



International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 10, October 2025



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Automated Vehicle Access Control and Unauthorized Entry Notification System

Bhavyashree H R, Dr. Rajendra C J

M.Tech in Electronics, Channabaswesara Institute of Technology, Gubbi, Tumkur, India

Associate Professor, Dept. of ECE, Channabaswesara Institute of Technology, Gubbi, Tumkur, India

ABSTRACT: In the rapidly evolving landscape of logistics, transportation, and industrial operations, the demand for secure, efficient, and automated systems has become increasingly significant. Imagine the daily rhythm of a modern warehouse or factory: the constant flow of delivery trucks, the urgent need to move goods efficiently, and the ever-present concern for security. For years, managing this has relied on manual, time-consuming methods—a security guard verifying paper IDs, handwritten logs at the gate, and workers manually sorting items. These outdated methods are more than just slow; they are a critical vulnerability. Each manual check is an opportunity for human error, and every paper log is a potential security gap. In today's fast-paced environment, a single unauthorized entry—whether by accident or malicious intent—can trigger a cascade of problems, from stolen assets to complete operational shutdown. As warehouses and factories scale up to meet rising demands, the fragility of these legacy systems becomes dangerously apparent.

I. INTRODUCTION

In the rapidly evolving landscape of logistics, transportation, and industrial operations, the demand for secure, efficient, and automated systems has become increasingly significant. Modern warehouses, manufacturing plants, and gated premises require robust mechanisms to control vehicle entry, ensure the safety of assets, and streamline operational workflows [2]. Traditional methods such as manual verification of identification cards, maintaining physical entry logs, and employing dedicated personnel for gate operations have long been in practice. These methods are often slow to execute and prone to mistakes. They can also be exploited, making them vulnerable to manipulation and security threats. In many instances, unauthorized entry can result in theft, loss of valuable resources, or disruption to ongoing operations. As industries expand and adapt to the growing demands of supply chains, the need for a more reliable, automated, and cost-effective approach has become essential [1].

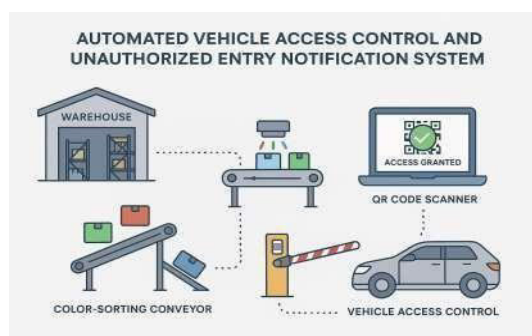
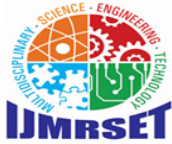


Fig.1 Automated Amazon Warehouse system

The advancements in automation and embedded systems have paved the way for innovative solutions that combine security with operational efficiency. It's no secret that the giants of e-commerce and logistics have turned their warehouses into high-tech marvels. They use sophisticated automation for everything from sorting millions of packages to controlling access, and the results are clear: things move faster, with fewer errors, and in a safer environment. However, this level of automation comes with a catch [2]. These systems often depend on a constant, high-speed internet connection, complex cloud computing, and expensive custom-built machinery.



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE SURVEY

The development of automated access control systems has seen significant advancements over the past two decades, driven by the growing demand for enhanced security, operational efficiency, and streamlined authentication processes. Traditional methods of vehicle access control, such as manual gate operation or visual inspection of identification documents, often introduce delays, require constant human supervision, and are prone to human error.

B. Anggara, A. H. Anshor, and W. Hadikristanto (2024) [1] highlighted the adoption of QR code-based authentication as a secure and low-cost identification method in warehouse inventory management. They emphasized its ease of generation and high storage capacity compared to traditional barcodes. Similarly, Udvaros et al. (2024) [4] investigated QR code use in e-business and logistics, confirming its adaptability for secure order tracking and authentication.

Petersen et al. (2025) [5] examined conveyor-based object sorting systems that employed sensors and optical methods for product classification, demonstrating improved accuracy and efficiency. In parallel, Chavan et al. (2024) [7] designed an IoT- based color sorting machine using ESP8266 and ThingSpeak, showing how microcontrollers can automate segregation processes.

Chavan et al. (2024) [7] also highlighted the use of multi-controller architectures, showing that separating tasks across ESP8266 microcontrollers enhanced both responsiveness and system reliability. IJAEM (n.d.) [10] similarly demonstrated that object sorting systems performed better when conveyor control and segregation logic were distributed, rather than centralized on a single unit.

Infizo (2023) [2] discussed the significance of security in vehicle access systems, emphasizing the role of real-time alerts in preventing unauthorized entry. Argosoftware (2025) [3] proposed email- based alerts as a cost-effective solution compatible with existing networks. According to IJAEM (n.d.) [10], integrating audible alarms on-site with GSM or email notifications creates a dual- layer security mechanism. Petersen et al. (2025) [5] further argued that such combined alerting systems help both on- site and remote staff to respond promptly to potential breaches.

IJRESM (n.d.) [9] reported that data logging and record-keeping are critical in access control and warehouse automation, as stored datasets enable both compliance tracking and incident investigation. ResearchGate (n.d.) [8] described how NodeMCU-based systems could log entry data for later analysis, thus improving transparency. Chavan et al. (2024) [7] added that analyzing historical segregation data provides insights into workflow optimization and predictive maintenance.

III. METHODOLOGY

The proposed system is developed as an integration of hardware and software components working in synchronization to manage vehicle entry and goods segregation. The system's access control is managed by a user-friendly Python application running on a laptop, which serves as the central command point. When a vehicle arrives, its QR code is presented to the laptop's camera.

The laptop serves as the main control interface for QR code detection and decision-making. The system commences a fully automated sequence upon vehicle detection. A real-time video feed from the laptop's integrated camera is processed to identify and authenticate a QR code. Following successful validation, a command is transmitted through a serial interface to an Arduino microcontroller, which subsequently actuates the gate mechanism.



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

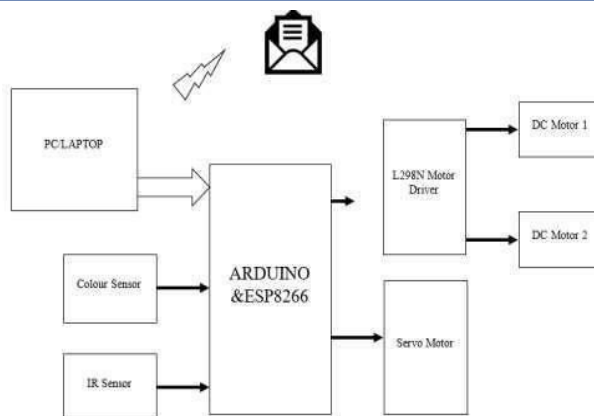


Fig.2 Block diagram of the proposed system

This deliberate functional allocation—delegating computationally intensive image processing to the laptop and discrete physical control to the microcontroller—optimizes system efficiency. The architecture ensures minimal latency and maximizes reliability at the point of entry, thereby enforcing access privileges with a high degree of accuracy.

ARDUINO UNO

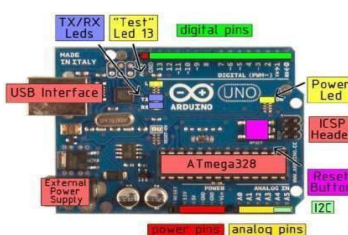
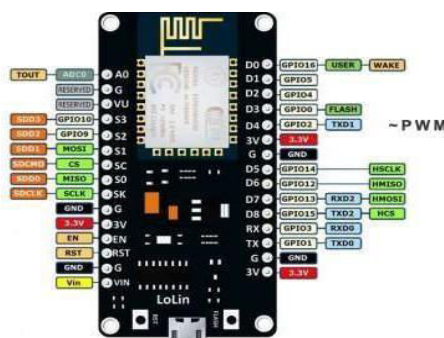


Fig.3 Arduino Uno

The Arduino Uno is one of the most popular microcontroller boards, built around the ATmega328 chip. It can be powered either through a USB connection or an external power source, such as a battery or an AC-to-DC adapter. The board automatically selects the appropriate power source, with a recommended input voltage range of 7–12 V for stable operation (although it can technically work between 6 V and 20 V). Supplying less than 7 V may cause instability, while going above 12 V can overheat the voltage regulator[4].

NODEMCU





International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

NodeMCU is an open-source IoT platform that combines firmware running on the **ESP8266 Wi-Fi SoC** from Espressif Systems with hardware based on the **ESP- 12 module**. While the term “NodeMCU” often refers to the firmware itself, it is also associated with the development boards that host it. The firmware is programmed using the **Lua scripting language**, built on the eLua project, and developed over the Espressif Non-OS SDK for the ESP8266. It integrates several open-source components, such as *lua-cjson* for JSON handling and *SPIFFS* for file storage [3].

DC MOTOR

A DC motor is an electromechanical device that converts direct current (DC) electrical energy into mechanical rotational energy. It is widely used in industrial, commercial, and robotic applications due to its simple construction, reliable performance, and ease of control.

Armature (rotor), A coil of wire carrying current, connected to the supply via commutator segments and carbon brushes. Magnetic Field Source to Provided either by permanent magnets or electromagnets (stator). Commutator & Brushes is to Maintain current flow in the armature windings while allowing rotation



Fig.5 DC Motor

COLOUR SENSOR

The color sensor is an optical sensing device designed to detect and distinguish different colors based on the light reflected from an object. It works by emitting light, typically through red, green, and blue (RGB) LEDs, and then measuring the intensity of the reflected light for each color channel. By analysing the intensity values, the sensor can determine the exact color or shade of the object being scanned [1].

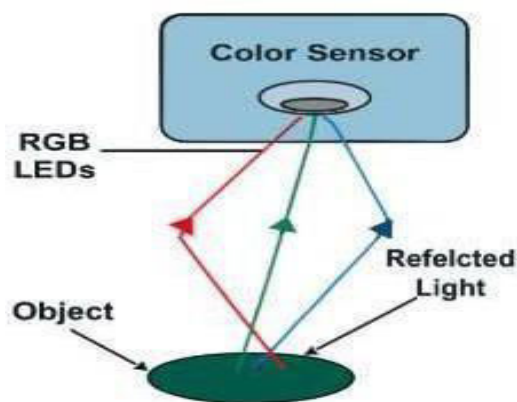


Fig.6 Colour Sensor



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. FLOWCHART

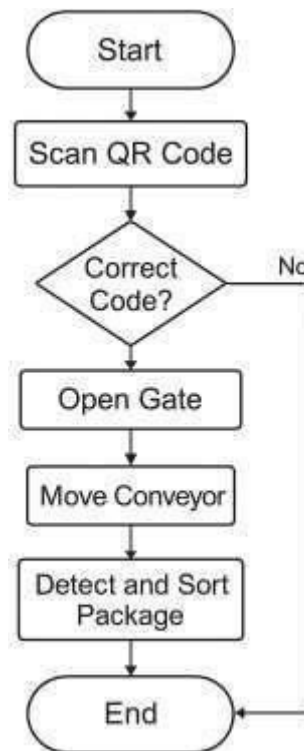


Fig.7 Flowchart of Proposed System

- Start

The process begins with the system in standby mode, waiting for a package or item to be scanned for verification.

- QR Code Scanning via Laptop

A QR code scanner connected to the laptop reads the code on the package. The laptop runs a program that verifies the QR data against the stored database.

- QR Verification

1) If the QR code is correct: The laptop sends a signal to the Arduino to initiate the conveyor mechanism.

2) If the QR code is incorrect: The process stops, and an alert is generated for manual inspection.

- Arduino Processing

When the correct QR signal is received from the laptop, the Arduino activates the conveyor motor, enabling the item to move along the belt.

- ESP8266 Module Control

The ESP8266 is dedicated to managing the conveyor mechanism. It receives data from:

1) IR Sensor: Senses and confirms the presence of a package on the conveyor belt.

2) Colour Sensor: Determines the color of the package to ensure sorting accuracy.

- Package Movement

As the conveyor runs, the IR sensor ensures continuous detection, while the color sensor confirms if the item meets the required specifications.

- Sorting or Processing

1) If the item matches the required specifications (color/size/position), it is directed to the correct bin or path.

2) If it doesn't match, the conveyor can be stopped, and the package can be diverted or rejected.

- End Process

The process completes for the current package, and the system resets to standby mode, ready for the next item.



International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. RESULTS & DISCUSSIONS

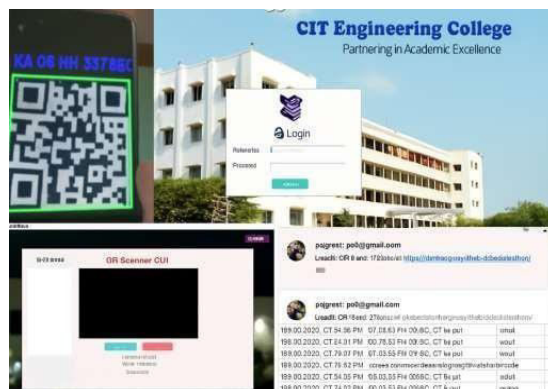


Fig.8 Result Analysis

The developed QR code authentication system was tested under real-time conditions to evaluate its performance, accuracy, and reliability. Various valid and invalid QR codes were scanned to assess detection speed, error handling, and the effectiveness of the alert mechanisms.

VI. CONCLUSION

The developed system successfully integrates NodeMCU and Arduino to automate conveyor operations with enhanced security through QR code authentication. By combining IR sensors, color sensors, and motor drivers, it achieves accurate detection, sorting, and controlled movement of items. The ability to log data into CSV files and send alert emails improves monitoring, traceability, and safety, even without remote access. Its compact design, low power consumption, and cost-effectiveness make it a practical solution for secure, small-to-medium scale automation needs.

REFERENCES

- [1] "Top 3 Ways QR Codes Can Simplify Inventory Management in Warehouses," Infizo, published ~1.2 years ago.
- [2] "Optimize Asset Management with Effective QR Code Tracking," Argosoftware blog, published last month.
- [3] J. Udvaros et al., "The Application of QR Codes in the Field of E- Business in the Case of Order Tracking and Logistics," EMC 2024, International Symposium, June 2024.
- [4] D. Petersen et al., "Conveyor Line Color Object Sorting using a Monochrome Camera, Colored Light and RGB Filters," arXiv, Feb 2025.
- [5] "Colour Based Product Sorting Project Report – Automation," Scribd, generic overview.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com