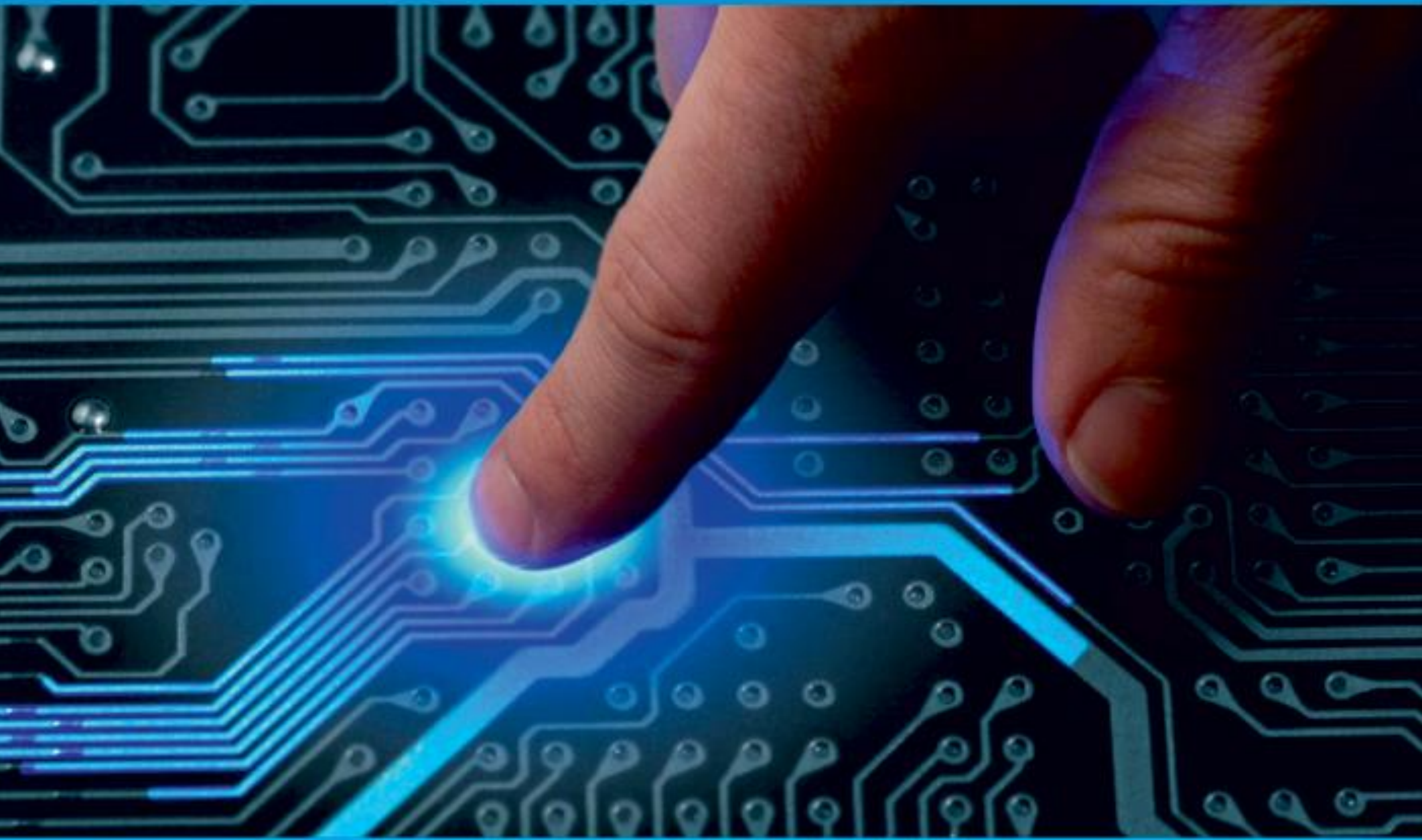
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| DOI: 10.15680/IJIRCCE.2024.1204073 |

Biometric Drive Guard Securing Vehicles with Facial and Fingerprint Recognition

Yashaswini M[1], Ashwini A V[2], Sahana P[3], Akash M P[4], Dr. Hemashree[5]

Student, Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India [1234]

Assistant Professor, Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India[4]

ABSTRACT: From the past years, the Vehicle theft has been increased double the time. The effort has been truly interdisciplinary, where, vehicle authentication system implementation have played their roles. The latest technology innovations have enabled the researchers to execute computational experiments which would had never been possible if would have tried using the traditional methods. This survey paper provides study of various methodologies for Vehicle authentication. This paper provides systematic analysis of various existing vehicle authentication techniques with precise and arranged representation. We have backed up the study with the merits and demerits of existing methods and the future scope in this area**.**

KEYWORDS: Fingerprint module; RFID; GSM techniques; face recognition module; LCD display; Security Alertness; Arduino uno; MQ3

I. INTRODUCTION

In this new era, car theft is increasing at an alarming rate all over the world. Vehicle safety and security is one of the most important aspect over the years. Cars parked on city streets, in dark and quiet areas, can be targets for thieves. And maximum number of road accidents cases reported in India are caused by drink driving. Some people in India still cannot reach hospitals and other medical facilities, hence there a need for device that provide an alert message to the nearest hospital when an accident has occurred.

A smart automobile is one that has a number of sensors that assist the driver in analyzing driving circumstances such as topography, weather, and engine temperature. Aside from that, automobiles feature buttons for starting the vehicle, controlling the power windows. AI and ML have had its impact on vehicles too making them smart. Smart automobiles are no longer considered a luxury item, but rather a necessity. Because of the intense rivalry among automotive manufacturers, adding new features to each edition of their vehicles has become the "success mantra." As a result, numerous businesses and colleges throughout the world are working around the clock to bring new characteristics. Enhancing the vehicle's security is one such feature that has received the most attention. Driving has now become a necessity for everyone. It is also very important to protect your car against theft. Simultaneously, protecting the vehicle against theft is also very important.

II. REVIEW OF LITERATURE

As a part of this survey review, almost 50 papers were downloaded in order to present a systematic technical analysis of the vehicle authentication techniques from various digital libraries, which include IEEE Xplore and many more. After studying the paper title, abstract, introduction, experiment and future scope, 16 most suitable paper for the review have been identified, In this part of the article, analysis and planning work is done.

The literature review discusses about previous attempts made in the field of research and development of vehicle authentication and usage of various technology. The discussion on literature survey includes significant contributions made by different scholars in this discipline.

In this work, authors have tried to address the problem in vehicle security system. Authors have used multiple library functions and features of models to design and develop a model for vehicle authentication. The system uses Global

System for Mobile (GSM) technology. The microcontroller receives a program containing the logic needed to control the vehicle's engine. The security system includes fingerprint scanner, LCD, GSM modem, driver, buzzer and other related features[1].

In this project, author used both hardware and the software, instead of using the traditional method to start the car, a new method is used to start the car. The owner's finger can start the car. Use a 16-bit AVR chip, which is a 40pin chip. A GSM module is also used, It also uses an LCD screen to display the status of the added, deleted or completed finger. Microcontroller programmer or microcontroller programmer is another piece of hardware but it is not included in the project module. Its sole purpose is to burn the program we wrote in the protein onto the chip[2].

In this paper, authors have proposed an approach to address the challenges posed by traditional vehicle security system. In this paper, author used GSM and GPS technology for tracking and monitoring the vehicle. Author used Arduino microcontroller and GSM modules Ensure security by incorporating biometrics (e.g. fingerprints). The design has a combination of fingerprint recognition module and authentication function [3].

In this paper, authors have designed a vehicle authentication technique for vehicle authentication and have worked upon reducing the error ratios. The results, which were compared with vehicle authentication vendor tests, were found to be better. In this article, the author announced a system with a smart card (driving license) that can collect fingerprints of a specific person, then it goes for alcohol detection and seatbelt checking. After passing all authentications, the vehicle will be lighted [4].

This study investigates cyber-attacks and security mechanisms for connected and autonomous vehicles (CAVs) to ensure their smooth operations and secure communication with support systems like Fog Computing (FC) and Cloud Computing (CC). CAVs, which are expected to transform the automotive landscape and provide a highly connected infrastructure for smart transportation, require a thorough examination for widespread acceptance. The ponder proposes a reference design for a CAVs environment to infer a common assault scientific classification for examining existing and developing cyber dangers. The security instruments for the CAVs biological system are talked about, based on comprehensive ponders of scholarly writing and industry white papers. The think about gives profitable experiences to security engineers and framework planners for examining security issues employing a top to bottom approach and helps in envisioning strong security arrangements to guarantee consistent CAVs operations. The consider too highlights the significance of a secure and solid biological system for CAVs, which can be accomplished through a rearranged three tier topology: CAVs as Edge gadgets, RSUs as Mist, and cloud computing as the spine [5].

The International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE) has published a study on a vehicle security system using biometric fingerprint recognition technology, GPS, and GSM systems. The system aims to provide high security to vehicles, allowing only authenticated users and utilizing fingerprint reorganization technology. The prototype model is built on an embedded platform using an ARM microcontroller, which controls all operations. The system also includes a metal sensor for detecting duplicated keys and sending SMS alerts to the owner. The fingerprint recognition system is provided at the engine ignition, and GPS technology makes vehicle tracking easy. The system is designed to be user-friendly, fast access, and fingerprint reorganization technology. The system is designed to be cost-effective and enhances security. The system also includes a fuel sensor for fuel theft and a metal sensor for key detection. The system is designed to be user-friendly, fast access, and cost-effective[6].

The International Journal of Industry and Sustainable Development (IJISD) has published a study on the design and implementation of an Integrated Vehicle Security System (IVSS). The study aims to enhance vehicle security by incorporating various applications to increase safety. The system includes a fingerprint sensor for door security, face recognition for ignition, and a driver alcohol detection system to prevent drunk driving and accidents. The system is connected to a GSM module for communication in case of recognition failure, and a GPS module for live vehicle location in case of theft. The study highlights the importance of identifying individuals to prevent property theft, particularly vehicle theft. The system uses an embedded system based on fingerprint sensors, face recognition cameras, and GSM technology, with an interfacing mobile connected to the microcontroller. The fingerprint sensor allows the door to open if the user matches the stored ID in the memory. Face recognition ensures the car engine starts if the user matches the stored ID[7].

This article discusses vehicle security that combines fingerprint recognition and RFID technology to prevent theft. The system uses GSM and GPS technology to track vehicles, allowing users to access vehicles via fingerprint and RFID modules. The system also uses smartphones to send and receive messages to vehicle owners, allowing them to track their vehicles and send real-time tracking information to vehicle owners via text message. The system also provides engine immobilization and alarm functions and allows users to control the vehicle remotely. GPS-GSM based tracking uses Google Maps as a tracking system to track the vehicle's location and send information when necessary. The system also uses a fingerprint scanner to detect attempted theft and sends a control signal to stop the engine. The system also uses the GPS-GSM module to send information to the owner's mobile phone in case of a theft attempt. This system aims to increase vehicle safety and reduce theft in developing countries [8].

In this study, the authors use biometrics (physical or human behavior) to protect vehicles from unauthorized or unknown persons. If fingers are crossed, the device can be unlocked, increasing security. In this case, they use a technology called RFID, which stands for "Radio Frequency Identity". Using radio waves, readers can capture digital information encoded in RFID tags. In this case, they use another module called EM18 RFID, which has a built-in antenna and operates on 5 volts. Determines unique 12-bit number from RFID or [9].

This work introduces real-time vehicle security using facial recognition and fingerprint scanners. The system consists of a Raspberry Pi board, USB camera, fingerprint scanner, breathalyzer and motorized relay. When a person enters the vehicle, the system will scan the driver's license using the eigenface algorithm. The camera captures the driver's image and compares it with existing data. If there is a match, the system will proceed with fingerprint verification. The fingerprint module is the key for the vehicle ignition. If the fingerprint matches with the existing dataset, the ignition is turned ON. If the person's face is not matched, the system sends an email alert to the vehicle owner and ring a buzzer. If the person fails in fingerprint verification or alcohol detection, the vehicle ignition is not turned ON. The experimental results show that the accuracy of the proposed vehicle security system is 98.3% at a threshold value of 3.2*10^3 and 3.5*10^3, achieved in different illumination conditions[10].

he increasing number of vehicles stolen and unlicensed drivers is a major concern for manufacturers and owners of luxury automobiles. This paper introduces the vehicle anti-theft system, including Arduino, driver card (DL), RFID reader (RFID), fingerprint (FP) and international mobile communication modem system (GSM).

Arduino acts like the entire brain of the body, allowing the driver's license and fingerprints of trusted people to be added to the program. When someone enters their driver's license into the RFID reader, the current information in the program is compared with the information in the program. If there is a match, the generator will be activated and the person will be able to use the vehicle. Otherwise, a Short Message Service (SMS) will be sent to the vehicle owner via GSM modem and the generator will be blocked. Additionally, SMS is sent to driver's license holders to renew their driver's license before it expires[11].

The research focuses on developing a car start-stop engine based on facial recognition systems. The system uses a camera processed by the system to capture the face in real time. The facial recognition is then input into the Arduino, which is connected to the car relay to start the car's engine. Viola-Jones method is used to capture and crop the faces of the face image while Canny edge method is used to segment the visible face. Fast Fourier transform is used as a video lifting technique to extract facial images, which are then fed into an artificial neural network (ANN) to identify the authorized person. Experimental results show that the training and evaluation accuracy are 100% and 100%, respectively. The proposed system is to prevent burglary and theft in non-motorized vehicles, especially for young drivers [12].

This work presents privacy-privacy Dynamic Authentication Method (DACOP) security for traffic networks using matrix-based signature generation. This approach is ideal for Vehicle-to-Everything (V2X) networks, where messages from the vehicle are signed before being broadcast to ensure authenticity and integrity. The proof-of-concept app also ensures privacy by using the vehicle's fake identity and anonymity. It minimizes the computer load caused by signatures. Experimental results using a real V2X network show that DACOP reduces the calculation time by 90% compared to previous methods and increases the security level by 2 times. This method solves the computational issues and communication costs associated with V2X security protocols by using authentication without the need for further negotiation and message exchange. This research was supported by the Department of Large-Scale Research, the Business Connected IoT Semiconductor System Convergence Incubation Center, and the AURI grant from the Ministry of Small and Medium Enterprises and New

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204073 |

Enterprises [13].

In this study, the authors use the fingerprint technique to reduce car theft and increase the security of the car as a whole. In this case, the connection between the fingerprint sensor and Arduino is used. ARM processor is used to control the engine starting system. They control the car's ignition system using an Arduino UNO with a fingerprint sensor that can recognize a person's fingerprint and check if the person has permission. Here they use a step-up transformer whose output voltage is greater than the input voltage. They provide 230V AC power to this 0-12V transformer. They then use a 16*2 LCD that can display 16 characters per line and has two registers, Command and Data. The fingerprint sensor module captures the image of the finger and then converts it into an equivalent pattern that is stored in memory by the Arduino. In this configuration they use a servo motor, which is an electric motor that controls position and speed. Use two cards: valid card and invalid card. The RFID reader is used to identify valid RFID tags, if it finds valid tags the vehicle is set [14].

This study focuses on the use of fingerprint recognition as a reliable human identification device and offers a security approach for electronic vehicle systems using the device. The project's embedded fingerprint module enters the fingerprint of the owner and all authorized users. The microcontroller that controls the vehicle's connection to the electrical outlet is connected to this module. Fingers need to be aligned correctly to start the car; Otherwise, the vehicle will not start and the letter will be sent to the owner. The concept also includes a GSM module connected to the controller, which can send a message to the real owner of the car in case an unauthorized person tries to open the car using the key [15].

This study presents a safety solution that combines smart bikes and smart helmets to reduce bike theft, drunk driving and accidents. The device uses RFID and FSR sensors to measure the rider's alcohol content and electronic devices to instantly identify motorcyclists. The pressure in the helmet is measured by collecting data. Two-wheelers, bicycles, motorcycles, scooters and skateboards can all use the system. The system also includes a pressure sensor-based system that ignites the engine when a certain level is reached, as well as a system for monitoring ambient pressure. We developed a LabVIEW GUI to display measured pressure as a live bar chart or simulated pressure-time curve. The system is designed to detect the person wearing the helmet and give the first warning [16].

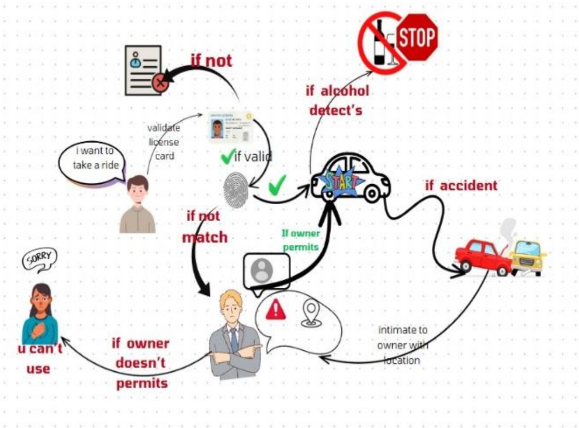


Fig:1 Summary diagram

III. METHODOLOGY

The vehicle authentication system consists of the following key components:

- License Verification Module: Scans the license card using RFID reader for initial authentication.
- Fingerprint Authentication Module: Authenticates authorized users based on stored fingerprint data.
- Face Recognition Module: Identifies authorized individuals through facial recognition.
- Alcohol Detection Sensor (MQ3): Monitors alcohol levels to prevent drunk driving.
- Angular Sensor: Detects accidents and triggers alerts.
- Communication Module: Facilitates communication between the vehicle and the owner's device.

The flow of working is as follow's

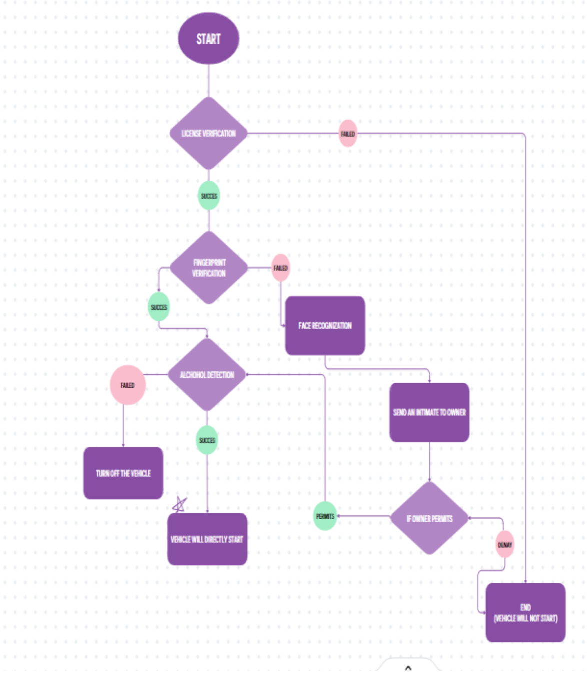


Fig:2 Flow Chart

License Verification: The user scans their license card using an RFID reader. The system validates the license details against a database of valid licenses.
Fingerprint Authentication: Authorized users undergo fingerprint authentication after successful license verification. The system matches the scanned fingerprint with stored biometric data.
Face Recognition: If fingerprint authentication fails or is unavailable, the system proceeds to face recognition. Authorized individuals are identified based on pre-trained facial data.
Alcohol Detection: The system continuously monitors alcohol levels using the MQ3 sensor. If the alcohol level exceeds the defined threshold, the user is denied access and an alert is sent to the owner.
Accident Detection: The angular sensor detects abrupt changes in vehicle orientation indicative of accidents. Upon detection, the system sends immediate alerts to the owner, including the accident location using longitude and latitude coordinates.
Alert Mechanism: In case of unauthorized access attempts or accidents, real-time alerts containing relevant information are sent to the vehicle owner's device.

Working of the components

The integration of various modules within the vehicle authentication system presents a comprehensive approach to ensuring security and safety. At the heart of this system lies the Arduino Uno microcontroller, a versatile component that orchestrates the interactions between different elements. With its ATmega328P microcontroller and extensive array of input/output pins and communication interfaces, the Arduino Uno serves as the central processing unit for the system. Its programming capabilities through the Arduino Integrated Development Environment (IDE) enable seamless integration and control of the system's functionalities.

Module 2 introduces the RFID reader, which utilizes radio waves to communicate with RFID tags or transponders, offering a reliable means of identification and authentication. Meanwhile, Module 3 highlights the use of biometric sensors, which provide a high level of security by authenticating individuals based on unique biological characteristics such as fingerprints or facial features. These sensors eliminate the need for passwords or physical keys, enhancing convenience and reducing the risk of unauthorized access.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204073 |

The Node MCU, as detailed in Module 4, adds connectivity to the system, enabling communication with external devices and services via Wi-Fi. This functionality allows for real-time notifications to be sent to the owner's device in the event of unauthorized access attempts or accidents, enhancing overall security and situational awareness. Additionally, the Node MCU can interface with various sensors, including the MQ3 alcohol sensor and angular sensor, to monitor alcohol levels and detect accidents.

Module 5 introduces the Zigbee sensor, which facilitates wireless communication between system components, ensuring reliable data transmission and scalability. The angular sensor, detailed in Module 6, plays a crucial role in accident detection by monitoring changes in the vehicle's acceleration and orientation. Upon detecting abrupt changes indicative of an accident, the angular sensor triggers the appropriate response within the authentication system.
Module 7 describes the MQ3 sensor, which detects a variety of gases, including alcohol, providing an additional layer of safety by monitoring for potentially hazardous conditions. The LCD display, detailed in Module 8, provides visual feedback to users, enhancing the user interface and overall user experience.

Module 9 introduces the multi-way switch, which allows for easy management of fingerprint data within the system, adding flexibility and convenience to the authentication process. The power supply, as detailed in Module 10, ensures reliable operation of the system by converting AC power into DC power for the various components.

The DC motor, described in Module 11, serves as a demo model to represent a vehicle within the system, showcasing the system's capabilities in a simulated environment. Module 12 highlights the use of sensor relays for managing power distribution and ensuring smooth operation of the system.

Finally, Module 13 introduces the buzzer, which provides audible alerts in case of critical events, further enhancing the system's ability to notify users of potential security breaches or accidents. Overall, the integration of these modules within the vehicle authentication system forms a robust and comprehensive solution for enhancing security and safety in vehicular environments.

IV. CONCLUSSION

In the described vehicle authentication system, a switch relay is used to control the ignition system, manage power distribution, integrate with authentication modules and sensors, and enhance safety features. It ensures authorized access and facilitates seamless operation by triggering the appropriate responses based on authentication results and sensor data. The system employs face and fingerprint detection, alcohol detection, and accident detection mechanisms to authenticate users and detect critical events. Notifications are sent to the owner in case of accidents or unauthorized access attempts, ensuring prompt action. Overall, the switch relay enhances security, reliability, and functionality in the vehicle authentication system.

REFERENCES

[1] Ahmed A. Elnga, & Mohammed Kayed. (2019). Vehicle Security Systems using Face Recognition based on Internet of Things. ResearchGate, 1–11.

[2] Alen Joseph Samuel, & Shoney Sebastian. (2019). An algorithm for IoT based vehicle verification system using RFID. International Journal of Electrical and Computer Engineering (IJECE), 9, 1–8.

[3] CHIEN-MING CHEN, bin XIANG, YINING LIU, & KING-HANG WANG. (2019). A Secure Authentication Protocol for Internet of Vehicles. IEEE Explore, 7, 1–10.

[4] Dalip Kamboj, Vijay Kumar, & Rohit Vaid. (2015). Secure and Authenticated Vehicle Navigation System. IScholar, 8(28), 1–4

[5] Fawzi M., & Al-Naima. (2015). Design of an RFID Vehicle Authentication System. International Journal of Scientific and Technological Research, 1, 0–13.

[6] Huibin Xu, Mengjia Zeng, Wenjun Hu, & Juan Wang. (2019). Authentication-Based Vehicle-to-Vehicle Secure Communication for VANETs. Hindawi, 2019, 1–9.

[7] Jie Zhang, Zhongmin Wang, & QingLi Yan. (2021). Intelligent user identity authentication in vehicle security system based on wireless signals. Springer, 1–15.

[8] Jie Zhang, Zhongmin Wang, & Qingli Yan. (2022). Intelligent user identity authentication in vehicle security system based on wireless signals. SpringerLink, 8, 1243–1257.

[9] Matthew A. Turk, & Alex P. Pentland. (2009). Face Recognition Using Eigenfaces . IEEE Explore, 1–6.

[10] Mr. Somnath A. Karmude, & Prof. G. R. Gidveer. (2014). Vehicular Identification and Authentication System using Zigbee. International Journal of Engineering Research & Technology, 3(11), 1–4.

[11] Muhammad Waqas, Muhammad Waqas, Sadaqat Ur Rehman, Zahid Halim, Sajid Anwar, Ghulam Abbas, Ziaul Haq Abbas, & Obaid Ur Rehman. (2020). Authentication of Vehicles and Road Side Units in Intelligent Transportation System. Techscience, 64, 1–10

[12] PALAK BAGGA, ASHOK KUMAR DAS, MOHAMMAD WAZID, JOEL J. P. C. RODRIGUES, & YOUNGHO PARK. (2020). Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges. IEEE Explore, 8, 1–20.

[13] Prerna Mohit, Ruhul Amin, & G.P Biswas. (2017). Design of authentication protocol for wireless sensor network-based smart vehicular system. ScienceDirect, 9, 1–10.

[14] R Monisha, Jessen Joseph Leo, B T Tharani Sri Sakthi, & A John Clement Sunder. (2016). Car Authentication and Accident Intimation System using GPS and GSM . International Conference on Systems, Science, Control, Communication, Engineering and Technology, 2, 1–6.

[15] Rajeshwar Rao Arabelli, & Keerthana Revuri. (2019). Fingerprint and Raspberri Pi Based Vehicle Authentication and Secured Tracking System. International Journal of Innovative Technology and Exploring Engineering, 8(5), 1–4.

[16] S . Prema, Mohamed Riyas V. S Deen, Murali V. P Krishna, & S .Praveen. (2019). Vehicle And License Authentication Using Finger Print. International Conference on Advanced Computing and Communication System, 1–6.

[17] S. D. Dissanayake, P. P. C. R. Karunasekara, D. D. Lakmanaarachchi, A. J. D. Rathnayaka, & A. T. L. K. Samarasinghe. (2010). Zigbee Wireless Vehicular Identification and Authentication System. IEEE Explore, 1–4.

[18] Sebastian Frank, & Arjan Kuijper. (2017). AuthentiCap - A Touchless Vehicle Authentication and Personalization System. European Conference on Ambient Intelligence, 1–17

[19] T.Anusha, & T. Sivakumar. (2012). VEHICLE IDENTIFICATION AND AUTHENTICATION SYSTEM. INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY, 2(2), 1–5.

[20] XIAOLIANG WANG, PENGJIE ZENG, NICK PATTERSON, FRANK JIANG, & ROBIN DOSS. (2019). An Improved Authentication Scheme for Internet of Vehicles Based on Blockchain Technology. IEEE Access, 7, 1–12

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING