International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
OPEN ACCESS
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST

Biometric-Based Anti-Theft Vehicle Security System with Fingerprint and Face Recognition Embedded in Python

Ms. G N Sandhya Devi[1], B. Rakesh[2], Ch. Naga Gopi[3], Ch. Anusha[4], B. Lakshman Kumar[5]

[1]Assistant professor, Electronics and Communication Department, Seshadri Rao Gudlavalleru Engineering College, India

[2,3,4,5] Electronics and Commination Department, Seshadri Rao Gudlavalleru Engineering College, India

ARTICLEINFO

Article History:

Accepted: 12 April 2024
Published: 22 April 2024

Publication Issue :
Volume 11, Issue 2
March-April-2024
Page Number :
775-784

ABSTRACT

The proposed anti-theft vehicle security system introduces a robust authentication framework to bolster security measures. Through the fusion of fingerprint recognition, facial scanning, and One-Time Password (OTP) verification, the system establishes multiple layers of user authentication. This multi-step process ensures that only authorized individuals can gain access to the vehicle's ignition system. Furthermore, the system integrates advanced features such as real-time location tracking using GPS technology and remote alerts via GSM communication. These functionalities empower vehicle owners with the ability to monitor their vehicle's whereabouts and receive immediate notifications in the event of unauthorized access or suspicious activities.

In addition to its authentication capabilities, the system incorporates surveillance elements to enhance security further. A USB web camera is employed to capture images of the vehicle's surroundings, facilitating potential identification of unauthorized users. The user interface, comprising an LCD display, LEDs, and a buzzer, provides intuitive feedback on authentication status and alerts users to potential security threats. By combining advanced authentication methods with robust surveillance and user feedback mechanisms, the system aims to effectively deter theft and unauthorized access while offering vehicle owners peace of mind and control over their vehicle's security.

Keywords: Biometric, LCD, OTP, Verification, GPS, GSM.

I. INTRODUCTION

The protection of vehicles against theft and unauthorized access has become increasingly paramount in contemporary society. As automotive technology evolves, so do the methods employed by thieves and intruders, necessitating advanced security measures to safeguard vehicles effectively. In response to this pressing need, the proposed anti-theft vehicle security system emerges as a comprehensive solution designed to fortify vehicle security through a multi-layered approach. By integrating cutting-edge authentication techniques such as fingerprint recognition, facial scanning, and One-Time Password (OTP) verification, the system aims to establish stringent barriers against unauthorized access while providing convenience and peace of mind to vehicle owners.

Moreover, the advent of GPS and GSM technologies has revolutionized the landscape of vehicle security, enabling real-time location tracking and remote communication capabilities. Leveraging these advancements, the proposed system not only enhances security but also empowers vehicle owners with unprecedented levels of control and oversight. With features such as GPS-based location monitoring and GSM-enabled remote alerts, owners can monitor their vehicles' whereabouts and receive instant notifications of any suspicious activities, thereby reinforcing their ability to safeguard their valuable assets. As vehicle theft continues to pose a significant threat, the implementation of advanced security systems like the one proposed herein represents a proactive step towards mitigating risks and ensuring the safety of vehicles and their occupants.

In today's dynamic landscape of automotive security, the need for robust and adaptable anti-theft systems has never been more critical. With the rise of sophisticated theft techniques and the increasing prevalence of vehicle-related crimes, traditional security measures are proving inadequate in deterring determined intruders. The proposed anti-theft vehicle security system stands at the forefront of innovation, offering a holistic approach to security that combines state-of-the-art authentication methods with advanced surveillance and communication technologies. By embracing a multi-layered authentication process that incorporates biometric identification and OTP verification, the system raises the bar for access control, ensuring that only authorized users can operate the vehicle. Furthermore, its integration of GPS tracking and GSM communication capabilities not only enhances security but also empowers owners with real-time monitoring and remote control functionalities, thus ushering in a new era of proactive vehicle protection. As vehicles continue to evolve into sophisticated technological entities, so too must the systems designed to safeguard them, and the proposed security solution exemplifies a forward-thinking approach to addressing the ever-evolving challenges of automotive security.

II. RELATED WORKS

"Biometric and Passcode-Based Anti-Theft Vehicle Security System." by Authors are Mr. Prashanth.S, Mr. Sachin Kumar.BU, Ms. Sahana.CE, and Mrs. Yojana Yadav are affiliated with the Department of Electronics and Communication Engineering at PES Institute of Technology and Management, located in Shivamogga, Karnataka, India.

Said it as Today, vehicle owners face a significant concern regarding the potential theft of their vehicles, whether parked in communal parking areas or outside their residences. To address this issue, a real-time vehicle theft detection and prevention system based on image processing is proposed, offering an effective solution. This paper presents a cost-effective and scalable framework for a smart vehicle security system, comprising a Fingerprint Detection Subsystem (FDS), a GPS module, a GSM module, and a control platform. The FDS verifies the driver's identity by scanning their fingerprint and comparing it with stored data, employing an optimized PCA algorithm for efficient fingerprint recognition within vehicles. The other system modules facilitate continuous monitoring of the vehicle's status and location, even in the event of theft. Implemented on a Microcontroller, the system enables the vehicle owner to remotely stop the vehicle via mobile message. Additionally, the GPS module tracks the vehicle's location, simplifying theft identification and recovery processes compared to conventional methods. Furthermore, a panic button is integrated for passenger safety during emergencies. This system offers a smarter and more economical alternative to traditional security measures.

"Vehicle Security System Utilizing Fingerprint Authentication" Authors Aditi Ramprasad, P Praveen, Chirag Chengappa M D, R Rohini, and S Sujay Kashyap are associated with the Department of Electronics & Instrumentation Engineering at JSS

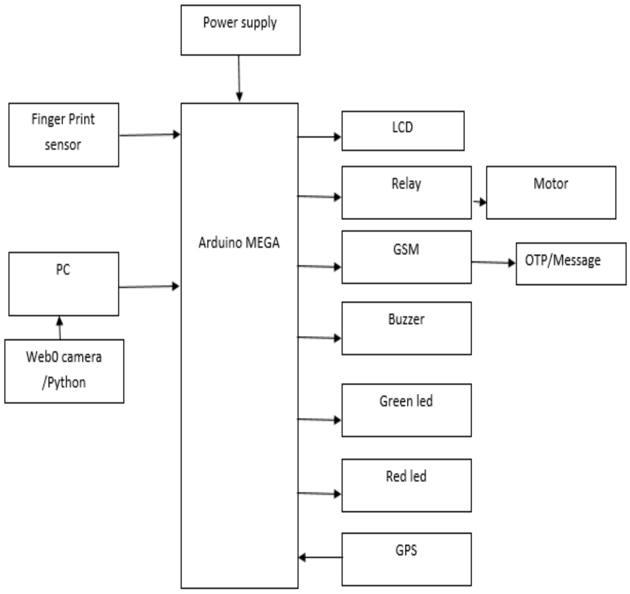
Academy of Technical Education in Bengaluru, India. They can be contacted via email at aditirp2000@gmail.com wrote that India, characterized by a high population density, also witnesses a corresponding increase in automobile numbers. Unfortunately, this surge in automobiles coincides with a rise in vehicle theft incidents. Current security systems exhibit shortcomings, failing to adequately address the concerns of vehicle owners. Particularly in urban areas, where vehicle thefts occur frequently, the issue of vehicle security has become paramount. Experts attribute the uptick in thefts to insufficient parking spaces and a lack of sophisticated security measures. Technological advancements have demonstrated efficacy in combating vehicle theft, emphasizing the importance of adopting appropriate security measures to mitigate these incidents. Thus, anti-theft systems emerge as pivotal tools in curbing vehicle thefts. This article explores various methods of anti-theft vehicle security systems in brief, emphasizing the need for robust security solutions in the face of escalating theft rates.

III. PROPOSED METHOD

The proposed anti-theft vehicle security system integrates various authentication methods to bolster security effectively. Users can verify their identity through either a fingerprint sensor embedded in the ignition key or facial recognition using a camera system. Upon authentication initiation, the system prompts users to provide their biometric data. If successfully matched with stored records, the system proceeds to the next step, where a One-Time Password (OTP) is sent to the user's registered mobile device via GSM communication. Upon OTP validation, authorized users gain access to the vehicle's ignition system, while any unsuccessful authentication triggers alerts to predefined numbers, notifying of potential security breaches. The system also employs GPS tracking for real-time location monitoring and utilizes a USB web camera for enhanced surveillance capabilities, capturing images of the vehicle's surroundings for potential identification of unauthorized users. This multifaceted approach, managed by an Arduino Mega microcontroller, aims to provide comprehensive security while offering intuitive feedback through an LCD display, LEDs, and a buzzer.

By incorporating biometric authentication and OTP verification, the proposed anti-theft vehicle security system presents a robust defense against unauthorized access. Whether through fingerprint recognition or facial scanning, users are required to authenticate their identity, with successful matches progressing to the OTP verification stage. Utilizing GSM communication, the system sends OTPs to registered mobile devices, ensuring an additional layer of security before granting access to the vehicle's ignition system. In the event of unsuccessful authentication attempts, the system promptly triggers alerts to predefined numbers, safeguarding against potential security breaches. Real-time GPS tracking enhances security measures by allowing vehicle owners to monitor their vehicle's location remotely, while a USB web camera supplements surveillance capabilities, capturing images of the vehicle's vicinity. Managed by an Arduino Mega microcontroller, the system provides intuitive feedback through an LCD display, LEDs, and a buzzer, enhancing user experience and ensuring efficient security management.

Block Diagram:

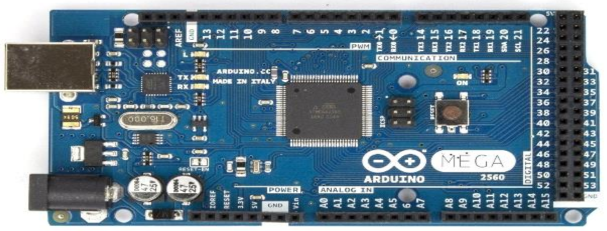


IV. METHODOLOGY

Hardware used here are:

Arduino Mega:

The Arduino Mega is a versatile microcontroller board renowned for its robust capabilities and extensive range of input/output pins, making it a favored choice for complex projects requiring multiple connections and functionalities. Equipped with a powerful ATmega2560 processor running at 16MHz, the Arduino Mega offers ample computing power for handling diverse tasks, from controlling motors and sensors to managing communication protocols. With 54 digital input/output pins, of which 15 can be used for PWM (Pulse Width Modulation) output, and 16 analog inputs, the Arduino Mega provides unparalleled flexibility in interfacing with various sensors, actuators, and peripheral devices. Its compatibility with a wide array of shields and modules further expands its functionality, allowing users to customize their projects according to specific requirements.



Moreover, the Arduino Mega's extensive memory resources, including 256KB of flash memory for storing program code and 8KB of SRAM for dynamic memory allocation, enable the implementation of complex algorithms and data processing tasks. Its robust design and open-source nature foster a vibrant community of developers, makers, and enthusiasts, who contribute to an extensive library of pre-written code and tutorials, facilitating rapid prototyping and development cycles. Whether used in hobbyist projects, educational initiatives, or professional applications, the Arduino Mega continues to be a cornerstone in the world of embedded systems, empowering users to bring their creative ideas to life with ease and efficiency.

Fingerprint Sensor:

The integration of a fingerprint sensor within the proposed anti-theft vehicle security system serves as a pivotal component in ensuring robust user authentication. This biometric technology offers a high level of security by uniquely identifying individuals based on their unique fingerprint patterns. When a user initiates the authentication process, they are prompted to place their finger on the sensor embedded in the ignition key. The sensor then captures the user's fingerprint data and compares it with the stored records in the system's database. If the fingerprint match is successful, indicating that the presented fingerprint matches an authorized user, the system proceeds to the next authentication stage. In case of a mismatch or failure to authenticate, the system denies access to the vehicle's ignition system and may trigger alerts to notify of potential security breaches. The fingerprint sensor thus plays a crucial role in preventing unauthorized access and enhancing the overall security of the vehicle.

Furthermore, the implementation of a fingerprint sensor offers several advantages beyond traditional authentication methods such as keys or passcodes. Unlike keys, which can be lost, stolen, or duplicated, fingerprints are inherently unique to each individual and cannot be easily replicated. This enhances the system's resistance to theft and unauthorized use, as only individuals with registered fingerprints can gain access to the vehicle. Additionally, the use of a fingerprint sensor adds a layer of convenience for users, eliminating the need to carry keys or remember passcodes. The seamless integration of biometric technology into the vehicle security system not only enhances security but also enhances user experience, offering a reliable and efficient means of authentication for vehicle owners.

Relay 5v:

A relay is an electromechanical device that functions as a switch, enabling the control of high-power circuits with low-power signals. Operating on the principle of electromagnetism, a relay consists of a coil, a movable armature, and one or more sets of contacts. When a low-voltage signal is applied to the coil, it generates a magnetic field, attracting the armature and causing the contacts to change position. This action effectively opens or closes the circuit connected to the relay's contacts, allowing or interrupting the flow of electricity. Relay modules typically feature multiple sets of contacts, enabling them to control multiple circuits simultaneously. The 5V designation refers to the voltage required to activate the relay coil, making it compatible with common microcontroller systems such as Arduino. Due to their versatility and reliability, 5V relays find extensive use in various applications, including home automation, industrial control systems, and automotive electronics.

In addition to their primary function as switches, 5V relays offer several advantages that make them suitable for a wide range of applications. Their ability to isolate control signals from high-power circuits provides an added layer of safety, preventing damage to sensitive electronic components. Furthermore, the mechanical nature of relays ensures robust performance in harsh environments, including temperature extremes and high humidity. The 5V voltage requirement makes these relays compatible with most microcontroller platforms, simplifying integration into electronic projects. Additionally, relay modules often feature opto-isolation, further enhancing their reliability by electrically isolating the control signal from the load circuit. This feature minimizes the risk of interference and ensures stable operation, even in noisy environments. Overall, the 5V relay's combination of versatility, reliability, and compatibility makes it a valuable component in numerous electronic and electrical systems.

GSM :

GSM (Global System for Mobile Communications) plays a pivotal role in modern telecommunications, particularly in enabling mobile communication across the globe. This standard for digital cellular networks facilitates voice calls, text messaging, and data transmission, offering widespread coverage and compatibility with a variety of mobile devices. GSM networks utilize a combination of Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) techniques to allocate radio channels efficiently, allowing multiple users to share the same frequency spectrum simultaneously. Additionally, GSM's encryption algorithms provide a layer of security for communications, safeguarding against eavesdropping and unauthorized access. With its widespread adoption and robust infrastructure, GSM remains a cornerstone of modern telecommunications, supporting a myriad of applications ranging from personal communication to machine-to-machine (M2M) communication in various sectors such as automotive, healthcare, and logistics.

Moreover, GSM technology serves as a vital component in the implementation of various remote monitoring and control systems, including security systems, asset tracking solutions, and IoT (Internet of Things) devices. Through GSM modules embedded in these systems, data can be transmitted wirelessly over cellular networks, enabling real-time communication and control from remote locations. This capability is particularly advantageous in scenarios where wired connectivity is impractical or unavailable, allowing for flexible deployment and scalability. Additionally, GSM's reliability and extensive coverage ensure consistent communication even in remote or challenging environments, making it a preferred choice for applications requiring seamless connectivity and remote management capabilities. As the backbone of mobile communication infrastructure, GSM continues to evolve, with advancements such as 4G LTE and emerging technologies like 5G promising even greater speed, capacity, and efficiency for future telecommunications networks.

DC Motor:

A DC motor, short for Direct Current motor, is a type of electrical machine that converts electrical energy into mechanical energy through the interaction of magnetic fields. It operates on the principle of electromagnetic induction, where a current-carrying conductor placed within a magnetic field experiences a force. In a DC motor, this force is utilized to generate rotational motion. The basic components of a DC motor include a stator (stationary part) consisting of permanent magnets or electromagnetic windings and a rotor (rotating part) comprising a coil of wire known as an armature. When a direct current is applied to the armature, it creates a magnetic field that interacts with the magnetic field produced by the stator, resulting in a torque that causes the rotor to rotate. By controlling the magnitude and direction of the applied current, the speed and direction of the motor can be regulated. DC motors find widespread applications in various industries, including automotive, robotics, aerospace, and manufacturing, due to their simplicity, reliability, and ease of control.

DC motors offer several advantages, including high efficiency, compact size, and smooth speed control, making them ideal for a wide range of applications. They are known for their linear torque-speed characteristics, providing consistent performance across different loads. Additionally, DC motors are relatively simple to control using techniques such as pulse width modulation (PWM), allowing for precise speed regulation and smooth operation. Another advantage is their ability to generate high starting torque, making them suitable for applications requiring quick acceleration, such as in electric vehicles and conveyor belts. Moreover, DC motors are versatile and can be easily adapted to various power sources, including batteries, solar panels, and power grids. However, they also have limitations, such as the requirement for periodic maintenance of brushes and commutators in brushed DC motors and the presence of electromagnetic interference in some applications. Despite these drawbacks, DC motors remain a popular choice in many industries due to their excellent performance, reliability, and ease of use.

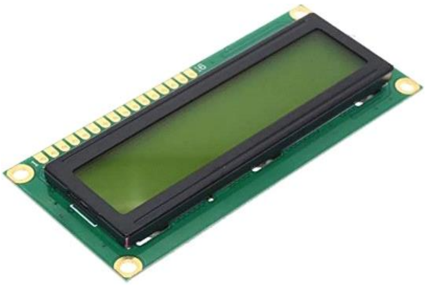
GPS:

Global Positioning System (GPS) technology has revolutionized various industries, including transportation, navigation, and security. GPS utilizes a network of satellites orbiting Earth to accurately determine the location, velocity, and time information of receivers on or near the planet's surface. These satellites transmit signals that are received by GPS receivers, commonly integrated into devices such as smartphones, vehicles, and wearable gadgets. Through a process called trilateration, GPS receivers calculate their precise position by measuring the time it takes for signals from multiple satellites to reach them. This information enables users to pinpoint their location anywhere on the globe with remarkable accuracy, typically within a few meters. In the context of vehicle security systems, GPS technology plays a crucial role in real-time tracking, allowing owners to monitor the whereabouts of their vehicles remotely. Additionally, GPS data can be used for route optimization, asset management, and geofencing, enhancing operational efficiency and security measures.

Beyond its applications in navigation and tracking, GPS technology has also significantly impacted emergency response, environmental monitoring, and scientific research. Emergency services rely on GPS to locate individuals in distress accurately, enabling swift and precise assistance in times of need. Environmental scientists use GPS to monitor changes in land use, track wildlife migrations, and study the Earth's crustal movements. Moreover, GPS plays a vital role in synchronizing time-sensitive operations across various industries, ensuring precise timing for telecommunications, financial transactions, and power grid management. As technology continues to evolve, advancements in GPS technology, such as the integration of augmentation systems like WAAS (Wide Area Augmentation System) and GLONASS (Global Navigation Satellite System), promise even greater accuracy and reliability in location-based services. With its widespread adoption and ongoing innovation, GPS continues to shape the way we navigate, communicate, and understand our world.

LCD:

The LCD (Liquid Crystal Display) plays a crucial role in the proposed anti-theft vehicle security system, serving as a user interface for providing real-time feedback and system status updates. Positioned within the vehicle dashboard, the LCD presents clear and concise information to users, such as authentication outcomes, security alerts, and GPS tracking data. Its intuitive design ensures ease of use, allowing vehicle owners to interact with the system effortlessly. Through the LCD, users can verify successful authentication, receive notifications about potential security threats, and monitor their vehicle's location in real-time. Additionally, the LCD can display prompts and instructions during the authentication process, guiding users through the necessary steps to gain access to the vehicle's ignition system. With its prominent placement and dynamic functionality, the LCD enhances the overall user experience and contributes to the system's effectiveness in preventing theft and unauthorized access.



Furthermore, the LCD serves as a vital component for visual feedback and system management within the anti-theft vehicle security system. Its ability to display authentication outcomes, security alerts, and GPS tracking information in real-time allows users to stay informed and make informed decisions regarding their vehicle's security. The LCD's role extends beyond mere communication to actively engaging users in the authentication process, providing clear instructions and prompts for seamless interaction. Its integration with other system components, such as the Arduino Mega microcontroller and GSM communication module, ensures coordinated functionality and efficient operation. Moreover, the LCD's versatility enables it to adapt to different user needs and preferences, offering customizable display options and settings. Overall, the LCD enhances the system's usability, visibility, and effectiveness, making it an indispensable component in the defense against theft and unauthorized access to vehicles.

Buzzer:

The buzzer serves as an essential component within the proposed anti-theft vehicle security system, contributing to its multifaceted security features. Integrated into the user interface, the buzzer provides audible feedback to users regarding the system's status, authentication outcomes, and potential security threats. In the event of unauthorized access attempts or suspicious activities, the buzzer emits warning signals, alerting nearby individuals and deterring potential intruders. Its presence enhances the system's effectiveness by providing an additional layer of security through audible alerts, ensuring that both vehicle owners and surrounding individuals are promptly informed of any security breaches or unauthorized access attempts.

Furthermore, the buzzer's functionality extends beyond security alerts to include intuitive feedback on the system's operation. During the authentication process, the buzzer may emit different tones or patterns to indicate successful authentication, prompting users to proceed to the next stage confidently. Additionally, in situations where the system detects potential issues or requires user intervention, the buzzer can alert users through distinct signals, prompting them to take appropriate action. By integrating the buzzer into the user interface, the system enhances usability and ensures that users can interact with the security system effectively, thereby reinforcing the overall security measures in place to protect the vehicle against theft and unauthorized access

Power supply:

In our system architecture, the power supply plays a critical role in establishing a stable and regulated electrical environment essential for the optimal operation of various components. To fulfill this role, we incorporate a DC to DC converter that integrates both a voltage regulator and a bridge rectifier. The bridge rectifier, positioned as a central element within the power supply setup, is responsible for converting incoming alternating current (AC) from the source into a consistent direct current (DC). This rectification process is crucial for ensuring a reliable one-way flow of electricity, laying a strong foundation for maintaining stability in the power input. Following this, the voltage regulator steps in to refine and stabilize the output of the pulsating DC. By employing this component, we ensure a steady voltage supply to the system, effectively minimizing the risk of fluctuations that could potentially impact the performance of sensitive electronic components.

Additionally, the voltage regulator assumes a critical function in securing a consistent power provision across the entire system. Through the regulation of voltage levels within specified parameters, it shields the interconnected components from voltage fluctuations, thereby amplifying the reliability of the system as a whole. The amalgamation of a bridge rectifier and voltage regulator not solely transforms the incoming electrical signal into an appropriate format but also ensures a steady power output to the intricate assortment of components. This steadfastness fosters peak performance and prolongs the operational longevity of the electronic system.

Advantages and Applications

ADVANTAGES

- Biometric Integration
- Enhanced Security
- Real-time Tracking
- Multi-layer Authentication
- Remote Control
- Surveillance
- User-friendly Interface
- Prompt Alerts
- Theft Prevention
- Effective Deterrent

APPLICATIONS

- Productivity
- Communication
- Entertainment
- Navigation
- Finance
- Health
- Social
- Gaming
- Education
- Photography
-

V. RESULTS

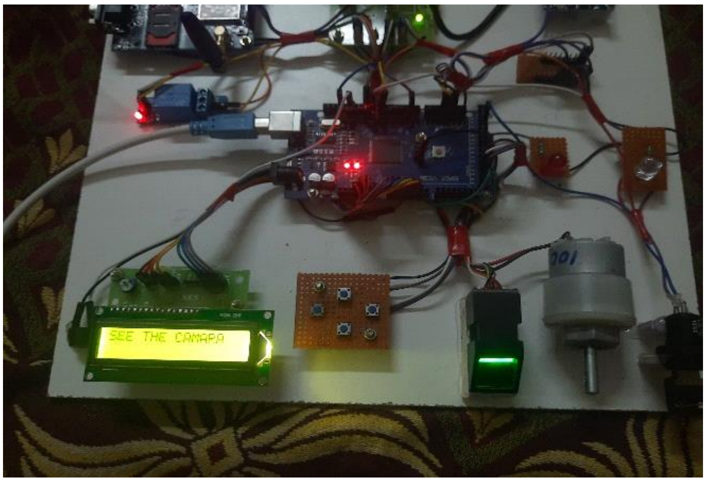


Fig1

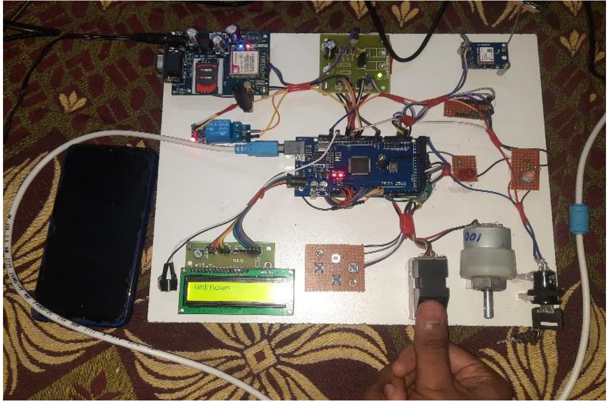


Fig2

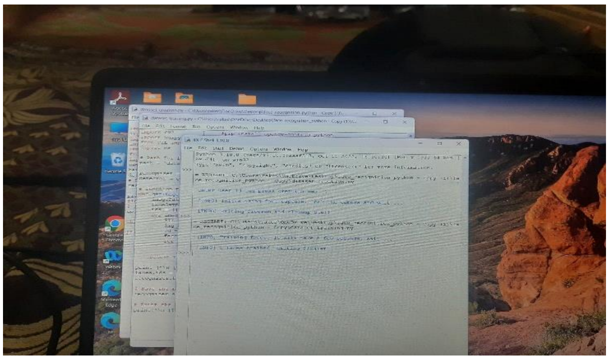


Fig3

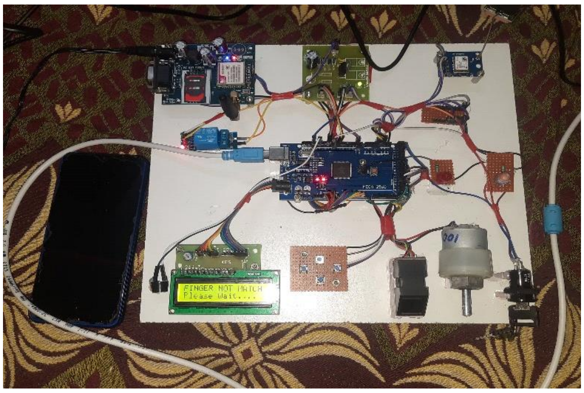


Fig4

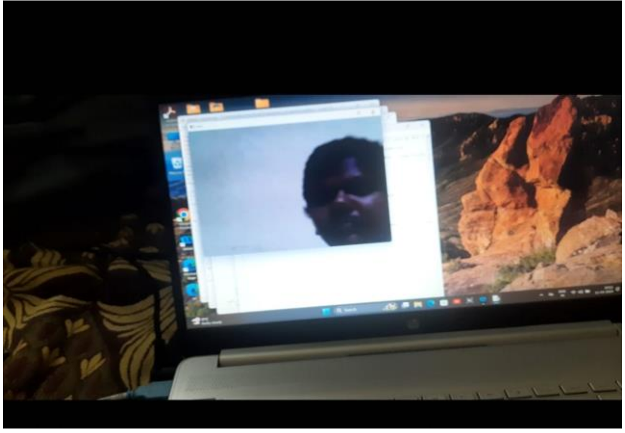


Fig 5

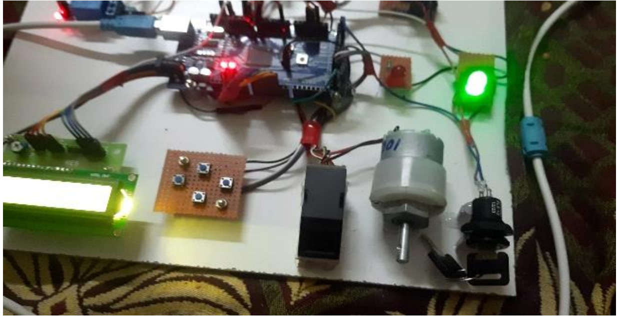


Fig6

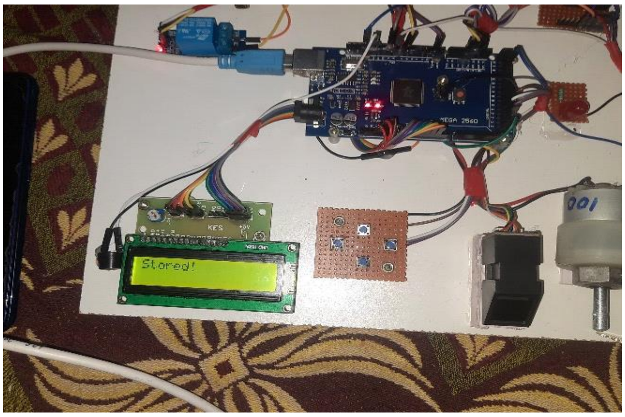


Fig7

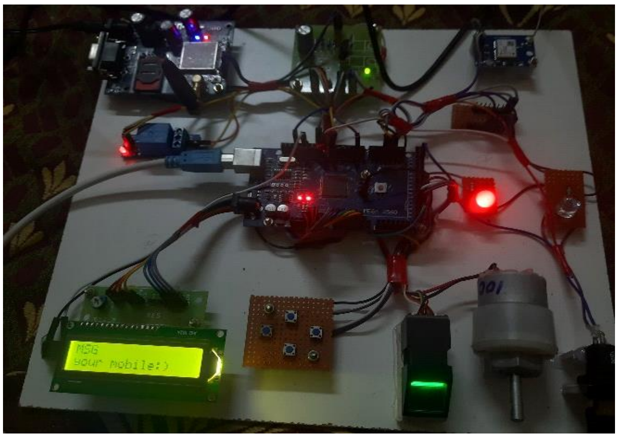


Fig 8

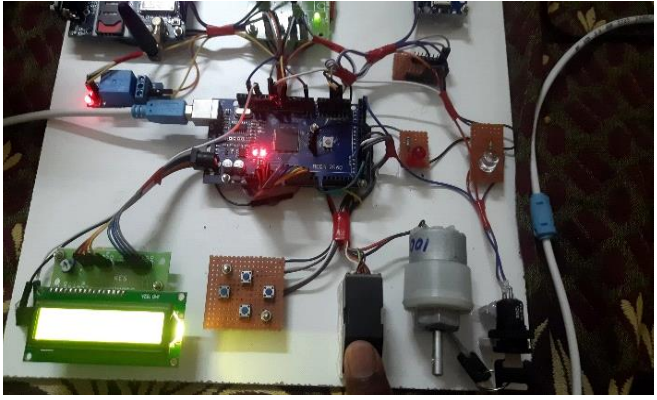


Fig 9

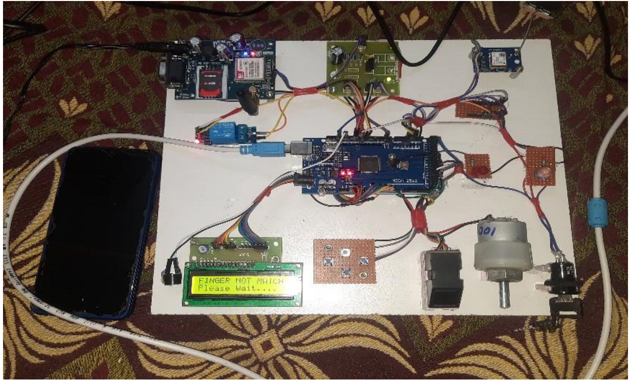


Fig 10

VI. CONCLUSION

In conclusion, the proposed anti-theft vehicle security system offers a comprehensive and robust solution to safeguard vehicles against unauthorized access and theft. By integrating biometric authentication, OTP verification, GPS tracking, and enhanced surveillance capabilities, the system provides multiple layers of security. Managed by an Arduino Mega microcontroller, the system ensures efficient authentication processes and real-time monitoring, while intuitive feedback mechanisms such as an LCD display, LEDs, and a buzzer enhance user experience. With these features in place, vehicle owners can have peace of mind knowing that their vehicles are well-protected, thereby deterring potential thieves and enhancing overall security measures.

VII. REFERENCES

[1]. Sadagopan, Vinoth Kumar, Upendran Rajendran, and Albert Joe Francis authored the paper titled "Design of an Anti-theft Control System Using Embedded Systems," which was presented at the 2011 IEEE International Conference on Vehicular Electronics and Safety.

[2]. Pawar, M.R., and Rizvi, I. (2018). "Development of an IoT-Based Embedded System for Vehicle Security and Driver Monitoring." In Proceedings of the Second International Conference on Inventive Communication and Computational Technologies (ICICCT), IEEE.

[3]. Manjunath, T. K., Andrews SamrajMaheswari, and Chidaravalli Sharmila authored a paper titled "Locking and Unlocking of Theft Vehicles Using CAN," which was presented at the 2013 International Conference on Green High Performance Computing.

[4]. Mukhopadhyay, D., et al. (2018). "Exploring the Development of an IoT-Driven Approach for Vehicle Security." In Proceedings of the 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS) (pp. 1-6). IEEE.

[5]. Ramadan, M. N., Al-Khedher, M. A., and Al-Kheder, S. A. published a paper titled "Intelligent vehicle security and tracking system" in the International Journal of Machine Learning and Computing in 2012 (Volume 2, Issue 1).

[6]. Jesudoss, A., Vybhavi, R., & Anusha, B. (2019). "Smart Helmet Design for Accident Avoidance." In Proceedings of the 2019 International Conference on Communication and Signal Processing (ICCSP). IEEE.

[7]. S. Ajaz, M. Asim, M. Ozair, M. Ahmed, M. Siddiqui, and Z. Mushtaq presented a paper titled "Autonomous Vehicle Monitoring Tracking System" at SCONEST 2005, which was published in the conference proceedings spanning pages 1-4 in 2005.

[8]. Joseph A. O'Sullivan and Robert Pless contributed to the article titled "Advances in Security Technologies: Imaging, Anomaly Detection, and Target and Biometric Recognition," which was published in the International Volume of the Microwave Symposium IEEE/MTT-S in 2007.