Received: 22 April 2024 | Revised: 20 September 2024 | Accepted: 8 October 2024 | Published online: 14 October 2024

RESEARCH ARTICLE

Archives of Advanced Engineering Science
2025, Vol. 3(3) 214–225
DOI: 10.47852/bonviewAAES42023179

RFID Occupied Advanced Framework for Specialized Vehicle Access, Operating System, and Wireless Data Transmission Without Human Intervention

Abdullah All Mamun Anik[1,*], **Mosammat Sadia Akter Moon**[2], **Fahim Faysal Arnob**[3], **Mehedi Hasan**[4], **S. A. Naimul Hoque**[5], **Mohammad Mashhunur Rahman**[6], **Tanzim Bin Ahmed**[7] **and Tonmoy Barua**[8]

[1]*Department of Mechanical Engineering, University of Huddersfield, UK*

[2]*Department of Computer Science and Engineering, University of Chittagong, Bangladesh*

[3]*Department of Mechanical Engineering, Military Institute of Science and Technology, Bangladesh*

[4]*Department of Mechanical Engineering, University of Arkansas, USA*

[5]*Department of Electrical, Electronics and Communication Engineering, Military Institute of Science and Technology, Bangladesh*

[6]*Department of Aeronautical Engineering, Military Institute of Science and Technology, Bangladesh*

[7]*Department of Electrical and Electronics Engineering, American International University Bangladesh, Bangladesh*

[8]*Department of Civil Engineering, Curtin University, Australia*

Abstract: Radio frequency identification system (RFID) tags are tiny electronic devices that include a distinctive code that can be detected by a reader that supports RFID. The string of characters is used for recognizing and monitoring the object to which the tag is connected. RFID tags interact with RFID readers using radio frequency. While the tag comes into close proximity to the scanner, that device sends a radio signal that triggers the tag. The tag then responds by sending its unique identity. RFID pinpointing ability is verified experimentally in two different techniques: one utilizing radar and the other a photosensitive transition. The initial phase is intended to test if the continuously changing location provided from RFID tags equals the precise position recorded by sonar. It is also excellent for getting into parking lots, private spaces, professional parking spots, and offices quickly and easily. The implementation of RFID will bring a revolutionary transformation in the authorization, administration, correspondence, computerization, and security systems for specialized vehicle access, operating system, and wireless data transmission without human intervention using an Internet-based wireless communication system. RFID vehicular registration is an authentication system which employs RFID readers to give authorization for automobiles. The technique normally consists of installing a reader with RFID technology at the entrance/exit entrance to an enclosed or a limited region. RFID scanning can deliver efficient techniques for transportation administration, making the process straightforward, dependable, as well as secure.

Keywords: wireless network, Internet of Things (IoT), radio frequency identification (RFID), automation, control, data transmission, artificial intelligence (AI)

1. Introduction

Vehicles/ robots may be automatically identified and tracked with tags that use radio frequency identification system (RFID) attributable to a mechanism called a radio frequency identification-based vehicular management system [1]. The components of the technology are RFID tags affixed to the robots and an RFID reader placed at the storage facility or storage lot's crossover points.

The technology immediately activates or disables the operating system upon detecting a vehicle with an RFID tag [2]. Specifically, the idea of a basic identification sequence that can be recognized by an instrument has been supplemented with the implementation of an automated vehicle resolution and a dual-direction conversation method. The RFID reader examines the data contained in the tag.

[*] **Corresponding author:** Abdullah All Mamun Anik, Department of Mechanical Engineering, University of Huddersfield, UK. Email: abdullahallmamun.anik@hud.ac.uk

This type of system offers a safe and effective method of controlling robotic vehicle entrance and operation in a variety of settings, including real-time monitoring, integration with other systems, remote access, scalability, user-friendly interface, analytics, and reporting capabilities, enabling better decision-making and management [3]. It will support the management of all RFID-related technologies, including electromagnetic and low bandwidth. In a vehicle authorization structure, RFID is essential [4]. By decreasing the number of employees and increasing precision and effectiveness, it streamlines the system. The data accessibility on clouds is the responsibility of cloud-based vehicular access control systems, so that any inquiry may be responded at any time and from any location [5]. In spite of the implementation, this structure's durable architecture, weather-related rebellion (precipitation, snowy conditions, extremes of temperature, and other ecological pressure), dirt and allergen obstructions, mechanical rattle pressure, toughness to shock, along with electromagnetic and field electrical objections all come together the demanding requirements of the transportation manufacturing while guaranteeing dependability, efficiency, and protection. For RFID activities, multiple spectrum bands are designated. The system offers technologies that are reliable, productive, and adaptable for all vehicle-based RFID applications.

2. Literature Review

2.1. RFID-based wireless communication system

Vehicle operating system verification, monitoring, and control have historically been the main focuses of RFID applications [6]. Nonetheless, Internet of Things (IoT) installations are employing contemporary applications based on RFID, which capitalize on the wide frequency bands in which RFID functions, especially the UHF and microwave band frequencies [7]. IoT item recognition is supported via RFID, which may be used as a wireless communication platform. Systems can keep an eye on and vehicle systems, which are represented in a framework that resembles the internet [8]. RFID and IoT technologies are presently coming together with the creation of IoT-based, self-governing data gathering, transmission, and response systems. RFID is currently being used to interconnect vehicular things and give them intelligence by combining it with additional data processing instruments like GPS technology, GPRS, or WSN system [9]. A number of advancements have been making place in light of the present state of technology for transit today. A significant amount of investigations and investigations focused on using webcams for automobile inspection, computerized methods for automobile recognition, and radio frequency identification, the IoT embedded microcontroller, as well as GPS communication for observation [10]. Thus, in order to address concerns about flexibility safeguarding, scientists have come up with mechanisms and techniques related to IoT, integrated transport systems, and autonomous automobile identification. These efforts have produced notable progress [11]. The makeup, fields of study, and additional objectives of the publications and specialties significantly differed [12]. The following article introduces the concept of using radiofrequency for identity management [13, 14]. It accumulates, archives, contends, and preserves details recognized from transportation robots operating on the highway, crossing road entrances, observing the robot's circumstance, and stepping into or out of a location utilizing RFID identifiers, additionally collecting and uploading Tag ID metadata to a central station, resulting in what the investigators want to bring in and respond in the present work [15]. On the flip side of the hand, it came to light that the stated solutions have flaws in that they are unable to determine whether the owner is driving his own car or being driven by another [16].

2.2. Challenges of using RFID in IoT applications

The RFID has a lot of promise for creative, combined, IoT purposes; nevertheless, there are right now several restrictions and difficulties.

- **Impediments:** RFID transmission is vulnerable to electromagnetic disturbance and espionage in its simplest form.
- **Interactions:** It may also arise from concurrent communications, as RFID devices and chips often utilize identical wireless links for operation. This results in higher energy and bandwidth utilization as well as authentication delays.
- **Safety and confidentiality categories:** RFID need strong defenses against hackers and snooping. RFID-based networks can be misused by unapproved people or malware and might jeopardize mainline IoT infrastructure if access control measures aren't in existence.
- **Expenses:** RFID chips are costly and more manufacturing, and research will be needed to combine IoT sensor and controller techniques and offer dependable verification.
- **Coordination:** In order to successfully integrate RFID into current IoT systems, standard modifications are needed.

2.3. List of abbreviations

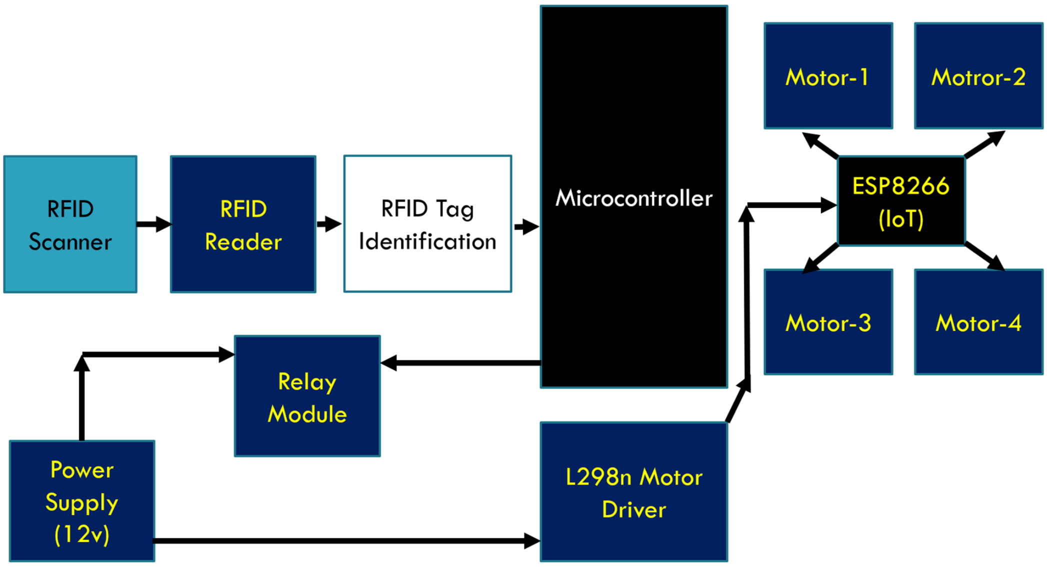
Mostly used abbreviations in this research paper are attached below:

- **RFID:** Radio Frequency Identification
- **IoT:** Internet of Things
- **UHF:** Ultra High Frequency
- **GPS:** Global Positioning System
- **GPRS:** General Packet Radio Service
- **WSN:** Wireless Sensor Network
- **AI:** Artificial Intelligence

3. Materials and Methodology

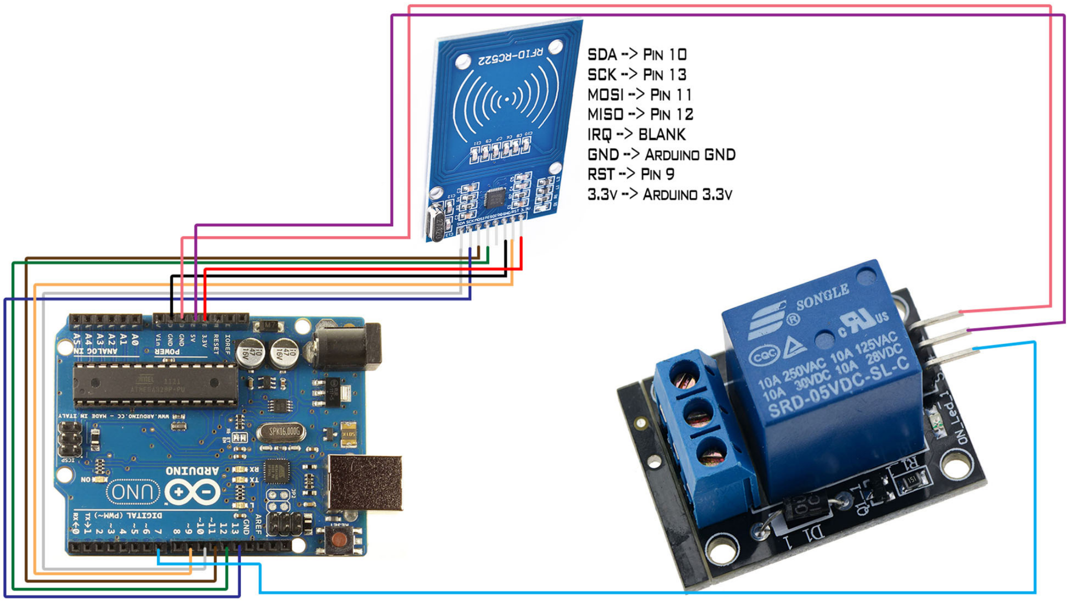
Towns are struggling to provide liveable, dependable, and convenient living circumstances as the world's population grows and industrialization takes place due to lack the requisite infrastructure to function properly. Thankfully, IoT, which links tangible things through electronic devices, software, sensing devices, and networked communication, has arisen as an approach to this problem. This has changed the supporting structures of smart cities, bringing in a variety of innovations that improve long-term viability, efficiency, and convenience for urban residents. There are now more options than earlier to plan and run prospective smart cities because of the use of artificial intelligence (AI) to evaluate the massive amounts of IoT data accessible. In the present paper, we define their features and explore the conceptual framework of IoT and RFID unification to give a general overview of RFID-occupied specialized robot. Figure 1 represents the basic architecture of IoT-integrated RFID-occupied specialized vehicle.

Figure 1
RFID-occupied vehicle with IoT architecture



The greater frequency of suspected transportation thefts was caused by an abundance of safety precautions in the transportation vehicle. RFID could deliver more safeguards and help to lower the quantity of vehicle thefts. When an individual wishes to ignition or depart on the engine of their vehicle, the device will function like an extra key. The intention of this system is to provide the vehicle with even more proactive security. A Programmable Interface Controller, a RFID chip, and an identification tag are the entire system's primary constituents. The blueprints will ultimately be followed in the assembly of all the parts. The Programmable Interface Controller will then be configured to correspond to the implementation, causing it to give an intense electrical signal to the LED that lights up. To enable its use in real-life situations, this LED will be tweaked and attached to a relay module. The device that holds the reader will decode the tag's contents when it is attached to it and communicate info to Programmable Interface Controller. The Programmable Interface Controller will scrutinize the information pertaining to that identification card's numerical serial number and match it to the number on file with the Programmable Interface Controller. The individual may begin their journey with vehicle if their identification information is accurate, but they are unable to do so if it is erroneous. The outcome demonstrates that the LED light turns on while the right tag is inserted into the reader with RFID tags. As a result, automotive manufacturers may consider this technology as a single prevention measure for vehicle burglaries. Identification process has been showcased in the Figure 2.

Figure 2
RFID accessed authentication system for robotic vehicle operation



The identity card can be switched with a different individual's ID or forgotten and eliminated by the proprietor of the vehicle, allowing a person who is not authorized to enter the vehicle. The proof of identity can be exchanged for another individual's Identity or forgotten and destroyed by the individual who owns the vehicle, allowing a third party to use it. As a result, new problems are permitted to enter the region. In additional cases, the robotic device's owner was notified through the application of sensor-integrated tags, a variety of Arduino microchips, an inherent video safeguarding alert, along with the convergence of RFID as a technology the IoT, embedded systems, and GSM wireless networks. This subsection includes thorough, concise descriptions of how each gadget works, predominantly with regard to the microprocessor that is used. In order to ensure the operational scope of the experiment, the researchers modified the pairing of RFID Identification, the foundation of GSM as well as the camera observation and included an entrance gateway mechanism employing a servo motor for movement. The procedure of RFID-occupied advanced robot framework integrated with IoT-based system is depicted in the structure schematic. Every authorized robot owner receives a wireless identification RFID tag with the same identifiable registration. When a card like this is inserted in front of the RFID scanner, the development board for Arduino analyzes the tag's characteristics. While the tracking device is inserted, the yellow signal of light demonstrates and the safety latch broadens with an electric servo motor, along with offering a text message alert by means of the worldwide positioning system component with the precise identification of the robot's proprietor as well as the specific day alongside period of time, resulting in instantly gets recorded on an encrypted repository by means of the text message. Whenever no tag has been identified from the robot's owner, the allocated safeguard transmits an SMS and then confirms about the system whether it will give permission to start the entire operating system or not. Block diagram of our recent contemporary work is shown in Figure 3.

Moreover, Figure 4's architecture demonstrates exactly the imaging device works with the help of a sensor that emits sound to identify an autonomous device and subsequently takes a photo of the automobile whose presence the scanner has detected and promptly saves data onto a Mini SD systems storage card for future reference. The photo acquisition timestamp has been determined using immediate duration. In addition, when an identification card is inserted near the edge of the RFID reader, a buzzer sounds to notify the designated guardian and boost protection within the robot boundaries. A portable transmitter mounted to an examining radar and a number of communicating and receiving tags—which act as probes and record data—make up the main components of RFID tracking devices. The attached antenna establishes a hyperlink amongst the scanner and its receiver. Depending on whether an electronic component is embedded in the identification device or not, two separate technologies for RFID exist: microchip-based RFID and chip-less RFID. There is another chip-less RFID that makes use of subsurface acoustic oscillations; fortunately, it is not the same as other chip-less RFID kinds since it depends on a piezoelectric phenomena rather than the dispersion of electromagnetic spectrum. The information subsequent to it will provide an introduction to such RFID techniques and each of their distinct detection strategies. GPS, wireless communication system, and RFID integrated operating system's advanced framework also give us real-time data and tracking information. It has been showed in the Figure 4.

3.1. System design and development

The electromagnetic waves emitted by radar imaging transmitter are often matched with the interaction that takes place between the gadget that tracks and the device being scanned. In reality, the infamous "tag equation", which resembles the formulae of the microwave segment, is used to represent variables like the effectiveness, radio advancement, and read range of the radio frequency antennas in the creation process. The objective's

Figure 3
Block diagram of RFID-occupied advanced framework for specialized vehicle access, operating system, and wireless data transmission without human intervention

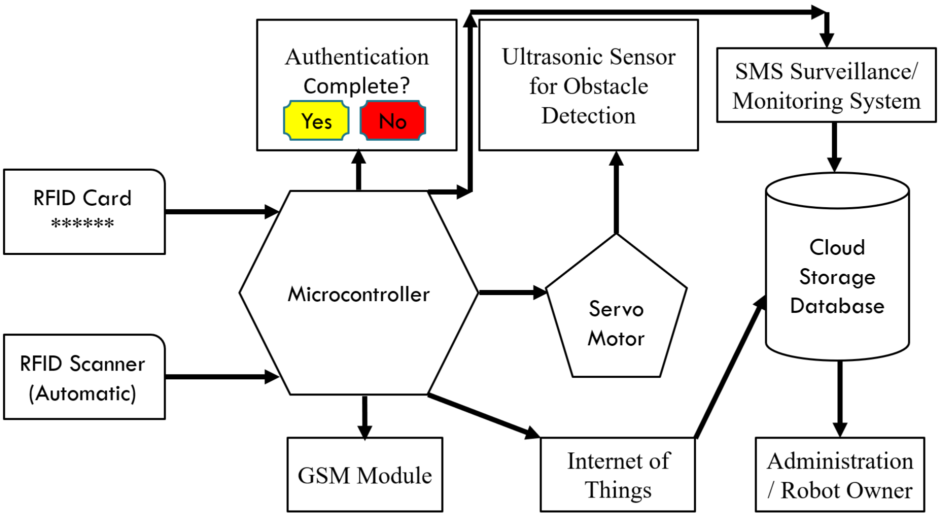


Figure 4
Advanced framework for specialized vehicle access, operating system, and wireless data transmission protocol

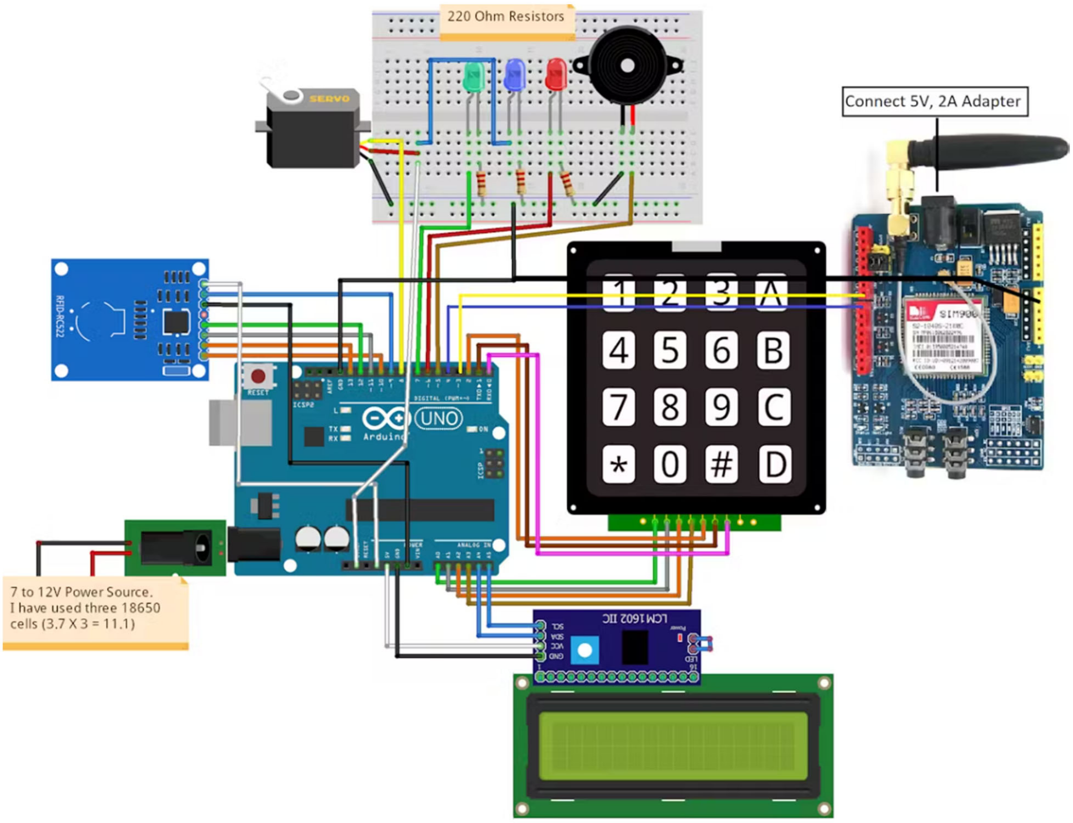
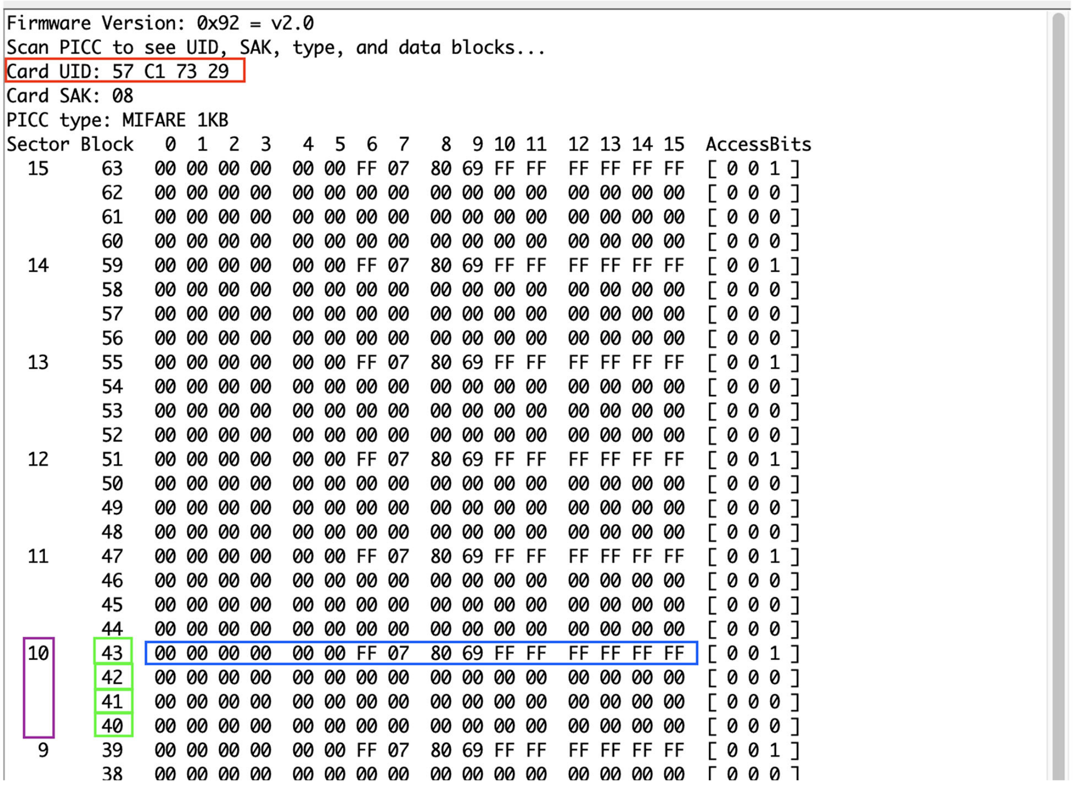


Figure 5
UID checking system for every RFID tag



```
Firmware Version: 0x92 = v2.0
Scan PICC to see UID, SAK, type, and data blocks...
Card UID: 57 C1 73 29
Card SAK: 08
PICC type: MIFARE 1KB
Sector Block   0  1  2  3   4  5  6  7   8  9 10 11  12 13 14 15  AccessBits
  15     63   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         62   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         61   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         60   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  14     59   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         57   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         56   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  13     55   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         53   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         52   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  12     51   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         50   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         49   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         48   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  11     47   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         46   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         45   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         44   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  10     43   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         42   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         41   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         40   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   9     39   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         38   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
```

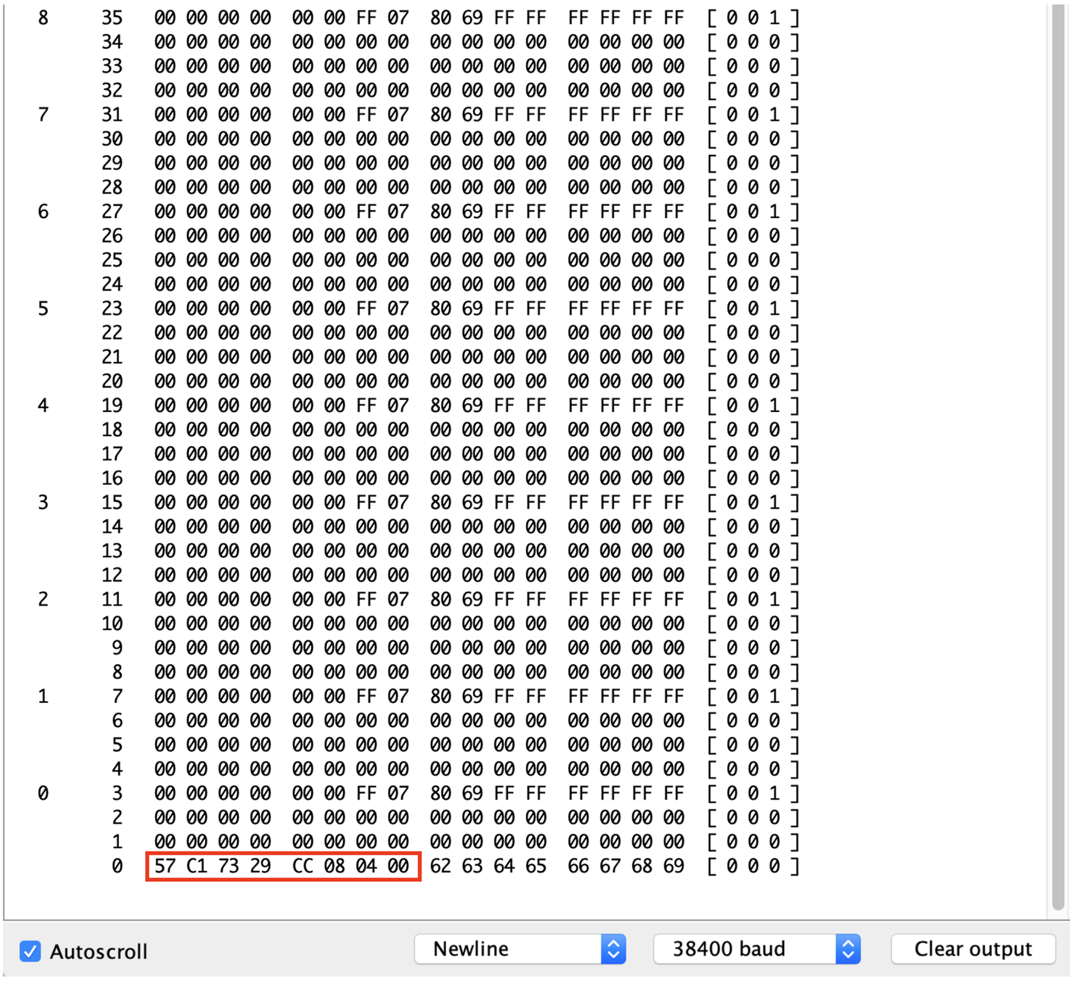
impedance compatibility issue is the sole distinction among microwave and RFID technologies; the object's frequency matching issue is not a cause for worry for radar-equipped devices. An antenna that is not only a scatterer is the objective of an RFID implementation. Taking into account the compatibility of susceptibility and divisiveness, the systems are used to calculate the energy received by the electronic equipment inside the terminal. It takes an enormous amount of effort to communicate through an RC522 RFID section, but fortunately, there is a library space named the MFRC522 library which renders the operation of reading and writing tags using RFID easy. The documentation must be installed first because it remains a component of Arduino microcontroller unified developmental setting. To configure the repository, choose the Sketch button first, then go to include specific libraries, after that use the button entitled manage to configure libraries. Finally, enable the System manager to update the file structure of enrolled databases while obtaining the stored indicator. The information saved in the tag is simply read by this sketch and displayed. Before attempting the latest identifiers, this layout might be quite helpful. Return to the initial phase of the schematic and ensure that RST_PIN is appropriately configured; in our scenario, we're using electronic pin #5, so update the value to 5. Now, activate Serial Monitor then publish the code. Once you move this tag nearer to the module, you'll observe something similar. Move the tag's position only after all of the details have been presented. It reveals all of the tag's pertinent details such as the Unique ID (UID), memory extent, and the complete 1K storage.

3.2. UID recognition for new RFID

For every RFID card, we will get its own RFID identification code/number which we will add for the authentication purpose for robot's main operating system. When a registered RFID Id will be recognized through microcontroller and IoT-integrated system, the operating system of the robot will start its own operation otherwise several attempts of the RFID tag will never be given access to continue the robot's operation. UID checking system and vehicle operating system-based RFID-generated recognition protocol is shown in Figures 5 and 6 consecutively.

We have used multiple RFID card for our recent experiment by using the same recognition process explained in Figure 7. We have attached those RFID card in our server to give access to the authorized RFID registered members. and so on.

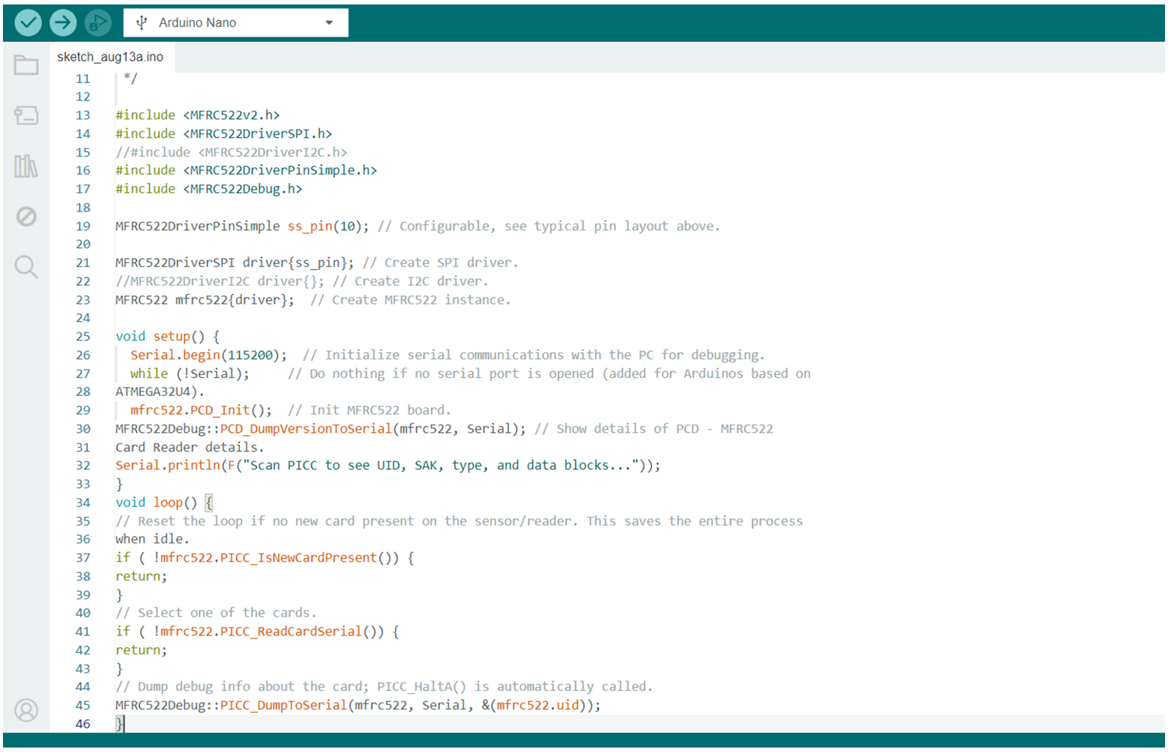
Figure 6
RFID-occupied operating system switching UID



```
  8     35   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
        34   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        33   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        32   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  7     31   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
        30   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        29   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        28   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  6     27   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
        26   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        25   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        24   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  5     23   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
        22   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        21   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        20   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  4     19   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
        18   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        17   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        16   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  3     15   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
        14   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        13   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
        12   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  2     11   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
        10   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         9   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         8   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  1      7   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         6   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         5   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         4   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  0      3   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         2   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         1   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         0   57 C1 73 29  CC 08 04 00  62 63 64 65  66 67 68 69  [ 0 0 0 ]
```

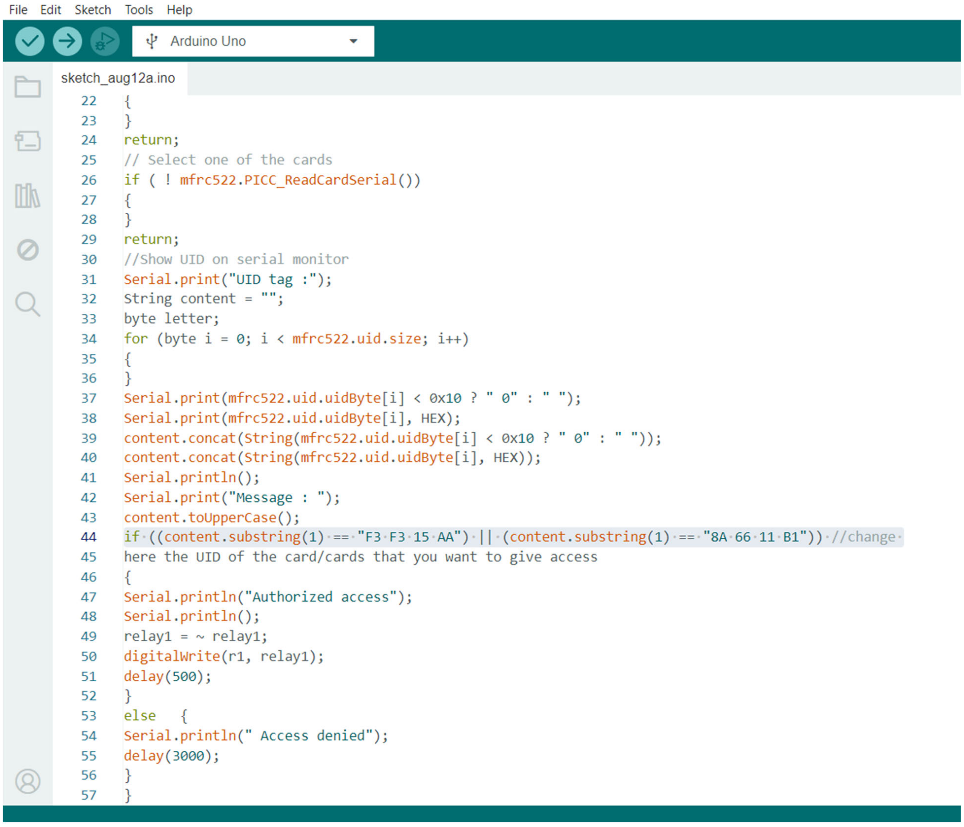
☑ Autoscroll Newline 38400 baud

Figure 7
RFID-generated authorization system



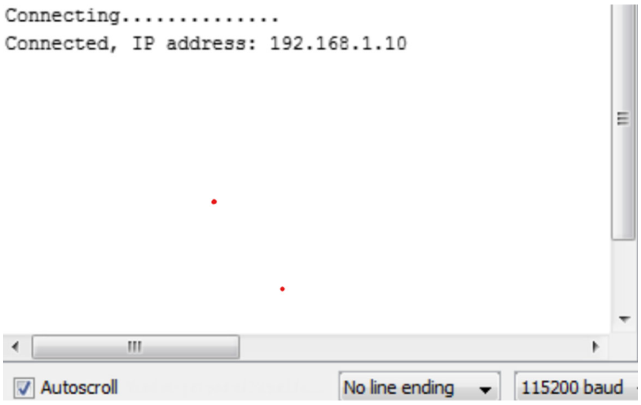
```
 */

#include <MFRC522v2.h>
#include <MFRC522DriverSPI.h>
//#include <MFRC522DriverI2C.h>
#include <MFRC522DriverPinSimple.h>
#include <MFRC522Debug.h>

MFRC522DriverPinSimple ss_pin(10); // Configurable, see typical pin layout above.

MFRC522DriverSPI driver{ss_pin}; // Create SPI driver.
//MFRC522DriverI2C driver{}; // Create I2C driver.
MFRC522 mfrc522{driver};  // Create MFRC522 instance.

void setup() {
  Serial.begin(115200);  // Initialize serial communications with the PC for debugging.
  while (!Serial);     // Do nothing if no serial port is opened (added for Arduinos based on
ATMEGA32U4).
  mfrc522.PCD_Init();  // Init MFRC522 board.
MFRC522Debug::PCD_DumpVersionToSerial(mfrc522, Serial); // Show details of PCD - MFRC522
Card Reader details.
Serial.println(F("Scan PICC to see UID, SAK, type, and data blocks..."));
}
void loop() {
// Reset the loop if no new card present on the sensor/reader. This saves the entire process
when idle.
if ( !mfrc522.PICC_IsNewCardPresent()) {
return;
}
// Select one of the cards.
if ( !mfrc522.PICC_ReadCardSerial()) {
return;
}
// Dump debug info about the card; PICC_HaltA() is automatically called.
MFRC522Debug::PICC_DumpToSerial(mfrc522, Serial, &(mfrc522.uid));
}
```

Figure 8
Registered: RFID tag authentication through AI



```
{
}
return;
// Select one of the cards
if ( ! mfrc522.PICC_ReadCardSerial())
{
}
return;
//Show UID on serial monitor
Serial.print("UID tag :");
String content = "";
byte letter;
for (byte i = 0; i < mfrc522.uid.size; i++)
{
}
Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
Serial.print(mfrc522.uid.uidByte[i], HEX);
content.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
content.concat(String(mfrc522.uid.uidByte[i], HEX));
Serial.println();
Serial.print("Message : ");
content.toUpperCase();
if ((content.substring(1) == "F3 F3 15 AA") || (content.substring(1) == "8A 66 11 B1")) //change
here the UID of the card/cards that you want to give access
{
Serial.println("Authorized access");
Serial.println();
relay1 = ~ relay1;
digitalWrite(r1, relay1);
delay(500);
}
else  {
Serial.println(" Access denied");
delay(3000);
}
}
```

Figure 9
Robot's Internet connection and IP address



```
Connecting..............
Connected, IP address: 192.168.1.10
```

3.3. Registered RFID tag authentication

Following the successful reading of an RFID tag, we will proceed to the next experiment. The confirmed UID will thereafter be granted permission to perform robot operations.

The use of RFID Particularized Robot is equipped with an RFID UID = B1 C7 K5 20, 8A 66 11 B1, 5M J4 23 O2, G7 80 33 K9, F2 B6 61 I5, 7C 33 44 T7 safeguarding authentication validating clearance via computerized automation technology by means of embedded system. Registered RFID tag authentication process using AI has been demonstrated in Figure 8. We must guarantee a functional internet connection and communication infrastructure in order to automate and operate robots. The confirmation of the Wi-Fi connection, and its unique IP address to access the server were stationed 192.160.0.104. After RFID-based verification, we can automate and operate the RFID-occupied robot by employing an Internet-based wireless communication system. Wireless connection and interconnected IP address are showcased in the Figure 9.

The concept is intended to drive an artificially intelligent robot utilizing IoT with an Android application. The NodeMCU device is connected to the robot's control board to detect instructions provided by the app running on Android over a web-based connectivity via a particular IP address. This information is sent to the operating system, which causes the robotic device to shift its position. The NodeMCU microchip is the driving force behind the entire project. Through an intuitive GUI that may depends on touchscreen communication working, any smartphone or tablet running an Android OS may perform faraway functions. On the opposite extremity of the bandwidth, a smartphone-enable device communicates through commands. At the intersection, commands are transmitted to the automation to move in all directions. Six independent electric motors which are controlled by an IoT incorporated microprocessor. Sequential input is sent via the application for smartphones and is collected by a NodeMCU equipment to communicate with the command framework. The software on the embedded system communicated with serial information in order to produce appropriate results considering the information provided to run the electric motors within the motor controller(L298n) integrated circuits. The engines are connected with the programming segment by the driveshaft operator Chip. Images and data, including transmitted footage, are being monitored via a cloud repository that is connected to the online via a specific protocol endpoint. One must finish the radio frequency detection procedure beforehand booting up the entire running system. Otherwise, we cannot start the robot's operating system without identity confirmation. Registered robot's owner can get the access to explore the robot easily. We can easily off the total operating system through another registered RFID authentication key. Operating system, reaction time, SMS notification, and cloud data information update status are shown in Table 1.

Table 1
Different RFID-occupied operating protocol

Operating system with RFID-occupied system	Access status	Reaction time (Second)	SMS notification status and cloud database information update
RFID(B1 C7 K5 20) Operating System(On)	Access given	0.81	Message Sent and Information Updated
RFID(8A 66 11 B1) Operating System(Off)	Access given	0.83	Message Sent and Information Updated
RFID(2C 57 34 D2) Operating System(On)	Access not given	1.33	Message Sent and Information Updated
RFID(H5 77 33 DD) Operating System(Off)	Access not given	0.95	Message Sent and Information Updated
RFID(5M J4 23 O2) Operating System(On)	Access given	0.92	Message Sent and Information Updated
RFID(G7 80 33 K9) Operating System(Off)	Access given	1.00	Message Sent and Information Updated
RFID(F2 B6 61 I5) Operating System(On)	Access given	0.87	Message Sent and Information Updated
RFID(7C 33 44 T7) Operating System(Off)	Access given	0.59	Message Sent and Information Updated
RFID(9D 46 32 F1) Operating System(On)	Access not given	1.05	Message Sent and Information Updated
RFID(44 BB 49 G4) Operating System(Off)	Access not given	0.90	Message Sent and Information Updated

Table 2
Different RFID-occupied operating system status

RFID tag	Card recognized?	Two-way data transmission speed (Kbit/s)	Data transmission signal response time with IoT (Second)	Operating system (Status)	Vehicular automation status	GSM location info
B1 C7 K5 20	Yes	536	2.38	On	Permission Given	Msg Sent
8A 66 11 B1	Yes	443	1.98	On	Permission Given	Msg Sent
2C 57 34 D2	No	495	1.56	Off	Permission Not Given	Msg Sent
H5 77 33 DD	No	502	2.11	Off	Permission Not Given	Msg Sent
5M J4 23 O2	Yes	460	2.00	On	Permission Given	Msg Sent
G7 80 33 K9	Yes	622	1.88	On	Permission Given	Msg Sent
F2 B6 61 I5	Yes	549	2.34	On	Permission Given	Msg Sent
7C 33 44 T7	Yes	645	2.20	On	Permission Given	Msg Sent
9D 46 32 F1	No	572	1.67	Off	Permission Not Given	Msg Sent
44 BB 49 G4	No	490	1.95	Off	Permission Not Given	Msg Sent

RFID-occupied specialized robot's card recognition, two-way data transmission speed, operating system status, and other information analysis are explained in Table 2.

Adopting radio frequency is an alternative method of implementing automated authorization. In this scenario, every individual receives a tag and an ID number that is picked up by a reader. The RFID writes a file with the person's entry time into the parking space's hour when the audience acknowledges their access. The fact that each tag identification is unique makes them appropriate for usage in databases. The wireless identification system ought to capture all personal data, including the user's arrival time and work hours. It should also prevent possession of any unregistered individuals.

4. Result and Analysis

Multiple RFID's response time, reaction time, and data transmission speed analysis criteria are shown in Figure 10 throughout a bar chart.

With the aid of data accumulation and data mining, the method advancement, sensor evaluation, and Matlab data evaluation, this robot is capable of analyzing a variety of parameters, including RFID UID Card connection and data transmission speed analysis, GPS tracking system communication-based data analysis, real-time communication through wireless network system, Channel's real-time data upgrading, and instant location navigation mechanism through Thingspeak software [17]. The RFID-occupied advanced framework-accessed vehicle's cloud storage, live data parameters, and data analysis system are simply accessible to us [18]. Different wireless network-based analytics is explained in the Figure 11.

Operational system without human interface and final output of our recent going over for Specialized Vehicle Access, Operating System, and Wireless Data Transmission without Human Intervention is shown in the Figure 12, step by step in section Figures 12 and 13.

Figure 10
Response and reaction time, data transmission speed analysis

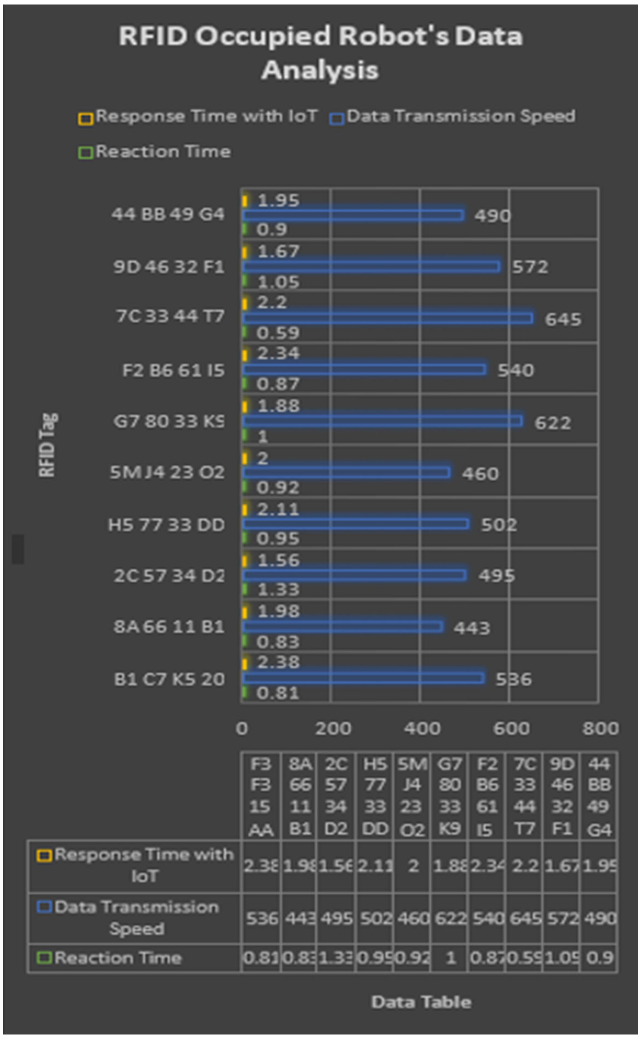
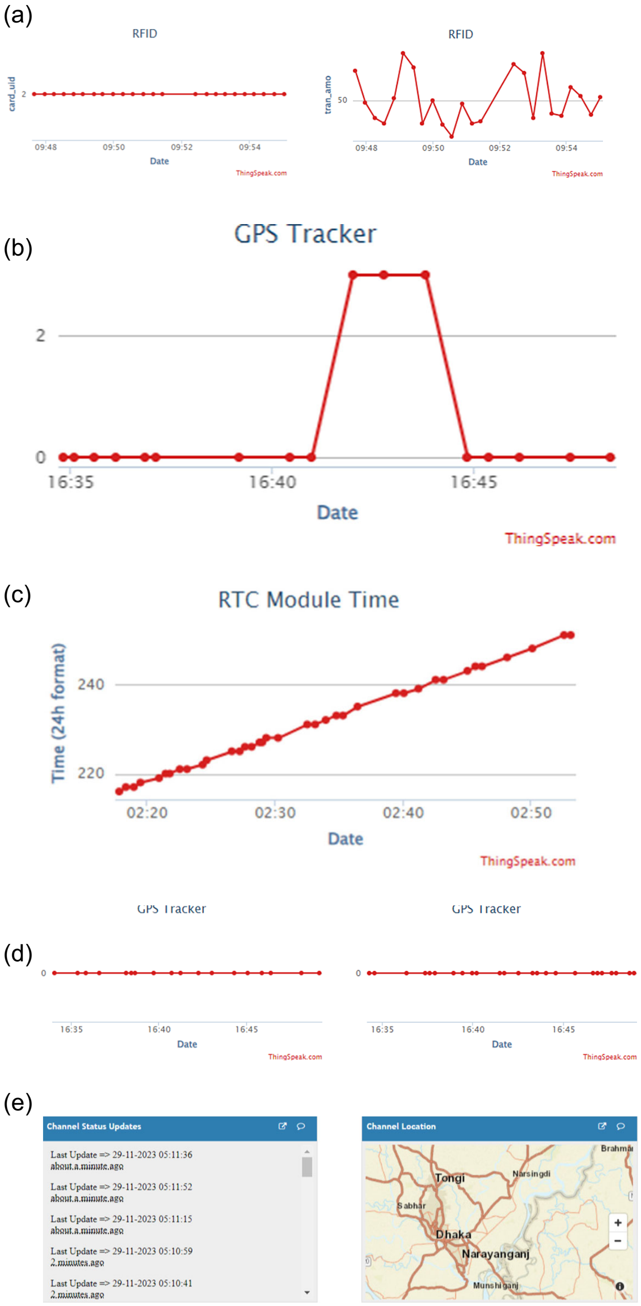


Figure 11
RFID and wireless network-based data analytics and informatics. (a) RFID UID card connection and data transmission speed analysis. (b) GPS tracking system communication-based data analysis. (c) Real-time communication (RTC) through wireless network system. (d) Channel's real-time data upgrading. (e) Instant location navigation mechanism through Thingspeak software



Channel Status Updates

Last Update => 29-11-2023 05:11:36
about.a.minute.ago

Last Update => 29-11-2023 05:11:52
about.a.minute.ago

Last Update => 29-11-2023 05:11:15
about.a.minute.ago

Last Update => 29-11-2023 05:10:59
2.minutes.ago

Last Update => 29-11-2023 05:10:41
2.minutes.ago

Figure 12
RFID-occupied vehicle's operational system. (a) RFID authentication. (b) Vehicle access. (c) Wireless communication (IoT). (d) Specialized operating system

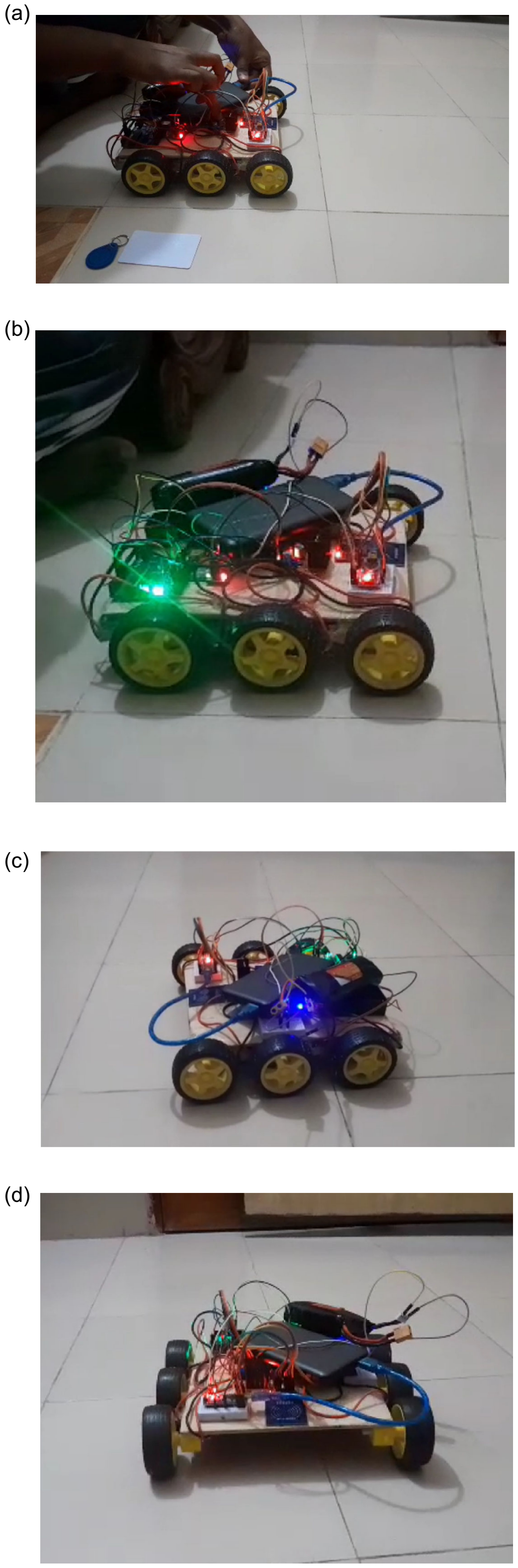
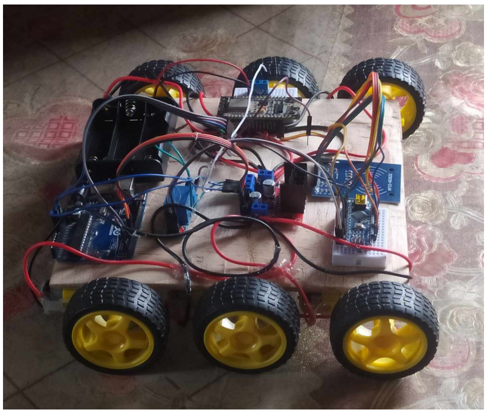


Figure 13
Final output of our RFID-occupied specialized vehicle



5. Conclusion and Future Work

This robot's automation system gives its owners a comfortable, intelligent, secure, and superior living environment. You might be able to lower your power costs by utilizing this ingenious technology. Our research is going on with the utilization of the world wide web of Things concept to facilitate virtual supervision of the constructed solution. This would enable consumers to manage the system's operations regardless of whether they are not present at their usual location of business by using the computing device of an internet site. To enhance the security and privacy through RFID-occupied system, we'll expand the kind and quantity of sensors that are available and provide a completely automated algorithm as an alternative [19]. To prevent cabling problems, we may replace several of these wired detectors using wireless varieties and create an interface to connect all of the instruments to a network for IoT. This technology can be utilized in inventory management, vehicle access, surveillance and security purposes, healthcare management, digital shopping, military authentication, and multiple identification in various sector [20].

Acknowledgement

The completion of this research work would not have been possible without the assistance and effort of our team members. This work was funded by our team members. Finally, we'd like to express our gratitude to everyone for providing their time, support, guidance, and effort to complete this work.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data are available on request from the corresponding author upon reasonable request.

Author Contribution Statement

Abdullah All Mamun Anik: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration. **Mosammat Sadia Akter Moon:** Conceptualization, Software, Validation, Formal analysis, Resources, Writing – review & editing. **Fahim Faysal Arnob:** Conceptualization, Software, Formal analysis, Writing – original draft, Writing – review & editing, Supervision. **Mehedi Hasan:** Conceptualization, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Supervision. **S. A. Naimul Hoque:** Conceptualization, Methodology, Formal analysis, Investigation, Resources, Data curation, Visualization, Supervision. **Mohammad Mashhunur Rahman:** Methodology, Software, Validation, Formal analysis, Investigation, Resources, Visualization, Supervision, Project administration. **Tanzim Bin Ahmed:** Methodology, Software, Validation, Formal analysis, Data curation, Writing – review & editing, Visualization, Project administration. **Tonmoy Barua:** Conceptualization, Software, Formal analysis, Investigation, Resources, Writing – original draft, Visualization, Project administration.

References

[1] Vamshi, B., Ajay, K., Shivani, K., & Badashah, S. J. (2023). RFID based vehicle entry system. *International Journal for Research in Applied Science & Engineering Technology*, *11*(1), 1466–1471. https://doi.org/10.22214/ijraset.2023.48809

[2] Javaid, O., Yu, F. R., & Huang, J. S. (2021). Autonomous vehicle navigation and communication by passive radio frequency (RFID) tags. In *The 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications,* 53–56. https://doi.org/10.1145/3479243.3487303

[3] Tzitzis, A., Megalou, S., Siachalou, S., Emmanouil, T. G., Kehagias, A., Yioultsis, T. V., & Dimitriou, A. G. (2019). Localization of RFID tags by a moving robot, via phase unwrapping and non-linear optimization. *IEEE Journal of Radio Frequency Identification*, *3*(4), 216–226.

[4] Anik, A. A. M., & Moon, M. S. A. (2023). IoT-driven sophisticated robot leveraging RFID identification. In *Proceedings of the 9th International Conference MMSE 2023*, 730–736.

[5] Anik, A. A. M., Adhikary, S., Habib, I., & Gafur, A. (2021). IoT based mechanized robot: An integrated process involving fulltime multipurpose control, automation and surveillance system. In *IEEE International Conference on Service Operations and Logistics, and Informatics*, 1–6.

[6] Magnago, V., Palopoli, L., Buffi, A., Tellini, B., Motroni, A., Nepa, P., . . . , & Fontanelli, D. (2020). Ranging-free UHF-RFID robot positioning through phase measurements of passive tags. *IEEE Transactions on Instrumentation and Measurement*, *69*(5), 2408–2418.

[7] Samuel, A. J., & Sebastian, S. (2019). An algorithm for IoT based vehicle verification system using RFID. *International Journal of Electrical and Computer Engineering*, *9*(5), 3751–3758.

[8] Sali, G. P., Deshmukh, M. J., Wankhede, M. S., & Patra, B. B. (2020). Smart IoT automation for advanced home security. *International Journal of Engineering Research in Electrical and Electronic Engineering*, *6*(4), 2395–2717.

[9] Poberznik, A., Leino, M., Huhtasalo, J., Jyräkoski, T., Valo, P., Lehtinen, T., . . . , & Virkki, J. (2021). Mobile robots and RFID technology-based smart care environment for minimizing risks related to employee turnover during pandemics. *Sustainability*, *13*(22), 12809. https://doi.org/10.3390/su132212809

[10] Mehmood, A., He, H., Chen, X., Vianto, A., Buruk, O., & Virkki, J. (2020). ClothFace: Battery-free user interface solution embedded into clothing and everyday surroundings. In *IEEE 8th International Conference on Serious Games and Applications for Health,* 1–5.

[11] Pavithra, N., Manasa, C. M., Preethi, & Sapna, R. (2022). Smart vehicle document verification system using IoT. In *IEEE International Conference on Data Science and Information System,* 1–5. https://doi.org/10.1109/ICDSIS55133.2022.9915875

[12] Chen, X., Liu, J., Wang, X., Liu, H., Jiang, D., & Chen, L. (2020). Eingerprint: Robust energy-related fingerprinting for passive RFID tags. In *17th USENIX Symposium on Networked Systems Design and Implementation,* 1101–1113.

[13] Li, C., Mo, L., & Zhang, D. (2019). Review on UHF RFID localization methods. *IEEE Journal of Radio Frequency Identification*, *3*(4), 205–215.

[14] Raptopoulos, A., Yioultsis, T., & Dimitriou, A. G. (2019). Particle filter object tracking by a handheld UHF RFID reader. In *IEEE International Conference on RFID Technology and Applications,* 342–347.

[15] Hasler, T., Wölbitsch, M., Goller, M., & Walk, S. (2020). Relative tag locations based on time-differences in read events for practical applications. *IEEE Journal of Radio Frequency Identification*, *4*(1), 55–64.

[16] Cao, S., Liu, W., Cao, L., He, X., & Ji, Z. (2019). An improved authentication protocol using smart cards for the internet of things. *IEEE Access*, *7*, 157284–157292. https://doi.org/10.1109/ACCESS.2019.2949649

[17] Pavithra, N., & Manasa, C. M. (2021). Big data analytics tools: A comparative study. In *IEEE International Conference on Computation System and Information Technology for Sustainable Solutions,* 1–6. https://doi.org/10.1109/CSITSS54238.2021.9683711

[18] Bae, W., & Kwak, J. (2020). Smart card-based secure authentication protocol in multi-server IoT environment. *Multimedia Tools and Applications*, *79*, 15793–15811. https://doi.org/10.1007/s11042-017-5548-2

[19] Vijayalakshmi, N., Kiruthiga, S., Hariprasath, A. P., Arunachalam, K., & Deepak Raja K. K. (2020). Automotive authentication using IoT. In *6th International Conference on Advanced Computing and Communication Systems,* 820–823. https://doi.org/10.1109/ICACCS48705.2020.9074214

[20] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access*, *7*, 82721–82743.

How to Cite: Anik, A. A. M., Moon, M. S. A., Arnob, F. F., Hasan, M., Hoque, S. A. N., Rahman, M. M., . . . , & Barua, T. (2025). RFID Occupied Advanced Framework for Specialized Vehicle Access, Operating System, and Wireless Data Transmission Without Human Intervention. *Archives of Advanced Engineering Science, 3*(3), 214–225. https://doi.org/10.47852/bonviewAAES42023179