IOT BASED SECURED VEHICLE IGNITION CONTROL

Dr. Sunitha Tappari[1], P.V.LK.S.S.Yasaswini[2], M.Swathi[3], Duggi Akhila[4], K.Ananya[5]

[1]Assistant Prof,. Electronics and Telematics Engineering, GNITS, Hyderabad, Telangana, India

[2] B.Tech Student, Electronics and Telematics Engineering, GNITS, Hyderabad, Telangana, India

[3] B.Tech Student, Electronics and Telematics Engineering, GNITS, Hyderabad, Telangana, India

[4] B.Tech Student, Electronics and Telematics Engineering, GNITS, Hyderabad, Telangana, India

[5] B.Tech Student, Electronics and Telematics Engineering, GNITS, Hyderabad, Telangana, India

Abstract- Urban areas have a continual growth trend in vehicle theft, which has created a need for additionallayers of security than that offered by traditional anti-theft systems that typically do not use real-time monitoring nor multi-factor authentication. The proposed system will require the user to enter expandthe password to begin the vehicle. With such a multi- layered approach, this system aims to prevent unauthorized access from starting the vehicle. In case of unauthorized access attempts, the system will indicate these attempts with an audible buzzer alarm and send real-time alerts via connected devices from potential unauthorized access attempts. Moreover, when employing cheap hardware components and wireless communication, the design considers trustworthiness, affordability, and usability aspects ofthe system to present a method that will help prevent vehicle theft as well as ethically increase vehicle security and safety. This system improves vehicle security using an ESP32 microcontroller with securedWi-Fi connectivity, a 4x4-key matrix keypad for user ID and password entry.

Keywords: IoT, vehicle security, ESP32, multi- factor authentication, Wi-Fi, vehicle ignition, real-time monitoring.

I. INTRODUCTION

Vehicle theft is an ongoing problem that traditional security methods such as mechanical locks and alarms are incapable of solving [1]. As criminals employ new and sophisticated tactics, traditional methods become outdated. Fortunately, the Internet of Things (IoT) has opened greater possibilities for enhancing vehicle security with real-time monitoring and control at the vehicle level[2]. This research proposes a smart vehicle ignition control system to increase vehicle ignition security and reduce the risk of vehicle theft by combining IoT technologies and multi-layered user access authentication. The ignition control utilizes an ESP32 microcontroller to control ignition through multiple layers of authentication that includes secure Wi-Fi access to a web-based interface, the user ID reference access via the web interface for authentication, and the 4x4 matrix keypad used to provide correct and unique passwords [3]. This presents an authentication method that complicates unauthorized access to vehicles while providing real-time monitoring and notifications based on unauthorized user activations to the vehicle ignition usage; thereby providing real-time notification to vehicle owners in compromised situations [4].

II. LITERATURE SURVEY

M. Pathak, K.N.Mishra, S.P.Singh,A.Mishra developed a centralized vehicle security system [5] that uses IoT and facial recognition. Theirsystem is complex but requires expensive hardwaresuch as facial recognition cameras and key-cardentry systems. Conversely, the proposed system is developed to utilize cost-effective components, suchas the ESP32 microcontroller and 4x4 matrix keypads. The system utilizes Wi-Fi based authentication, along with user ID and password protection, to provide the same level of security.

Arwa M. Ali, Heisus M. Awad and Ibrahim K.Abdalgader constructed a vehicle access system utilizing RFID and fingerprint scanning technology [6], issuing an SMS alert in response to any unauthorized vehicle access. Their approach adds complexity and expense to hardware requirements. The proposed system streamlines this, using multi- layered security, reliance on Wi-Fi connection, and user verification, eliminating some of the cost of required RFID and biometric sensors.

Mithileysh Sathiyanarayan, Santosh Mahendra and Rajesh Babu Vasu designed a smart vehicle system utilizing remote access, GPS tracking, and GSM technology [7]. Their method emphasizes control via remote access, while theproposed system has been developed using local multi-factor authentication with no need for externalcommunication networks. Thus, by eliminating network communication, the proposed system is lessvulnerable to GSM hacking or remote threats.

Fathima Jabeen, Sudhir Rao Rupanagudi and Varsha G Bhat developed a solution aimed at safety for motor vehicle drivers highlighting alcohol detection and distress notifications [8]. This solution addresses important safety factors, but the mainfocus is on securing the motor vehicle against unauthorized access and theft using Wi-Fiauthentication and password verification. The proposed system protects against theft but is a simpler solution.

Yassine Sabri, Siham Aouad and Abderrahim MaiZate developed an IoT-based motorvehicle safety solution focusing on pre-accident scenarios and post-accident response [9]. Although it aims to successfully improve vehicle driver safety, it does not focus on unauthorized access to motor vehicles. The proposed is uniquely different as it will focus on theft prevention through multi-factor authentication allowing peace of mind to the vehicleowner with alerts of any breaches while being simple to use.

Debajyoti Mukhopadhyay, Megha Guptha proposed an IoT-enabled security prototype using GSM and Bluetooth technologies [10] to provide control over vehicle ignition and other services suchas intrusion detection. However, Bluetooth and GSM systems are more vulnerable to attacks and require consistently connected network services. In proposed system using local Wi-Fi networks improves the security and reliability of the system without external device reliance making it less prone to net-work-related vulnerabilities.

Tuyisenge Jean Claude proposed a vehicle ignition system [11] which is controlled over a smartphone application. Their system allows remote controllability but would be vulnerable to app bugs or connectivity issues from the network. The proposed system is completely keypad based and prepares for these potential consequences, using thisinput methodology as a form of multipleauthenticating layers to ensure a safe local ignition system with no external application capability.

III. PROPOSED SYSTEM

The proposed system seeks to improve vehicle security through an IoT-enabled ignitioncontrol concept. The integrated hardware andsoftware together form the basis of an authenticationsystem, which can admit only authorized users to use the vehicle. Therefore, the system is built off an ESP32 microcontroller that handles Wi-Fi communication, user input, and management of the vehicle's ignition system.

The block diagram shows the overall system architecture where the ESP32 microcontroller will accept inputs from both thekeypad and the web interface, turning on the ignition through a relay module. The system alsoincorporates other feedback mechanisms, such as a buzzer and a few LEDs, to provide visual and auditory warning signals during unauthorized accessattempts.

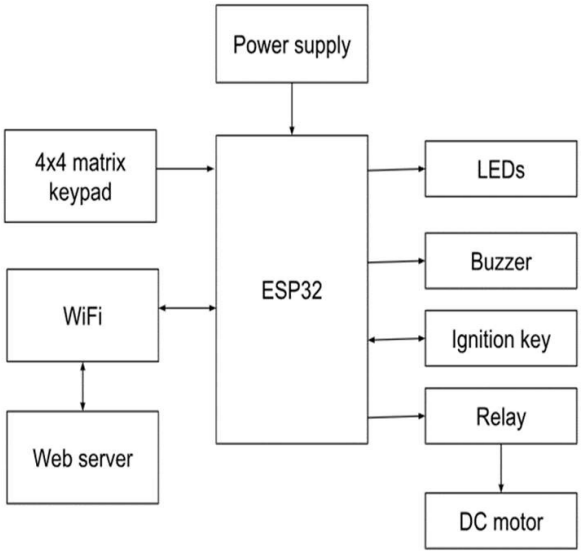


Fig-1 Block diagram of vehicle ignition controlsystem

- **HARDWARE COMPONENTS:**

1. ESP32 Microcontroller: Serves as the main controller for Wi-Fi communication, user input, and ignition control with added Wi-Fi communication capabilities that ensurea secure connection.

2. 4x4 Matrix Keypad: Enables the user to enter a password (code) for verification and then sends that code to the ESP32 and conveys that code to the ESP32 for verification.

3. Relay Module: Responsible for controlling the ignition circuit, allowing the vehicle to start as long as the user has entered the correctpassword.

4. DC Motor: Represents the functioning vehicle engine and indicates whether sufficient efforts are made to start the engine,as long as the password is verified to be correct.

5. Push Button: A simple switch to reset thesystem, or knowingly start the reconfigured code.

6. Buzzer: Sounds and alarm in the event of an unauthorized access attempt, thereby alerting the owner.

7. LED Indicators: Provide the user with feedback on the status of the system, for example, successful authentication, or alarm sounds.

- **SOFTWARE COMPONENTS:**

1. **Programming (C/C++):** The ESP32 is programmed in C/C++ using the Arduino IDE, preferably using the ESP-IDF, to control various aspects including communication, authentication, andignition.

2. **Web Interface (HTML, CSS, JavaScript):** Provides a user-friendly interface for remote access, which allows the user to enter credentials for verification of access, and confirmation of input via smartphone or computer, to monitor thevehicle's access.

3. **Wi-Fi Communication:** Establishes a secure, wireless communication link between a user's device and the vehicle, enabling access control to the vehicle without using the vehicle key.

IV. WORKING PRINCIPLE

The flow chart represents the processof the system. An outline of the processes starting from user identification to controllingthe vehicle's ignition is demonstrated in the flow chart.

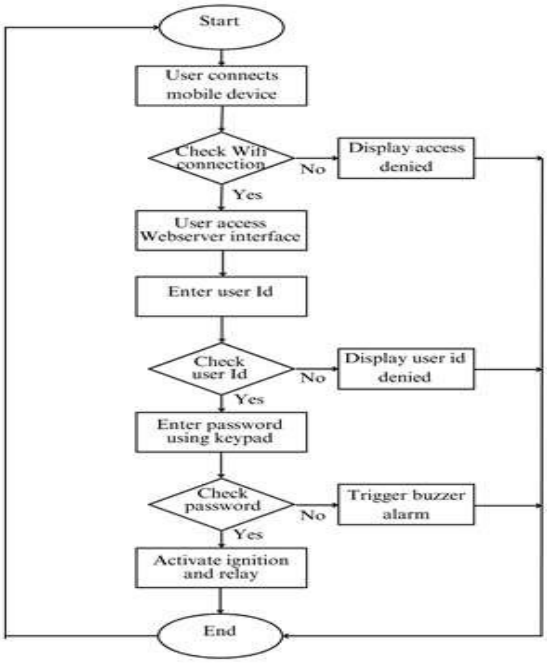


Fig-2 Flow Diagram

1. Connection Setup:

- The process begins with the user connecting a mobile device to the vehicle's local Wi-Finetwork.
- If the Wi-Fi connection is unsuccessful, access isdenied, and no further action is taken.

2. Web Server Access:

- After connecting to the Wi-Fi, the user interacts with a web server interface hosted on the vehicle's ESP32 microcontroller. This interface contains a login page where users input their credentials.

3. Authentication:

- The user enters a user ID on the web interface. If the user ID entered is valid and matches the storeddata, the process continues. If not, an "ID denied"message is displayed.
- Upon successful user ID verification, the user is prompted to enter a password via a keypad on theweb app.

4. Password Verification:

- The entered password is checked against the stored data. If the password is correct, the vehicle’s ignition is activated.
- If the password is incorrect, a buzzer is triggered,signalling an unauthorized access attempt, andalerts may be sent to connected devices.

5. Ignition Activation:

- Once both the user ID and password are verified successfully, the system activates the vehicle'signition and relay.

6. Security and Monitoring:

- **Encryption & Storage**: All sensitive data, such as user IDs and passwords, are encrypted and securely stored within the microcontroller to prevent unauthorized access.
- **Monitoring**: The system logs every login attempt, both successful and failed, to help detect unauthorized access attempts.
- **Fail-Safe Mechanisms**: In the event of any security breaches or failed checks, the systemensures that the vehicle cannot be started until theissue is resolved.

7. Alarm and Error Handling:

- If an unauthorized login attempt occurs, a buzzer immediately sounds to alert the owner of a potential breach.
- The system includes error handling to manage network issues or incorrect inputs, maintaining security until the issue is resolved.

➢ **Web Server Features:**

- **Login Page**: Only accessible via the vehicle's Wi- Fi network, this page prompts the user to input their credentials.
- **Keypad Interface**: The web app features a virtual keypad to enter the password, adding another layer of security.
- **Alerts**: Real-time alerts notify the user of any unauthorized access attempts, enhancing securityfurther.

➢ **Security Configuration:** The ESP32 microcontroller is initiated to create a secure Wi-Fi network with a predefined password. It also runs a web server with several endpoints, including login, status, and shutdown pages.

V. RESULTS AND DISCUSSIONS

➢ **User Authentication Interface:**

The system employs a strong login interface to verify that a user who uses the application can start the vehicle ignition only after being authenticated. The following login window (Fig-3) will prompt the user to enter their User ID. If the user enters a valid credential, the user will be authenticated as a valid user and redirected to the vehicle control page after a successful log in. Otherwise, the system will throw an error message and offer the user a chance to retry log in (Fig-6).

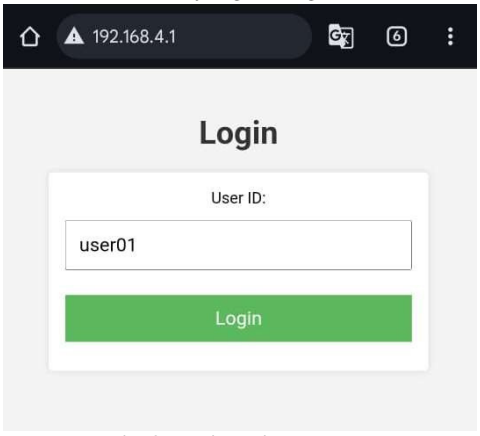


Fig-3 Login Window

➢ **Vehicle Status – Stopped and Running:**

The Vehicle Status page shows the current status of the vehicle after being authenticated. As

shown in Fig-4, the vehicle has stopped, and the usermust enter a password to start the vehicle. Thisserves as a security measure against unauthorized users starting the vehicle.

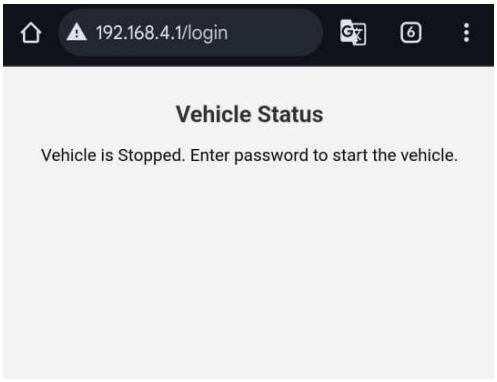
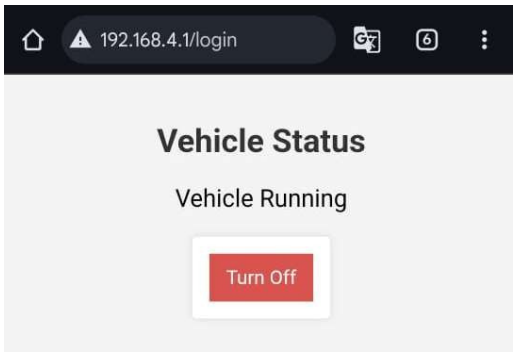


Fig-4 Vehicle status (when vehicle is to bestarted)

As an alternative, when the automobile is moving, as demonstrated in Fig-5, the user may click on the "Turn Off" button to power down the vehicle.



Fig–5 Vehicle status (when vehicle is to beturned off)

If the User ID provided while logging into the portal is invalid, the system will respond with a "Login Failed" message, as shown in Fig-6, and the user will be instructed to attempt logging in again.

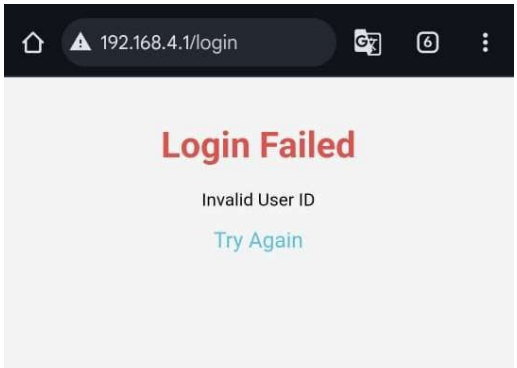


Fig-6 Invalid user id or password onwebpage

- **System Overview:**

The system utilizes a multi-layered vehicle ignition security system. Here is apicture showing

the hardware system, which includes important parts - ESP32 controller, keypad, relay module, speaker, and LED. Allthese parts work hand in hand to implement secure and controlled vehicle access.

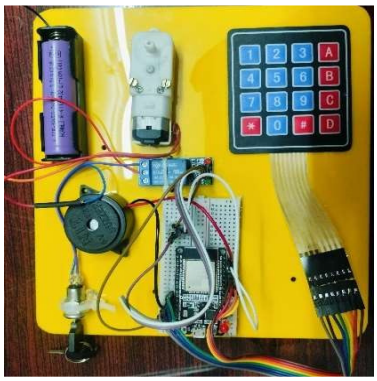


Fig-7 IOT based secured vehicle ignitioncontrol kit

VI. CONCLUSION AND FUTURE SCOPE

This system represents a dramatic advancement in automobile security. It incorporatesan ESP32 microcontroller whose securityobligations include secure Wi-Fi user authentication, user ID verification and obtaining a user password through a 4x4 matrix keypad. The resulting system can, to some degree, diminish security vulnerabilities. It is supplemented by other components like, the relay module, DC motor, buzzer, and LEDs, to provide a layered system. At any time, the system is in an alarm state it will provide alerts in real time to mobile devices connected to it through the app. An integrated smartphone app also allows further options for usersthrough their smartphones. It improves security efficiency and monitoring, thereby demonstrating the possibility of advanced tech features. It is an IoTmodel of a security system that combats issues withautomobile security in today's environment with thebenefits of reliability, efficiency, and ease of use andexcludes the capabilities of what it could do the future.

VII. REFERENCES

[1] Syed fasiuddin, Amena Tamkeen, KhanSohelrana and Mohammed Abdul Rasheed, "Real Time Application of Vehicle Anti-Theft Detection and Protection with Shock Using Facial Recognitionand IoT Notification", Fourth International Conference on Computing Methodologies and Communication ICCMC 2020.

[2] Dhruvi K. Zala, "Bike Security with Theft Prevention", International Conference on Inventive Computation Technologies (ICICT-2018).

[3] Iconic Research and Engineering Journals,Volume 1 Issue 8

[4] International Journal of RecentTechnology and Engineering (IJRTE) Volume-8, Issue-2S11, September 2019

[5] M. Pathak, K. N. Mishra, S. P. Singh and

A. Mishra, "An Automated Smart Centralised Vehicle Security System for Controlling the Vehicle Thefts/Hacking Using IOT and Facial Recognition," 2023 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE),

Dubai, United Arab Emirates, 2023

[6] Arwa M. Ali ,Heisus M. Awad ,Ibrahim K.Abdalgader ,"Authenticated Access Control for Vehicle Ignition System by Driver Licence and Fingerprint Tech", IEEE International Conference on Computer, Control, Electrical and Electronics Engineering (ICCCEEE), pp.26-02,2021

[7] Mithileysh Sathiyanarayan, Santosh Mahendra, Rajesh Babu Vasu, "smart security system for

vehicles using iotSmart Security Systemfor vehicles using iot", IEEE Conference onInternational Conference on Green Computing and iot(ICGCIoT), pp.16-18,2018

[8] Fathima Jabeen, Sudhir Rao Rupanagudi and Varsha G Bhat, "IOT based Smart Vehicle Ignition and Monitoring System", IEEE International Conference on Advances in Computing, Communication and Control (ICAC3), 20-21 ,2019

[9] Yassine Sabri, Siham Aouad and Abderrahim MaiZate, "IOT based Smart vehicle Security and Safety System", IEEE InternationalConference on Advanced CS Applications, pp.22- 04 ,2022

[10] Debajyoti Mukhopadhyay, Megha Guptha, "An Attempt to develop an IOT based Vehicle Security System", IEEE International Conference on Symposium on Smart Electronic Systms (iSES),pp.20-12,2018

[11] Tuyisenge Jean Claude, Ishimwe Viviane "Development of Security Starting System for Vehicles based on IoT", IEEE International Conference on Information Technology (ICIT), pp.14-15,2021---11

[12] Ahmed A. Elngar and Mohammed Kayed, "Vehicle Security Systems using Face Recognition based on Internet of Things", Open Com Sc. J., vol.10, pp. 17-29, 2020

[13] W. Lim et al., "Automotive Start-Stop Engine Based on Face Recognition System", E3S Web of Conferences, vol. 130, pp. 1-15, 2019

[14] Ankit Raj et al., "IOT Based Driver Authorization Vehicle Security System and Accident Detection and Vehicle Tracking using Android App", JETIR, vol. 6, no. 6, pp. 267-271, 2019

[15] D. Mukhopadhyay, M. Gupta, T. Attar, P. Chavan and V. Patel, "An Attempt to Develop an IOT Based Vehicle Security System," 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), Hyderabad, India,2018, pp. 195-198

[16] Abdurrahman A. Nasr et al., "A survey of IoT security threats and defences", Int. J. of Adv Comp Research, vol. 15, pp. 325-350, 2019

[17] M. Sanket et al., "Anti-Theft Alert Systemfor Smart Vehicles", IJRASET, vol. 10, no. 7, pp. 562-568, 2022

[18] R. Samir et al., "Anti-Theft SecuritySystems for Vehicles", Int J of Engg & Tech, vol. 7,no. 4, pp. 42-46, 2018