Enhancing Vehicle Security And Safety Integrating GPS With Biometric And Password Verification

Dr. C.Selvi[1], M. Mohamed Irfan[2], P. MughilEzhilavan[3], K. Muthazhaku[4]
[1, 2, 3, 4] Dept of Electronics and Communication Engineering
[1, 2, 3, 4] Muthayammal Engineering College, Rasipuram, India.

Abstract- *An IoT-based system using GPS technology has been developed to detect vehicle theft and enable remote engine locking. The system, which uses high-priced products like ignition keys, aims to minimize complications by preventing theft by allowing the vehicle to start only when the correct password is entered or a fingerprint is recognized. The system also prevents the engine from starting if the user is not wearing a helmet. In case of unauthorized scans or password attempts, the system alerts the user via the Blynk app, providing the vehicle's GPS location.*

Keywords- Safety Enhancement, Multi factor Authentication, Password Security, GPS tracking,

I. INTRODUCTION

In recent years vehicle theft has become a significant issue which should be traced and detected. The safety and security of the vehicle is essential. Even there are many existing mechanisms this have some limitations and high cost. So, an efficient security mechanism is needed. This project detects vehicle theft using Arduino and GPS.With the help of the ESP 8266 Wi-Fi module, the vehicle's location is detected using the Global Positioning System(GPS).The GPS system is a satellite-based navigation tool utilized for vehicle tracking, enabling the location of stolen devices to be determined regardless of weather conditions. Through the use of a GPS antenna, it offers precise latitude and longitude coordinates for the device.The Vehicle Tracking system is gaining popularity and is widely utilized in numerous countries across the globe. It offers numerous benefits to users, particularly to vehicle owners, as it enables them to easily monitor the whereabouts of their vehicles. In today's world, smartphones have become an indispensable part of everyone's life. A survey conducted by Time magazine, involving five thousand individuals from the USA, UK, South Korea, India, China, South Africa, Indonesia, and Brazil, revealed that the majority of people are inseparable from their smartphones. Eighty-four percent of the respondents claimed that they could not survive without their smartphones. Additionally, a study indicated that smartphones hold a seventy-five percent market share, with a total of one hundred and six million smartphones shipped in the latter half of 2012. Smartphones have emerged as the primary telecommunication medium in the global market, becoming the most widely used communication tool. The survey results clearly demonstrate the significance of smartphones in modern-day life, underscoring the importance of developing an IOT message-oriented vehicle tracking system. This system allows users to conveniently monitor their vehicles with a single touch on their smartphones. By utilizing the internet connection on their smartphones, users can track the real-time location of their vehicles. The tracking system is designed to provide users with an easy and user-friendly interface for accessing their vehicle information.

Literature Survey:

An Automotive Security System for Anti-Theft, 2022

Author Name: Huaqun Guo, J. J. Ang, F. Tao, C. H. Kwek
Automotive theft is a widespread issue globally, especially with the rise of professional thieves. This paper introduces an automotive security system that can remotely disable a stolen vehicle and its key systems, serving as a deterrent to potential thieves. By implementing four layers of security features in the form of firmware embedded in the Electronic Control Units (ECUs), the system effectively prevents the theft of key auto components for resale. The paper outlines the system's design and implementation, with experimental results demonstrating its feasibility and the owner's ability to regain control of their vehicle within seconds. The most successful automotive security system is one that dissuades thieves from targeting a vehicle in the first place, knowing that the risks outweigh the potential economic gains. By ensuring that stolen vehicles and their key systems can be disabled remotely, thieves are less likely to attempt theft.

II. METHODOLOGY

Workflow of The System

User Authentication Initiation:

When a user approaches the vehicle, they begin the authentication process by activating the system using either a

physical or electronic method. This can be done by pressing a button on a key fob or utilizing a mobile app.

Biometric Identification:

The system requests the user to provide biometric data, such as fingerprint or facial recognition. Biometric sensors capture the user's biometric information.

Biometric Verification:

The captured biometric data is compared against the stored templates of authorized users.If the biometric data matches an authorized user's template, the system proceeds to the next step. If not, access is denied.

Password Verification:

In case the biometric verification fails or as an additional security measure, the system prompts the user to enter a password or PIN using a keypad or touchscreen interface.The entered password is compared against the stored passwords associated with authorized users.If the password matches, access is granted. Otherwise, access is denied.

GPS Verification:

After successful biometric and/or password verification, the system verifies the vehicle's current GPS location.If the vehicle's location matches pre-defined safe zones or authorized areas, access is granted.If the vehicle is outside the designated zones or areas, the system may activate additional security measures, such as sending alerts to the owner or disabling engine ignition.

Access Granted:

If all authentication criteria are met (biometric, password, and GPS verification), the system allows access to the vehicle.Access may involve unlocking doors, disabling immobilizers, and enabling ignition systems.

Access Denied:

If any authentication step fails or if the vehicle is located in an unauthorized area, access is denied.The system may activate alarms, implement deterrent measures like flashing lights, or send notifications to the owner or security personnel.

III. PROPOSED WORK

The proposed system effectively addresses the limitations by utilizing high-priced items such as ignition keys. It offers a cost-effective solution that minimizes complications. Moreover, the vehicle will only start if the password or fingerprint is authenticated. Additionally, the engine will refuse to start if the person is not wearing a helmet. Unauthorized attempts, such as scanning an unauthorized fingerprint or entering the wrong password, will trigger a notification through the blynk app. The app also sends the GPS location, making it a valuable tool for preventing theft. By implementing this system, vehicles are equipped with a superior control mechanism, resulting in a reduction in crimes. Furthermore, the incorporation of password verification adds an extra layer of security, requiring a verified code for ignition or entry. This two-factor authentication approach significantly reduces the risk of unauthorized access, reinforcing the system's security measures. The proposed system's strength lies in its multifaceted security design, which combines GPS tracking, biometric verification, and password authentication. This integrated approach not only prevents theft but also deters unauthorized usage by increasing the complexity of breaching the security measures. By leveraging these advanced technologies, the system aims to provide comprehensive protection against vehicle theft, offering a robust defense against potential threats.

Block Diagram:

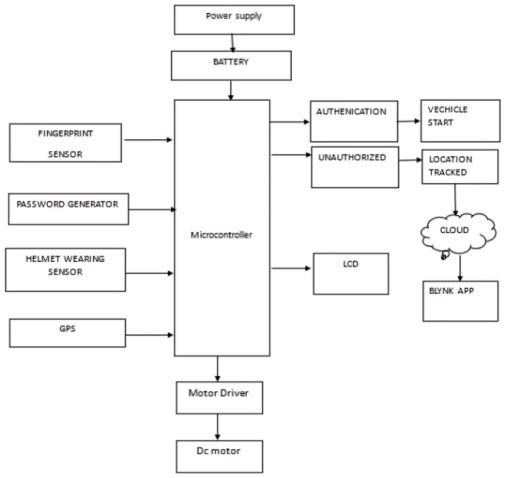

Fig1.1BlockDiagram

Hardware Requirements:

Arduino UNO
Arduino cable
Node MCU
IR Sensor
Matrix Keypad
Fingerprint Sensor
16X2 LCD Display
Gear Motor
Motor Driver
GPS Module
Power Supply

Software Requirements:

- Arduino IDE
- Blynk Application

System Architecture:

The system architecture has been meticulously designed to enhance vehicle security by seamlessly integrating GPS, IoT, biometric, and password verification. This is achieved through a highly sophisticated multi-layered framework. At the heart of this architecture lies the Vehicle Control Unit (VCU), which acts as the central processing entity responsible for orchestrating interactions between various tiers. The Sensor Layer consists of a network of IoT sensors strategically placed throughout the vehicle, collecting crucial data on the vehicle's status, location, and environmental conditions. Simultaneously, the Authentication Layer utilizes biometric scanners or devices, along with password-based systems, to authenticate useridentity before granting access. Beyond the vehicle, the Central Server/Cloud Infrastructure effectively manages data processing, storage, and authentication, while also enabling remote control functionalities. An integral component of this architecture is the Security and Encryption Layer, which employs robust encryption protocols to ensure the integrity and confidentiality of data during transmission.

Sensor Technology:

Sensor technology plays a pivotal role in fortifying vehicle security through the integration of GPS, IoT, biometric, and password verification systems. The implementation of various sensors, such as GPS receivers for precise location tracking, proximity sensors to monitor access points, accelerometers for motion detection, and environmental sensors to gauge surroundings, collectively forms a comprehensive Sensor Layer. These sensors constantly gather and transmit data about the vehicle's status, location, and external conditions to the Vehicle Control Unit (VCU). The amalgamation of these sensor technologies empowers the system to detect unauthorized access, track real-time vehicle movement, and discern abnormal behaviors, thereby enabling swift responses to potential security threats.

IV. FUTURE ENHANCEMENT

The future scope of this paper is in the place RFID reader we can use biometric system. We can send alert message to the owner and nearby police station to track the vehicle by using Global Positioning System and Global System for Mobile. In future we will incorporate vibration sensor inside the framework, which may distinguish the force of auto hitting an item. On the off Chance that force surpasses creatin level, it identifies mishap and may send SMS to family members.

V. RESULT

Integrating GPS tracking with biometric and password verification for vehicle theft protection represents a sophisticated and multi-layered security approach. By combining GPS technology for real-time location tracking with biometric systems such as fingerprint or facial recognition, alongside password verification, this concept significantly fortifies vehicle security.

The GPS element enables owners and authorities to pinpoint a stolen vehicle's location swiftly, facilitating its recovery. Biometric authentication adds an extra level of security by allowing only authorized individual access to the vehicle, reducing the risk of unauthorized usage or theft. Moreover, the inclusion of password or PIN verification serves as a backup method, ensuring access in cases where biometric data might be unavailable or compromised.

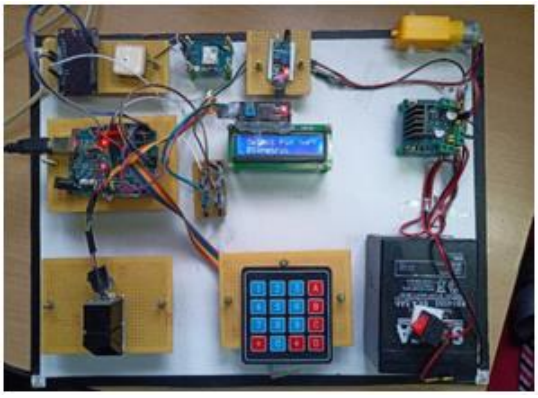

Fig1.2Select Pin or Biometric

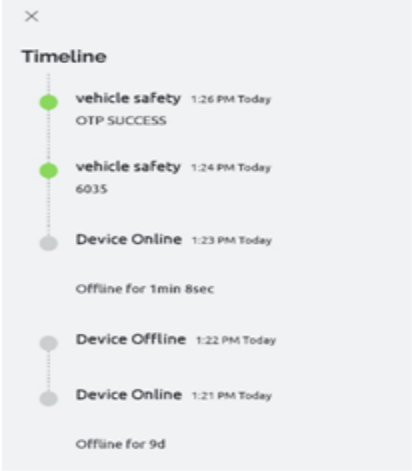

Fig1.3Blynk Notification for OTP

Fig1.4Biometric Authentication

Select Pin or Biometric	Press **A** for Pin	Helmet Weared	OTP Sent	Mobile Notification	OTP Success	Vehicle Started
		Helmet Weared	OTP Sent	Mobile Notification	OTP Invalid (IP Address)	Vehicle not Started
		Helmet not Weared	OTP Sent	Mobile Notification	OTP Success	Vehicle not Started
		Helmet not Weared	OTP Sent	Mobile Notification	OTP Invalid (IP Address)	Vehicle not Started

Select Pin or Biometric	Press **C** for Finger Print	Helmet Weared	Scanning Finger	Authorized (Mobile Notification)	Vehicle Started
		Helmet Weared	Scanning Finger	Unauthorized (Mobile Notification (IP Address))	Vehicle not Started
		Helmet not Weared	Scanning Finger	Authorized (Mobile Notification)	Vehicle not Started
		Helmet not Weared	Scanning Finger	Unauthorized (Mobile Notification (IP Address))	Vehicle not Started

Fig1.5Notification for Biometric

Fig1.6Table of detailed working process

VI. CONCLUSION

We have proposed a novel method of vehicle tracking and locking systems used to track the theft vehicle by using GPS. An IOT based vehicle theft detection and remote engine locking system is GPS technology that helps the users identify the vehicle in theft mode and enables the controlling mechanism technique and, in this way vehicles are provided with better controlling mechanism and thus reducing the crimes. Vehicle theft, but not for violent crimes, has inflicted more damage to its victims in monetary value and secondary financial effects. The proposed system provides vehicle security and recognizes a very low cost efficient and efficient theft. Thus in this way crimes can be reduced to a great extent as vehicles today are being stolen in large number. Hence, vehicles today require high security which can be achieved with the help of this application.

REFERENCES

[1] Pham Hoang DAT,MICHEAL DRIEBERG, Nguyen chi CUONG, “development of vehicle tracking system using GPS and GSM modem”, 2013 IEEE conference on open system (ICOS), December 2-4, 2013, Sarawak , Malaysia.

[2] Sudarsan K and Kumaraguru Diderot P (2014), “Helmet for Road Hazard Warning with Wireless Bike

Authentication and Traffic Adaptive Mp3 Playback", International Journal of Science andResearch (IJSR), Vol. 3, No. 3, ISSN (Online): 2319-7064] V.Krishna Chaitanya, K.Praveen Kumar, "Smart helmet using arduino", Hyderabad, 2013.

[3] Manjesh N, Prof. Sudarshan Raj, "Smart Helmet Using GSM &GPS Technology for Accident Detection and Reporting System", International Journal of Electrical and Electronics Research, Vol. 2, Issue 4, October - December 2014.

[4] K.Dineshkumar, G. Nirmal, S.Prakash, S.Raguvaran A Review of Bike Security System UsingFingerprint GSM&GPS International Journal of Innovative Research in Computerand Communication Engineering(An ISO 3297: 2007 Certified Organization)Vol. 3, Issue 3, March 2015.

[5] Mr. N. BalaSundara Ganapathy, S. Akash, R. Alex Prabhu, T. Kirubakaran, S.Shyam Kumar, 'Anti-Theft Protection of Vehicle by GSM GPS with Fingerprint Verification', International Journal of Advanced Engineering, Management and Science (IJAEMS), Vol-4,Issue-4,April 2018.

[6] A Smart Safety Helmet using IMU and EEG sensors for worker fatigue detection Ping Li, RamyMeziane, Martin J.-D. Otis, Hassan Ezzaidi, REPARTI Center, University of Quebec at Chicoutimi Chicoutimi, Canada Email: Martin_Otis@uqac.ca Philippe Cardou REPARTI Center, Laval University Quebec, Canada Email: pcardou@gmc.ulaval.ca).

[7] Safety measures for "Two wheelers by Smart Helmet and Four wheelers by Vehicular Communication" Manjesh N 1, Prof. Sudarshan raju C H 2 M Tech, ECEDSCE, JNTUA, Hindupur Email: manjesh405@gmail.com HOD & Asst. Prof. BIT-IT, Hindupur International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences (NCDATES09th & 10th January 2015).