IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Remote Vehicle Authentication, Authorization And GPS Tracking

[1] Kuldeep Rathor, [2]Amankumar Singh, [3]Ananya Raorane, [4]Vinayak Ranjane, [5]Prof. Umesh B. Mantale

[1]Student, [2]Student, [3]Student, [4]Student, [5]Professor

Computer Engineering

Terna Engineering College, Navi Mumbai, India

Abstract: In response to escalating concerns regarding vehicle security and unauthorized usage, this paper presents a comprehensive solution incorporating Remote Vehicle Authentication, Authorization, and GPS Tracking systems. With a focus on addressing the prevailing security lacunae in diverse vehicular contexts, the proposed Internet of Things (IoT) device, seamlessly adaptable to vehicles of varying makes and models, integrates with an intuitive mobile application for real-time access to vehicle security status. Key to this system is the integration of GPS tracking technology, facilitating precise location monitoring and verification, thereby fortifying security measures and enabling efficient fleet management. The methodology encompasses the development of the IoT device utilizing Arduino and ESP32 board, alongside the implementation of fingerprint authentication and encryption techniques for remote vehicle authentication. Concurrently, the mobile application, constructed on the Flutter framework, incorporates features for authentication, authorization, and GPS tracking, interfacing with the Blynk server for seamless communication with the IoT device. Rigorous testing and evaluation ensure the system's functionality, reliability, and security under diverse operational scenarios, while user feedback mechanisms inform iterative enhancements. The culmination of this endeavor heralds a significant advancement in vehicular security protocols, poised to augment operational efficiencies and mitigate security risks across diverse vehicular domains.

Index Terms **-** Remote Vehicle Authentication, Authorization, GPS Tracking, IoT, Flutter Application, Blynk Server, Arduino, ESP32 Board, Fingerprint Authentication, Fleet Management

I. INTRODUCTION

With the advent of urbanization, population growth has significantly altered the demographic and socio-cultural landscape of urban settings. As millions migrate to cities in search of better economic and social opportunities, cities are grappling with challenges like congestion, untidy slum formations, income inequalities, and competition for scarce resources[3]. This accelerated urbanization, coupled with poor management and inadequate infrastructure, has resulted in a rise in crime incidents. Crime is not a random or spontaneous phenomenon but is intricately linked to social exclusion, discrimination, and disparities in resource availability, power, wealth, and opportunities[3]. Among the various challenges posed by urbanization, vehicle security stands out as a significant concern. Alarming statistics, such as the revelation that every 14 minutes, a vehicle is stolen in Delhi, underscore the pressing need for robust security measures to safeguard vehicles against theft and unauthorized use[9].

Indeed, high-end cars often come equipped with sophisticated inbuilt security systems; however, there remains a gap in providing comprehensive security solutions for a broader range of vehicles. Our proposed solution involves the development of an Internet of Things (IoT) device that can be seamlessly attached to any vehicle, regardless of its make or model. This IoT device will integrate with a user-friendly mobile application, granting owners convenient access to their vehicle's security features and status in real-time.

The Internet of Things (IoT) has become ubiquitous across various domains, revolutionizing industries such as healthcare, gastronomy, fitness, automotive, and infrastructure [8]. Its versatile implementation extends to providing remote access and control over devices, amplifying convenience in daily operations. Particularly, in the automotive sector, IoT plays a pivotal role in ensuring vehicle safety, a concern paramount for both manufacturers and owners alike[7]. However, despite the rapid advancements in technology, the security of vehicles on the road remains a pressing issue[7]. Instances of unauthorized access and vehicle theft persist, underscoring the need for robust security measures to mitigate such risks[7][1]. Remote vehicle authentication and authorization, coupled with GPS tracking, are crucial components in ensuring secure and efficient vehicle monitoring systems. GSM and GPS allows for continuous monitoring of a vehicle's location and route, facilitating remote access to this information from any location [4][6]. Additionally, the use of GPS technology in vehicle tracking systems has been widely recognized for its effectiveness in providing accurate location data[2].

This research aim is crucial in response to the escalating demand for heightened vehicle security, precise tracking, and data-driven insights, along with the increasing reliance on keyless access technology. With a surge in vehicle theft and inefficient fleet management, there is a clear need for a solution that ensures secure keyless access, real-time tracking, and comprehensive activity records.

II. LITERATURE REVIEW

The increasing prevalence of vehicle theft has spurred research into advanced security systems, with a focus on preventing unauthorized access and enhancing vehicle security. One of the prominent approaches involves the use of Radio Frequency Identification (RFID) and password authentication systems. These systems require correct sensor inputs, RFID tags, and passwords to ignite the engine, effectively thwarting unauthorized access[5]. Our proposed solution leverages the ESP32 board, integrated with Wi-Fi module for wireless connectivity and a relay module for controlling the vehicle's ignition system. An existing system focuses on testing the RFID sensor system for accuracy in reading the E-KTP sensor and validating the GPS tracking accuracy for determining displacement distance[7], our project takes a different approach by integrating a Flutter-based mobile application and cloud-based platforms like Blynk and Firebase for enhanced authentication and remote control functionalities. The ESP32 board's robust capabilities, coupled with the flexibility of cloud-based IoT platforms, allow for real-time tracking and remote control over the vehicle's ignition system, offering both security and convenience for vehicle owners. Our system's automation of vehicle checking and authentication processes reduces the workload on law enforcement agencies and provides an efficient solution to combat vehicle theft.

III. METHODOLOGY

A. Introduction

In contemporary automotive security systems, the incorporation of remote control mechanisms has become imperative to address concerns related to vehicle theft and unauthorized usage. This paper delves into a sophisticated solution that integrates an ESP32-based relay module with the Blynk server, facilitating seamless communication between a mobile application and a vehicle's ignition system. The system architecture encompasses various components, including the relay module, ESP32 board, vehicle battery-powered step-down converter, Wi-Fi module, and the Blynk server, to enable remote control functionalities.

B.System Architecture

At the core of the system lies the ESP32 board, a versatile microcontroller known for its robust capabilities and compatibility with IoT applications. The ESP32 board is directly powered by the vehicle's battery via a step-down converter, ensuring a stable power supply for uninterrupted operation. The Wi-Fi module integrated into the ESP32 board enables wireless connectivity to the internet, facilitating communication with external devices and servers.

The relay module serves as the intermediary between the ESP32 board and the vehicle's ignition system. By controlling the relay module's switch, the ESP32 board can regulate the flow of power to the ignition coil, thereby enabling remote control over the vehicle's ignition mechanism. This setup offers a secure and efficient means of remotely starting or stopping the vehicle's engine, enhancing both security and convenience for vehicle owners.

Error!

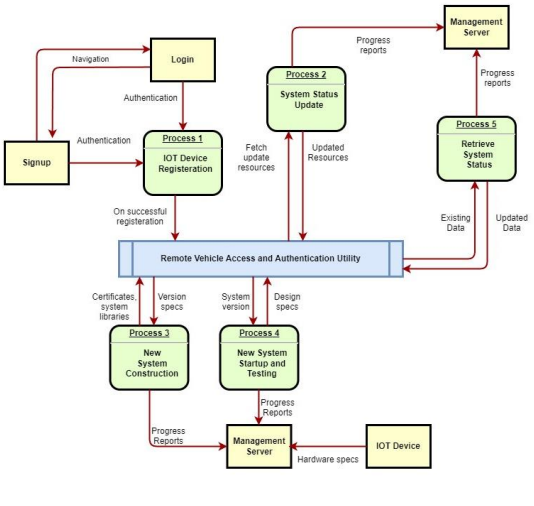

Fig. 1. Data Flow Diagram

C.Integration with Blynk Server

To enable remote control functionalities via a mobile application, the system leverages the Blynk server—a cloud-based platform designed for IoT projects. Within the Blynk environment, a virtual switch (designated as V1) is configured to control the relay module's operation.

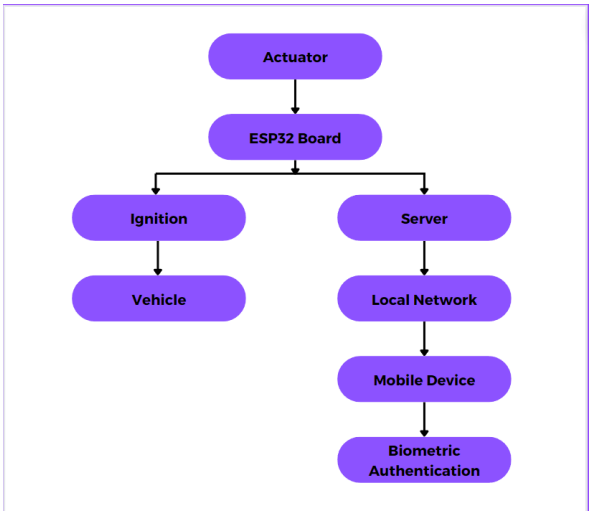

Fig. 2. Hierarchy of RVAA

D. Operational Workflow

The operational workflow of the system begins with user authentication. Before sending any input from the mobile application, users must authenticate themselves through fingerprint or facial recognition methods, ensuring secure access to the system. Upon successful authentication and on receiving the user input, the Blynk server triggers the virtual switch associated with the designated digital pin on the ESP32 board. Alongside this action, the current timestamp is read and stored, capturing the exact moment of ignition control. In response to the Blynk server's signal, the ESP32 board activates or deactivates the relay module, thereby controlling the power supply to the ignition coil. This seamless integration of hardware and software components, combined with timestamped actions and user authentication, enables real-time remote control over the vehicle's ignition system, irrespective of the vehicle's location.

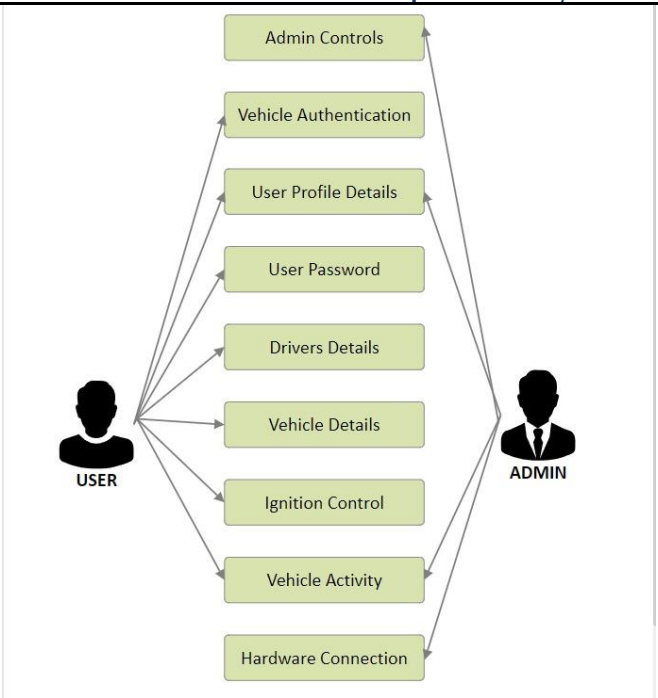

Fig. 3. Use case diagram

E. Data Tracking and User Management with Firebase

Firebase underpins the system's backend, providing robust data storage, analytics, and user management capabilities. It securely stores crucial data such as ignition on/off times, user profiles, and vehicle details. Firebase Authentication facilitates seamless account registration, offering methods like email/password and Google Sign-In. Additionally, fingerprint authentication is integrated to bolster the system's security, ensuring only authorized users can access the vehicle's ignition system.

F. Flutter-based Mobile Interface Development

Harnessing the power of Flutter, a cross-platform framework, we crafted an intuitive mobile interface. This interface offers real-time updates on vehicle status and ignition controls, pulling data from Firebase in real-time. The Flutter-based mobile application provides users with a user-friendly interface to interact with the virtual switch, allowing them to remotely toggle the vehicle's ignition system between on and off states. Push notifications, facilitated by Firebase Cloud Messaging, keep users apprised of critical events.

G. Alternative Platforms and Considerations

While Blynk serves as the primary platform for this project, alternative platforms such as Firebase or Senric Pro can also be considered for achieving similar functionalities. Each platform offers unique features and capabilities, allowing developers to choose the most suitable option based on project requirements and constraints.

IV. RESULTS AND DISCUSSIONS

The implementation of the proposed system, integrating an ESP32-based relay module with the Blynk server for remote vehicle control, yielded promising results in terms of functionality, reliability, and usability. Through rigorous testing and evaluation, the system demonstrated seamless communication between the mobile application and the vehicle's ignition system, allowing users to remotely start or stop the engine with ease.

Performance testing conducted under various scenarios validated the system's robustness and responsiveness, ensuring consistent operation across different network conditions and environmental factors. Feedback collected from users through surveys and usability testing indicated a high level of satisfaction with the system's user interface and overall performance.

Moreover, the integration of alternative platforms such as Firebase or Senric Pro was explored, offering insights into potential enhancements and scalability options for future iterations of the system. While Blynk served as the primary platform for this project, the versatility of the ESP32 board and the modular architecture of the system facilitate seamless integration with alternative platforms to meet diverse project requirements.

Overall, the results of this study underscore the efficacy of the proposed solution in enhancing vehicle security and enabling convenient remote control functionalities. The successful implementation of the system lays the foundation for further research and development in the field of automotive security systems, with the potential to revolutionize remote vehicle control mechanisms and redefine industry standards.

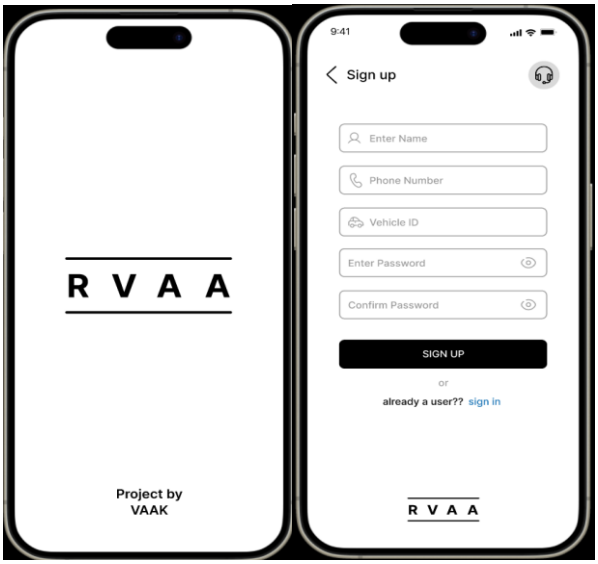

Fig. 4. Onboarding Screens

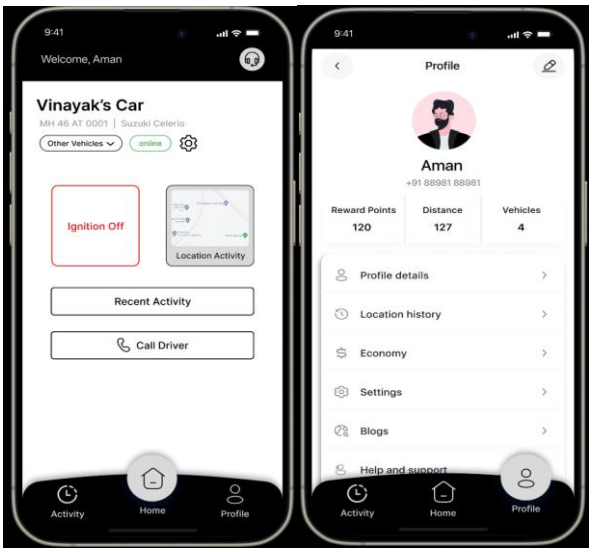

Fig. 5. Home Screen and Profile Screen

V. CONCLUSIONS

In conclusion, the integration of an ESP32-based relay module with the Blynk server offers a comprehensive solution for remote vehicle control, addressing concerns related to vehicle security and unauthorized usage. This paper has explored the system architecture, operational workflow, and alternative platforms, highlighting the potential for advancements in automotive security systems. By leveraging wireless connectivity and cloud-based platforms, this system enhances both security and convenience for vehicle owners, paving the way for future innovations in remote vehicle control mechanisms. As automotive technologies continue to evolve, further research and development in this domain promise to redefine the landscape of vehicular security and remote control functionalities.

REFERENCES

[1] Adeyemi, Ikuesan & Ganiyu, Shefiu & Majigi, Muhammad & Opaluwa, Yusuf & Venter, H.s. (2020). Practical Approach to Urban Crime Prevention in Developing Nations. 1-8. 10.1145/3386723.3387867.

[2] Lyu, Zhihan & Qiao, Liang & Singh, Amit & Wang, Qingjun. (2021). AI-empowered IoT Security for Smart Cities. ACM Transactions on Internet Technology. 21. 1-21. 10.1145/3406115.

[3] Mondal, S., Singh, D. & Kumar, R. Crime hotspot detection using statistical and geospatial methods: a case study of Pune City, Maharashtra, India. GeoJournal 87, 5287–5303 (2022). https://doi.org/10.1007/s10708-022-10573-z

[4] N. Morallo, "Vehicle tracker system design based on gsm and gps interface using arduino as platform", Indonesian Journal of Electrical Engineering and Computer Science, vol. 23, no. 1, p. 258, 2021. https://doi.org/10.11591/ijeecs.v23.i1.pp258-264

[5] Pillai, A. U., Das, P. P., Pawar, D. N., Kotwal, A. N., & Department of Computer Engineering, Late G.N. Sapkal College of Engineering, University of Pune, Nashik, India. (n.d.). Device Verification and Safety using RFID Tag. In International Journal of Scientific Research and Engineering Development: https://www.ijsred.com

[6] Ramani, Raagav & Valarmathy, S. & SuthanthiraVanitha, N. & Selvaraju, Sriram & Thiruppathi, M. & Thangam, R.. (2013). Vehicle Tracking and Locking System Based on GSM and GPS. International Journal of Intelligent Systems and Applications. 5. 86-93. 10.5815/ijisa.2013.09.10.

[7] Said Achmad, Raditya Adinugroho, Nur Safii Hendrawan,Thomas Franklin, IoT Based Vehicle Safety Controller Using Arduino, JURNAL EMACS (Engineering, Mathematics and Computer Science) Vol.5 No.1 January 2023: 1-6

[8] Widjaja, Daniel & Derrick, Derrick & Octaviandra, Muhammad & Achmad, Said & Sutoyo, Rhio. (2022). Important Security Factors for Implementing Internet of Things in Smart Home Systems. 1-7. 10.1109/ICIEE55596.2022.10010228.

[9] Yash Sharma / TIMESOFINDIA.COM / Mar 13, 2024 (2024) One vehicle stolen every 14 mins in Delhi-NCR: Nearly half of stolen cars are Maruti Suzuki - Times of India, The Times of India. Available at: https://timesofindia.indiatimes.com/auto/cars/one-vehicle-stolen-every-14-mins-in-delhi-ncr-nearly-half-of-stolen-cars-are-maruti-suzuki/articleshow/108456054.cms (Accessed: 20 March, 2024).