IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FINGERPRINT VEHICLE ACCESS AND GSM COMMUNICATION FOR ENHANCED SECURITY

1Mr. D Vijendra Kumar,2Pedamallu Pavan Kumar,3Boddepalli Chandu,4Tumula Umesh Chandra,5Challa Madhav Reddy

1AssistantProfessor, Dept of ECE, Godavari Institute of Engineering and Technology(A), Rajahmundry, AP 2,3,4,5Students, Dept of ECE, Godavari Institute of Engineering and Technology (A), Rajahmundry, AP

Abstract: The cutting-edge Biometric Vehicle Access and GSM Communication for Enhanced Security seamlessly combines biometric technology with mobile communication to fortify vehicle security. Utilizing fingerprint recognition and GSM connectivity, it establishes robust authentication processes while ensuring user convenience. The integrated GSM module enables instant communication between the vehicle and the owner's mobile device, providing real-time alerts for suspicious activities. Sophisticated algorithms minimize false acceptances, adapting to changes in finger conditions and environmental variables. Engine ignition depends on successful biometric authentication and owner verification via SMS, ensuring foolproof security. Using of Arduino mega 2560, GSM sim900A, AS608 fingerprint sensor module provides accuracy and efficiency outputs. This innovative system enhances user experience by eliminating traditional keys and addresses concerns regarding vehicle theft and unauthorized usage in today's dynamic landscape.

Index Terms - **Arduino Mega 2560, GSM SIM 900A Module, As608 Fingerprint sensor Module**.

I. INTRODUCTION

The automotive industry has witnessed the production of an estimated 1.47 billion automobiles to date, alongside a concerning rise in compromised vehicles. instances of car theft by unauthorized individuals have prompted manufacturers to explore various security enhancements. intense competition among manufacturers drives innovation, leading to advancements in vehicle security across various fronts. Some pioneering companies are integrating cutting-edge technologies such as biometric authentication, rfid tags, and iris recognition to bolster security measures. Leveraging insights from past inventions, we can strategically address previous shortcomings, turning them into strengths within the system

2. LITERATURE REVIEW

Jamilah Karim and colleagues (2009) delved into the intriguing concept of remotely starting car ignitions using mobile phones. This innovative approach allowed users to send SMS commands from their mobile devices to activate their vehicle's engine, leveraging GSM technology. What's particularly fascinating is their vision for the future expansion of this system beyond mere ignition control. They envisioned a system that could seamlessly integrate with various household devices, such as garage doors, house lights, and even electric parasols, all controllable via mobile phones. This foresight not only enhances convenience but also adds an extra layer of security and functionality to users' lives.

Similarly, Hariz Hazli Bin Aziz and co-authors (2011) embarked on a journey to revolutionize vehicle ignition control by harnessing the power of Bluetooth-enabled mobile devices. Their system, which employed the Blue 506 technology, allowed users to pair their smartphones with the vehicle's Embedded Blue 506 module, granting them the ability to issue ignition commands remotely. By focusing on user experience, security, and safety, they not only modernized the ignition process but also ensured compatibility with both iOS and Android platforms, catering to a wide range of users.

Moving forward, Ajinkya Kawale and team (2013) directed their efforts towards enhancing bike safety through the implementation of a Fingerprint Sensor Module. This module, coupled with a signaling buzzer, provided bike owners with a robust security solution, allowing them to manage fingerprint templates and control access to their motorcycles. However, they also acknowledged a potential drawback: the system's reliance on battery power. Nonetheless, its cost-effectiveness made it a viable option for enhancing security measures.

Amit Saxena and collaborators (2014) took a different approach by proposing a fingerprint-based security system tailored specifically for vehicles. Their system utilized a combination of microcontrollers and interface circuits to enable/disable the vehicle's lock based on stored fingerprint templates. By storing authorized users' fingerprints in a database and comparing them during authentication, they ensured that only permitted individuals could access and start the vehicle. This method represented a significant advancement in vehicle security compared to traditional key-based systems.

Kiran Rana Gill and associates (2016) introduced yet another innovative solution by focusing on fingerprint-based car ignition systems. By leveraging AVR microcontrollers, they developed a system where the owner's unique fingerprint served as the key to starting the vehicle. This not only eliminated the need for conventional keys but also enhanced security measures by utilizing biometric authentication. However, they noted a potential downside: the cost associated with using AVR microcontrollers.

Similarly, Karan Siyal and co-researchers (2016) explored the realm of vehicle theft prevention through wireless technology. Their system allowed vehicle owners to remotely deactivate the ignition via SMS, triggered by a GSM modem connected to a microcontroller. While effective, the complexity of the system may result in higher costs, indicating a trade-off between enhanced security and affordability.

In a parallel effort, Sayantam Sadhukhan and team (2017) emphasized the importance of securing vehicles using a combination of fingerprint technology and mobile applications. Their biometric auto-entry system not only restricted access to authorized individuals but also sent instant notifications to the owner in case of theft. This approach mirrored the security measures commonly employed to safeguard personal cell phones, highlighting the importance of protecting valuable assets.

Lastly, Bhojane K.J and collaborators (2018) sought to establish a secure environment for vehicle ignition and access through facial recognition techniques. Their system utilized sophisticated face detection algorithms, including neural networks and fuzzy theory, to accurately identify confirmed users based on facial features. By incorporating shading and eye detection, they ensured robust security measures for vehicle access, paving the way for future advancements in biometric authentication technology.

3. EXISTING SYSTEM

The current security system outlined in the project paper utilizes Iris scanning, Facial recognition, and RFID tags. However, these methods are not without their challenges. Issues such as imperfect visibility, inaccuracies in scanning, variations in resolution, and the impact of factors like facial expressions, aging, and the potential loss of RFID tags pose significant limitations to the system's effectiveness. These challenges highlight the need for further refinement and innovation to overcome these hurdles and ensure reliable and robust security measures.

DRAWBACKS:

a. Frequently, these technologies exhibit low recognition rates and are susceptible to variations in resolution. Additionally, their effective verification range typically spans less than 30 centimeters, posing challenges to achieving perfect authentication processes.

b. The potential loss or forgetfulness of RFID tags presents grave concerns. Should a tag be misplaced or fall into the wrong hands, there's a significant risk of it being exploited for vehicle theft, underscoring the critical importance of safeguarding these tags.

4.PROPOSED SYSTEM

The proposed system comprises several key components, including the Arduino Mega 2560, GSM sim 900a Module, As608 Fingerprint Sensor Module, Single Channel Relay, DC Motors, Battery, LED, Switch, and Connecting wires. These elements are meticulously organized and depicted in Figure 1.

The functionality of the system revolves around the control of the fingerprint sensor, GSM Module, and Relay Module by the Arduino Mega 2560. Each module is programmed to operate in sync, ensuring seamless performance. Specifically, the Arduino Mega is programmed to initiate the Fingerprint reader followed by the GSM Module, executing a series of tasks in a desired sequence.

Upon user interaction, the Fingerprint Module reads the user's fingerprint and verifies it against stored data. If a match is found, a message is generated via the GSM Module, prompting the registered user to reply with "Yes" to ignite the vehicle. Upon receiving the affirmative response, the Arduino Mega signals the Single Channel Relay, causing an LED to illuminate, indicating readiness for vehicle operation. Additionally, a switch connected to the relay serves as a gear system, enabling control over the DC motors for vehicle movement.

In the event of a failed fingerprint match, a warning message is sent, alerting the user of potential unauthorized access attempts. Furthermore, if the fingerprint is verified but the user replies with "NO" during GSM Module verification, vehicle operation is halted as a security measure. This intricate system ensures not only seamless functionality but also robust security measures to safeguard against unauthorized usage.

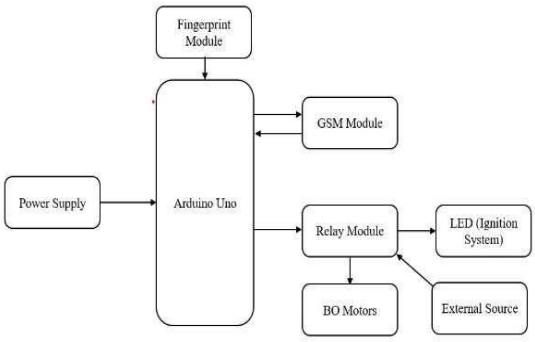

Fig. a. Block Diagram of Proposed System

V. REQUIRED COMPONENTS

A. HARDWARE USED

The following hardware is used in the project which is explained as follows:-

1. Arduino Mega 2560

The Arduino Mega 2560, built around the AT Mega 2560 microcontroller, stands out as a robust microcontroller board renowned for its versatility and extensive capabilities. Serving as a compact computing device, it facilitates seamless communication with a diverse array of electrical components, including displays, motors, and sensors.

At the heart of the Arduino Mega 2560 lies the AT Mega 2560 microcontroller, functioning as the central processing unit responsible for executing instructions and managing inputs and outputs. With its ample resources, the Mega 2560 offers an expanded array of digital and analog pins, boasting 54 digital input/output pins and 16 analog inputs. This generous pin count, coupled with its larger physical size, provides ample space for tackling more complex projects.

Furthermore, the Mega 2560 offers enhanced memory capacity compared to standard Arduino AVR boards, featuring 8 KB of SRAM for variable storage and a total of 256 KB of flash memory for software storage. This ample memory allocation empowers developers to undertake projects of varying complexities, ranging from robotics to home automation.

Renowned for its flexibility, the Arduino Mega 2560 is compatible with a plethora of Arduino shields and software libraries, facilitating seamless integration into a wide range of applications. Its wealth of ports, memory, and capabilities make it an ideal choice for projects requiring extensive input and output connections, cementing its status as a stalwart microcontroller board for demanding endeavors.

2. The GSM SIM900A

The GSM SIM900a module serves as a vital bridge between electronic devices and mobile networks, leveraging GSM technology for seamless communication. Compact and versatile, this module is easily integrated into projects involving platforms such as Arduino or Raspberry Pi. By enabling connectivity to the GSM network, it empowers projects to send/receive messages, make phone calls, and access the internet remotely.

Utilizing a SIM card akin to those found in mobile phones, the SIM900A module facilitates access to the network, complete with necessary information like phone numbers. Capable of handling SMS, voice calls, and data connections, it proves invaluable for projects requiring remote communication or guidance.

Integration is simplified thanks to compatibility with various microcontroller platforms, ensuring ease of incorporation into diverse projects. With the GSM SIM900A module, electronic projects gain the ability to communicate over cellular networks, akin to conventional mobile phones, thus expanding their capabilities and functionality significantly.

3. AS608 Fingerprint Sensor

The AS608 Fingerprint Sensor is a compact electronic device designed for the identification and storage of fingerprints. Utilizing advanced scanning technology, it captures the unique patterns present on an individual's fingertip and converts them into digital data. Similar to a personalized signature, each fingerprint is distinct, enabling secure authentication. Commonly employed in security systems, the AS608 sensor offers a convenient alternative to traditional passkeys or passwords. By simply placing a finger on the sensor, users can unlock doors or access systems with ease. Upon contact, the sensor captures a snapshot of the fingerprint using an integrated camera and analyzes its ridge and valley patterns to generate a digital representation. With the capability to store multiple fingerprints in its memory, the AS608 sensor facilitates efficient access

control. During authentication, the scanned fingerprint is compared against the stored database. If a match is found, access is granted, enhancing security measures. Versatile in application, the AS608 fingerprint sensor seamlessly integrates into various electronic projects, including door locks, safes, and smartphones, to augment safety protocols. By providing a straightforward and protective means of fingerprint recognition and storage, the AS608 sensor serves as a valuable tool for ensuring secure access to devices and systems.

4. Single-Channel Relay

A single-channel relay serves as an essential electromechanical switch capable of managing the connection and disconnection of a single electrical circuit. At its core lies an electromagnet (coil) that, upon activation, maneuvers an armature to establish or disrupt connections between multiple terminals. This mechanism regulates the flow of current within the circuit. Engineered with specific voltage and current ratings, single-channel relays ensure safe switching operations. Voltage ratings typically range from 5V to 24V DC, while current ratings vary based on the relay model. These relays feature two primary contacts: normally closed (NC) and normally open (NO). In their default state, the NC contact is engaged, and the NO contact remains open. However, when energized, this configuration reverses. Activation of the relay coil necessitates the application of voltage to the coil terminals, achievable through a microcontroller, digital signal, or manual switch. Crucially, relays offer electrical isolation between the control circuit (coil side) and the load circuit (contact side), shielding control circuitry from voltage fluctuations or noise generated by the load. The durability of a relay is gauged by its operational lifespan, often spanning hundreds of thousands or even millions of cycles under normal conditions. Renowned for their reliability, single-channel relays find widespread utility across industrial automation, home automation, and automotive applications, facilitating seamless control over electrical circuits with precision and efficiency.

5. SWITCH

A switch, in its essence, is an electronic component designed to regulate power within a circuit, toggling between an on and off state. Functioning as a pivotal element within electrical systems, it possesses the ability to establish or sever connections, thereby controlling the flow of electric current. The most commonly encountered type is the electromechanical switch, featuring one or more terminals linked to external circuits. In operation, current flows through the switch only when there is contact between its terminals; otherwise, the circuit remains inactive. This contact can be established either manually or via electrical means. Typically, a switch comprises two terminals: one serves as the power source, while the other directs power to the intended device or circuit. Its two primary states, on and off, dictate whether a connection exists between the terminals, thereby determining the flow of current. Switches serve diverse purposes, with some operated manually by users to control systems, while others function automatically to manage machinery and devices autonomously, sans human intervention. Utilizing sensors such as pressure, temperature, flow, current, voltage, or force, automatic switches seamlessly orchestrate device operations based on predetermined parameters within the circuit.

6. DC BO Motors

DC motors are fundamental electric motors powered by direct current (DC). They harness the principles of magnetic fields to transform electrical energy into mechanical energy. Operating on the Lorentz force principle, these motors exploit the interaction between a conductor carrying current and a magnetic field, generating a force perpendicular to both the magnetic field lines and the current path. Each DC motor is rated for specific voltage and current levels, which dictate its performance attributes such as speed, torque, and power output. Versatile in control methods, DC motors can be managed through techniques like adjusting the applied voltage, employing pulse-width modulation (PWM), or utilizing motor controllers or drivers. DC motors feature widespread applications across diverse industries and devices, including robotics, electric vehicles, industrial machinery, household appliances, power tools, and HVAC systems. When choosing a DC motor for a particular application, it's crucial to assess factors like voltage and current requirements, speed and torque characteristics, efficiency, size, and cost to ensure optimal performance and suitability.

7. LED

LED stands for Light Emitting Diode, a small but powerful piece of technology that emits light when an electric current passes through it. By harnessing the movement of electrons within a semiconductor material, LEDs produce light efficiently. This emission of energy in the form of light occurs as electrons navigate through the semiconductor material. One of the remarkable features of LEDs is their high efficiency in converting electrical power into light. In comparison to traditional incandescent lights, LEDs consume less energy, rendering them both cost-effective and environmentally friendly. The applications of LEDs are vast and varied, spanning from electronic devices like cellphones and TVs to automobile headlights, as well as lighting solutions for homes, offices, and outdoor environments. Their energy efficiency, longevity, and adaptability have revolutionized the lighting industry, making LEDs a staple in a multitude of global applications.

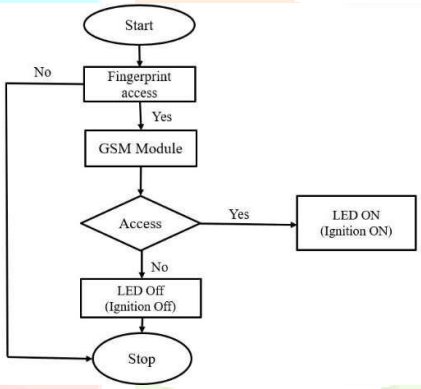

Fig. b. Flow chart of Proposed System

SOFTWARE USED

1.ARDUINO IDE

The Arduino IDE, or Integrated Development Environment, serves as a comprehensive software tool tailored for Arduino microcontroller boards. It facilitates the creation, compilation, and uploading of code to these boards, all within a user-friendly interface.

Programmers can write code in the Arduino programming language, a variant of C/C++, directly within the IDE. Upon completion, the code undergoes compilation, transforming it into instructions comprehensible by the Arduino board. Once compiled successfully, the code is uploaded to the Arduino board connected via USB cable. This enables the microcontroller to execute the specified instructions.

An integral feature of the Arduino IDE is its library manager, enabling users to easily integrate external libraries. These libraries offer pre-written code, expanding the capabilities of Arduino projects with sensor interfaces and more. Additionally, the IDE incorporates a serial monitor tool, facilitating interaction with the Arduino board over the serial port. This tool aids in debugging code and monitoring data exchange between the computer and the board. Accessible across multiple operating systems such as Windows, macOS, and Linux, the Arduino IDE caters to a diverse user base. Being open-source software, it encourages community involvement, fostering collaboration and innovation within the Arduino ecosystem. With its intuitive interface and extensive functionality, the Arduino IDE accommodates both novice and seasoned programmers, empowering them to develop a wide array of projects effortlessly.

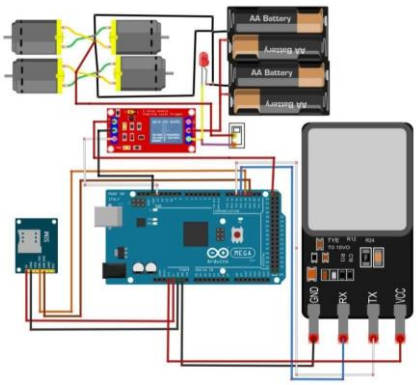

Fig. 1. CIRCUIT DIAGRAM

VI. RESULT

In the event of an unauthorized attempt to access the vehicle using a fingerprint obtained through illicit means, the system is designed to prevent entry. The owner, upon receiving a request from the vehicle, is immediately alerted to any tampering attempts, enabling swift action.

For ignition to commence, the system mandates both the presence of an authorized fingerprint and the user's authentication via reply. This dual verification ensures that only individuals with valid fingerprints and explicit owner authorization can operate the vehicle.

Should the authorization process involve both fingerprint scanning and GSM reply, failure in either component, such as an unauthorized GSM reply or a mismatched fingerprint, will result in the vehicle's ignition remaining inactive. Access to the vehicle is strictly restricted to users authorized to utilize both fingerprint and GSM authentication, ensuring robust security measures are in place.

Fig. 2. Hardware Design of Vehicle prototype

VII. FUTURE SCOPE

Future enhancements for the aforementioned system include the integration of multiple biometric methods, such as fingerprint, iris, and voice recognition, to bolster authentication reliability while maintaining cost-effectiveness. Implementing alerts capable of locking the steering and capturing an image of intruders for transmission to registered user IDs further enhances security measures. System upgrades will enable detection and notification of any attempts to access or bypass the system by intruders, providing added layers of protection. Advancements in technology, particularly advanced encryption techniques, contribute to strengthening system security. The incorporation of machine learning and artificial intelligence promises to enhance the accuracy and efficiency of future system advancements. Secure communication protocols, cloud-

based authentication services, and heightened anti-theft features are anticipated to become prevalent in the automobile industry, elevating vehicle security standards.

VIII. CONCLUSION

The Biometric Vehicle Access and GSM Communication for Enhanced Security system represents a robust approach to bolster vehicle security while offering convenience to authorized users. By seamlessly integrating biometric technology with GSM communication, the system ensures dependable authentication and real-time alerts, contributing to the advancement of automotive security. Utilizing components such as the Arduino Mega 2560, GSM SIM900a Module, AS608 Fingerprint Sensor Module, Single Channel Relay, among others, the system is engineered for smooth operation. The Arduino Mega acts as the central hub, coordinating interactions between the fingerprint sensor, GSM module, and relay to ensure synchronized functionality. Upon fingerprint authentication, the system prompts user confirmation via GSM communication. The vehicle remains inactive until receiving affirmative confirmation, effectively thwarting unauthorized usage.

Furthermore, unauthorized access attempts trigger warning messages, providing an additional layer of security. While potential limitations such as false acceptances are acknowledged, the inclusion of a manual switch offers control over engine activation, effectively mitigating this concern.

In summary, the proposed system offers a comprehensive solution to vehicle security challenges by leveraging biometric authentication and GSM communication. With its user-friendly interface and seamless integration, it represents a significant advancement in automotive security technology, addressing the evolving needs of both the industry and consumers.

IX. REFERENCES

[1] Jamilah Karim, Wan Mohd Arman Bin Wan Amat, Abdul Hadi Abdul Razak University Technology MARA (UiTM), "**control the car ignition using mobile phone**", published in IEEE, *International Conference on Future Computer and Communication,* 2009.

[2] Hariz Hazli Bin Aziz, Noor Hafizah Abdul Aziz and Kama Azura Othman Faculty of Electrical Engineering
University Technology MARA Malaysia used "**Bluetooth technology to control the car ignition via mobile phone**", in IEEE, *Control and System Graduate Research Colloquium,* published in the year 2011.

[3] Prashantkumar R, "**Two Wheeler Vehicle Security System**" Published in *International Journal of Engineering Sciences & Emerging Technologies,* Dec 2013.

[4] Winda Astuti, E. Byan Wahyu Riyandwita, Bina Nusantara University, "**Intelligent automatic starting engine based on voice recognition system**", 2016 IEEE Student Conference on *Research and Development (SCOReD).*

[5] Ali Akbar Shah, Zulfiqar Ali Zaidi, Bhawani Shankar Chowdhry, Jawaid Daudpoto, Mehran University of Engineering and Technology Jamshoro, "**Real time Face Detection/Monitor using Raspberry pi and MATLAB**", IEEE 10th *International Conference on Application of Information and Communication Technology (AICT),* 2016.

[6] Amit Saxena, 2014 worked on the project, "**Ignition based on the fingerprint recognition**" in *International Journal of Scientific Research and Management Studies (IJSRMS)* Vol. 2 Issue 1 in 2014.

[7] Bhumi Bhatt, "**Smart Vehicle Security System Using GSM & GPS**", Published in the journal *International Journal of Engineering and Computer Science (IJECS),* Volume 4 Issue 6 in June 2015.

[8] K. A. Amusa, "**Design of SMS-Enabled Car Security System**", Published in *Transnational Journal of Science and Technology*, in Nov 2012.

[9] Roopam Arora, made a project on "**Start-Up the Engine Using Fingerprinting**", in *International Journal of Computer Engineering and Applications (IJCEA),* in Oct 2015.

[10] Sayantam Sadhukhan, used IoT components and a Fingerprint Scanner, "**Car Security System Employing Fingerprint Scanner and IoT**", released in *Indian Journal of Science and Technology* and published in the year 2017.