Kumar Adabala. (2026). IoT-Driven Digital Twins for Manufacturing Optimization: Hybrid Modelling, Reinforcement Learning and Sustainable Operations. International Journal of Computational and Experimental Science and Engineering, 12(1). https://doi.org/10.22399/ijcesen.5050.

[11] P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. Eudoxus Press Journal.

[12] Pavan Kumar Adabala. (2026). Smart Retail Fuel Systems: IoT-Enabled Solutions for Loss Prevention and Environmental Safety. Computer Fraud and Security, 868–875. https://doi.org/10.52710/cfs.995.

[13] Pavan Kumar Adabala. (2026). Best Practices for Enterprise System Integration in Modern Organizations. Journal of Information Systems Engineering and Management, 11(2s), 1137–1146. https://doi.org/10.52783/jisem.v11i2s.14558.

[14] Srikanth Kavuri. (2025). AI-DRIVEN TEST AUTOMATION FRAMEWORKS: ENHANCING EFFICIENCY AND ACCURACY IN SOFTWARE QUALITY ASSURANCE. International Journal of Applied Mathematics, 38(10s), 699–710. https://doi.org/10.12732/ijam.v38i10s.990.

[15] Kavuri, S. (2025). Critical Review of Software Testing Problems in the Current Decade. International Journal on Science and

Technology, 16(2). https://doi.org/10.71097/ijsat.v16.i2.9469.

[16] Srikanth Kavuri. (2024). Probabilistic Generative Modeling for Synthesizing High-Coverage Test Data in Safety-Critical Software Applications. Computer Fraud and Security, 633–642. https://doi.org/10.52710/cfs.838.

[17] Kavuri, S. (Ed.). (2024). Shift-left and shift-right testing approaches: A practical roadmap for continuous quality in agile and DevOps. Journal of Information Systems Engineering and Management, 9(4). https://doi.org/10.52783/jisem.v9i4.127.

[18] Srikanth Kavuri. (2023). Machine Learning Approaches for Security Vulnerability Detection in Software Testing. Computer Fraud and Security. https://doi.org/10.52710/cfs.837.

[19] Srikanth Kavuri. (2022). Large Language Model (LLM)-Based Automation for Software Test Script Generation. Computer Fraud and Security. https://doi.org/10.52710/cfs.836.

[20] Venkata Pavan Kumar Gummadi. (2023). MuleSoft Batch Processing: High-Volume Streaming Architecture. Computer Fraud and Security, 50–57. https://doi.org/10.52710/cfs.886.

[21] Venkata Pavan Kumar Gummadi. (2026). Infrastructure Optimization Techniques for Enterprise Integration Platforms: A Comprehensive Analysis. Computer Fraud and Security, 37–44. https://doi.org/10.52710/cfs.875.

[22] Venkata Pavan Kumar Gummadi. (2024). API Design and Implementation: RAML and OpenAPI Specification. Journal of Electrical Systems, 16(4), 76–85. https://doi.org/10.52783/jes.9329.

[23] Venkata Pavan Kumar Gummadi. (2025). MuleSoft's Role in Advancing Sustainable Digital Infrastructure: An Enterprise Integration Perspective. Journal of Information Systems Engineering and Management, 10(62s), 1313–1321. https://doi.org/10.52783/jisem.v10i62s.13783.

[24] Venkata Pavan Kumar Gummadi. (2025). MuleSoft Architectural Paradigms and Sustainability: A Comprehensive Technical Analysis. Journal of Computer Science and Technology Studies, 7(12), 534–540. https://doi.org/10.32996/jcsts.2025.7.12.59.

[25] Harshitha, G. K., & Rajashekar, K. K. (2025). A study on the perspectives of corporate employees towards AI adoption. Journal of International Commercial Law and Technology, 6(1), 699–706.

[26] Kandula, S. T. R., Susarla, R. S., & Boyapati, P. K. (2025, July). Enhanced Cyber Security Using Global Local Artificial Neural Network Based Intrusion Detection in Big Data Environment. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 426-431). IEEE.

[27] Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219