*Technoscience Journal for Community Development in Africa* 3 (2024) 167-174
ISSN 2659-0573

*Research Article*

# Development of a secured ignition and notification for an anti-theft vehicle detection system using one-time password

**Bem Sombo[1,*], Simon Tooswem Apeh[1], Edoghogho Olaye[1], Jumoke Falilat Ajao[2], Lukman Adewale Ajao [3]**

[1]Department of Computer Engineering, University of Benin, Benin City, Nigeria
[2]Department of Computer Science, Kwara State University, Malete, Nigeria
[3]Department of Computer Engineering, Federal University of Technology, Minna, Nigeria

**Abstract*:*** Criminals have devised various ways to steal vehicles by exploiting the loopholes associated with the vehicle anti-theft detection systems, and this has become a threat to vehicle owners. This paper aims to put forward an embedded system-based secured ignition and notification of an anti-theft vehicle detection system. The applied research was carried out to develop an embedded anti-theft vehicle detection system using an ESP32 microcontroller as a control unit. The control unit was programmed to control the peripheral devices interfacing, in line with the designed security functionalities of the system. The ignition vehicle system is secured to prevent unauthorized users using One-Time Password (OTP), and coded ignition key. The system is tested, and the response reveals the identity of the intruder through the SMS, and alarm system about the suspected unauthorized user. It is expected that this technology will assist in preventing the theft of a vehicle in the society.

**Keywords:** Anti-theft system, Microcontroller, One-time Password, Security, Vehicle Notification

## 1. INTRODUCTION

An anti-theft security system is a technology designed to protect cars from theft or unauthorized access, and it comprises various components that are used to prevent unauthorized users, thieves, and others related to theft from stealing vehicles (Aliyu et al. 2019; Bukola, 2020). These anti-theft car security systems employ advanced technology-based Internet of Things (IoT) such as the Global Positioning System (GPS), Global System for Mobile (GSM) communication, Radio Frequency Identification (RFID), biometrics, among other technologies to secure cars from theft (Inalegwu et al. 2018; Dang et al. 2021; Das et al. 2021). Other technologies involved are a surveillance wireless camera, bluetooth, and a one-time password to secure the ignition system of a car and notify the owner about unauthorized access (Ajao et al. 2018; Omer et al. 2020).

However, the ignition system plays a significant role in the prevention of unauthorized user access to the car operation and can be properly secured to prevent vehicle theft (Alsayaydeh et al., 2019; Sanwat et al., 2021; Ahmed et al., 2022). An Ignition system can be defined as the rapid combination of hydrogen and carbon in the fuel with oxygen mixture to generate energy in the form of heat (Stadler et al., 2019; Patane et al., 2020; Umar et al., 2020). This ignition system generates a very high voltage from the vehicle's battery and creates a spark to ignite the fuel-air mixture in the engine's combustion chamber, to start a vehicle's engine (Shu et al., 2022) as illustrated in Figure 1. Therefore, a vehicle ignition system is a good approach for securing vehicles from theft. The traditional vehicle ignition key employed this technique to prevent stealing of the vehicle which has become a criminal practice. Several kinds of vehicle anti-theft systems mechanical locks, alarms, vehicle immobilizers, biometric systems, GPS tracking systems and computer-controlled electronic systems have been developed over the years to tackle the stealing of vehicles (Ajao et al., 2020; Claude et al., 2021).

*Corresponding author's:
Email: sombopeter@gmail.com

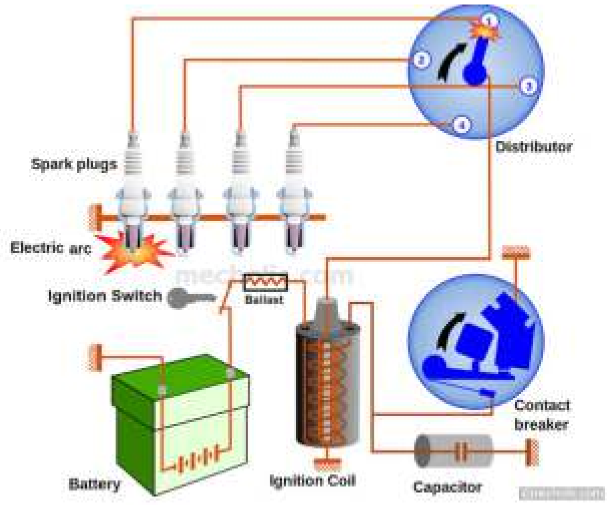

Figure 1: Overview of the Vehicle Ignition System

Consequently, the innovation of a vehicle security system generally reduces the trend of vehicle theft at the initial stage, but it is consequently defeated by criminals once they have identified the system's loophole (Jimoh et al., 2020; Dixon & Farrell, 2020). From 1960 to 1991, car theft has increased five-folds peaking at 1,661,738 cars stolen in 1991. Since then, car theft began falling, with 699,594 cars reported stolen in 2013. Over the past 22 years (1991 - 2013), vehicle theft rates dropped sharply until the year 2000, and rose slightly in 2004 (Hodgkinson & Andresen, 2020). The average dollar loss per theft was $7,680 and motor vehicles were stolen at a rate of 236.9 per 100,000 people in 2016. Preliminary data from the Federal Bureau of Investigation review that in the first half of 2017, vehicle theft increased by another 4.1%, and the statistical trend of vehicle theft from 1960 to 2017 (Circo & Scranton, 2020; Sundt, 2022) is presented in Figure 2. Therefore, this research contributes to knowledge by developing a robust and secured anti-theft vehicle system using a one-time password (OTP) approach for starting the ignition, which is programmed and embedded into the ignition car key, and multifactor authentication components.

The rest of the paper is organized as follows: section 2 discussed related works to the vehicle anti-theft systems, and the summary was presented in a meta-analysis table. Section 3 presented the methodology, which includes the system implementation architecture, and unauthorized user detection algorithm. Section 4 presents and discussed the results of the proposed system. Section 5 concludes the research work.

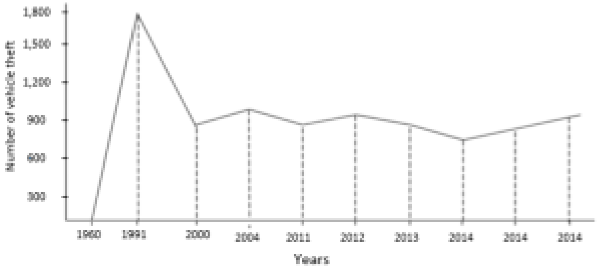

Figure 2: Statistical Analysis of Vehicle Theft Trend

## 2. RELATED WORKS

Balakrishnan et al. (2022) presented a paper on the topic: Vehicle Anti-theft Face Recognition Systems, Speed Control, and Obstacle Detection Using Raspberry Pi. The Raspberry Pi 4B technology was utilized in this study to develop a dual-purpose system for securing vehicles from theft using face identity verification and for obstacle avoidance using a pi-camera and ultrasonic sensors. The proposed system allow only validated users access to the vehicle and the vehicle stops on detection of an obstacle in the given range. Although the system have false acceptance and false rejection ratios. Das et al. (2021) proposed a decentralized vehicle anti-theft system using blockchain and smart contracts. Blockchain technology was used to implement a vehicle anti-theft system that can authorize more than one person to drive a vehicle without hampering the vehicle data and maintaining security. From the experimental results and comparative analysis of the system, it has been revealed that the blockchain technology provides a transparent way to reduce the possibility of personal information leakage and improves the vehicle's anti-theft system's safety. However, scratches on the fingerprint scanner can lead to the inefficiency of the system.

Bukola (2020) presented the development of an anti-theft vehicle security system using GPS and GSM technology with biometric authentication. The GPS, GSM and biometric technologies were utilized. The system secures a vehicle from authorized users and accepts the SMS commands to immobilize and demobilize a vehicle, although it will have false acceptance and rejection ratios and cannot work efficiently in areas without mobile networks and GPS signals can be blocked. Virmani et al. (2019) worked on a smart anti-theft system for vehicles using mobile phones. The SMS technology was employed for controlling the vehicle engine via mobile phone. The proposed system authenticates the owner every time it senses an ignition and it gives the owner remote access to control his/her vehicle's engine function. However, the system cannot efficiently work in areas without a mobile network and cannot reveal the identity of an unauthorized user.

Ramesh et al. (2019) proposed a biometric vehicle security system. The system employs fingerprint and wearable car orbit for validating and granting access to authorized vehicle users. It can reject unauthorized vehicle users; however, it will have low accuracy if scratches develop on the fingerprint scanner, it also has a false acceptance and rejection ratio. Mendoza (2017) developed a microcontroller-based vehicle security system with tracking capability using the GSM and GPS technologies. The system tracks the location of the vehicle and alerts the vehicle owner and public when vibration is detected around the vehicle via SMS and alarm respectively, although the GPS signals can be blocked. Chaudhari et al (2016) put forward a vehicle theft control system. The system was built on the GPS and GSM technology. It constantly watches a moving vehicle and reports the status on demand and allows the vehicle owner to remotely turn off the vehicle via SMS. However, the system will become inefficient when the GPS signals are blocked, and the GSM network is not available. Lokol et al. (2015) proposed a microcontroller-based smart card car security system. The system grants users access to start a vehicle by scanning and verifying the user's smart card and calls a vehicle owner when an invalid card is detected three consecutive times, although the smart card can easily be stolen.

Singh and Tejaswi (2013) presented a real-time vehicle theft identity and control system based on ARM 9. The system employed facial recognition technology for granting access to authorized (registered) users. The system demobilizes a car's engine and sends the message and current location of a vehicle to the vehicle owner when an unauthorized user is detected. However, it has a false acceptance and rejection ratio of users. The summary of the related work is presented in Table 1, and the comparative analysis of the secured ignition and anti-theft vehicle detection is presented in Table 2.

Table1: A Meta-Analysis Table for Literature on Vehicle Anti-Theft Systems

| S/N | Author | Methodology | Strength | Limitation |
|---|---|---|---|---|
| 1. | Balakrishnan et al., 2022 | Face recognition, ultrasonic sensor, and Pi camera technologies were employed. | The system secures a vehicle from unauthorized users. | Face recognition is associated with false acceptance and false rejection ratios. |
| 2. | Das et al., 2021 | Blockchain and fingerprint technologies were used to implement a vehicle anti-theft system. | It reduces the possibility of personal information leakage and improves the vehicle anti-theft system's safety. | Scratches on the fingerprint scanner can result to system inefficiency. |
| 3. | Bukola, 2020 | GPS, GSM and biometric technologies were employed. | The system secured a vehicle from authorized users and accepts SMS commands to immobilize and demobilize a vehicle. | GPS signals can be blocked. A vehicle will only be immobilized in the areas with mobile network coverage. |
| 4. | Virmani et al., 2019 | SMS technology was employed for controlling the vehicle engine via mobile phone. | The owner has remote access to control his/her vehicle's engine function. | The system works only in areas with mobile network. |
| 5. | Ramesh et al., 2019 | The system employs fingerprint technology for validating authorized users. | It has the ability to reject unauthorized vehicle users. | Scratches on the fingerprint scanner dramatically affect s the performance of the system. |
| 6. | Mendoza, 2017 | GSM and GPS technologies were employed to develop a vehicle anti-theft system. | It tracks the location of a vehicle and alerts the owner and the public when vibration is sensed around the vehicle. | GPS signals can be blocked. It will have a high rate of false alerts. |
| 7. | Chaudhari et al., 2016 | GPS and GSM technologies were employed. | It reports a vehicle's status on demand. The owner can remotely demobilize a vehicle via SMS. | The system is efficient only in areas with mobile network coverage. GPS signals can be blocked. |
| 8. | Lokol et al., 2015 | The smart card technology was employed for validating an authorized user. | It authorizes only users with valid smart card. | Smart cards can easily be stolen. |
| 9. | Singh & Tejaswi, 2013 | Facial recognition technology was employed for granting access to authorized (registered) users. | It denies access to unauthorized users and alerts the vehicle owner. | Facial recognition is associated with false acceptance and false rejection ratios. |

## 3.0 MATERIALS AND METHODS

The proposed system employs bi-factor authentication methods with the bluetooth technologies, which are interfaced with microcontrollers to secure the vehicle ignition system from unauthorized user. This secured car ignition and anti-theft vehicle detection system is designed to accept a valid password from a user and respond by sending OTP to a user's mobile device through the GSM module. The system responds to an invalid password operation by alerting the authentic car owners about a suspected intruder and triggers an alarm for two consecutive attempts. The secured car ignition and anti-theft detection system incorporate a dual-layer authentication mechanism for authorized car users using both a static password and a one-time password (OTP) for authorization. When a valid password is provided, the system generates an OTP which is then sent to the user's mobile phone. Upon entering the password, the system captures the user's picture and forwards it to the vehicle owner. However, in the event of an invalid password being provided, the system sends an SMS alert to authorized users. If the invalid password attempts occur twice or more, both authorized users and the public are alerted through SMS with an alarm system respectively. But once a valid OTP is provided, the system grants the user access to start the car using the ignition key. This system allows the car owner to remotely control the vehicle's security through SMS. The detailed principle of the system operation flowchart is presented in Figure 3.

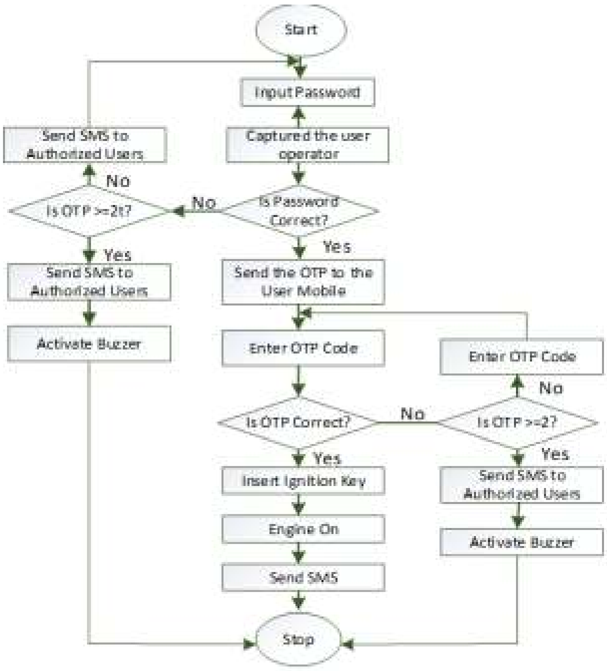

**Figure 3:** Secured Ignition and Anti-theft Vehicle Detection System Flowchart

### 3.1 System Design and Implementation

The secured ignition and anti-theft vehicle detection system is developed and implemented through the integration of several embedded security components, a wireless system, a communication module, and a microcontroller chip as in the block diagram presented in Figure 4. This secured ignition and anti-theft vehicle detection system utilized a low-power integrated both Wi-Fi and dual-mode Bluetooth technology on a microcontroller chip called ESP8266 processor. The controller chip helps to control and coordinate all the activities performed on the system. This system consists of a 4*4 keypad which serves as an input to enter the password code for the user authorization to the vehicle key ignition control, while the liquid crystal display (LCD) was used as the display unit system. The fuel pump and ignition are connected to the car starter relay switch with solenoid for remote control, and to regulate the high-current flow in the circuit, which both are connected to the microcontroller chip. The system also consists of a GSM module for the communication of remote information/messages through a universal asynchronous receiver and transmitter (USART) port. The wireless module which includes the bluetooth technology and a camera is also integrated into the controller chip for the purpose of authorized or unauthorized image capturing and transmission to the user through the GSM module or Bluetooth. The complete circuit diagram of the secured ignition and anti-theft vehicle detection is presented in Figure 5.

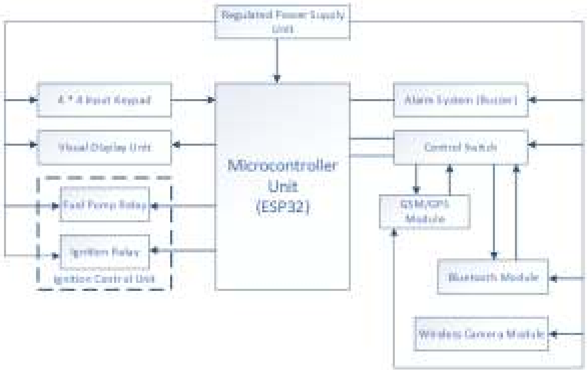

Figure 4: Block Diagram of the Secured Ignition and Anti-theft Vehicle Detection System

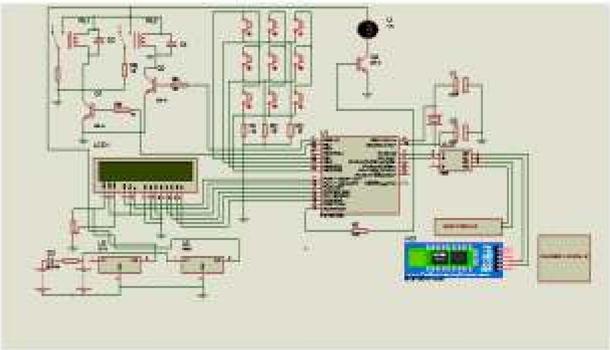

Figure 5: Architecture of the Secured Ignition and Anti-theft Vehicle Detection System

### 3.2 Software Design and Coding

The programming of secured ignition and anti-theft vehicle detection system is achieved in the Arduino Interface Development Environment (AIDE) and linked to the Adafruit IO for storing information. Also, to fetch the stored information remotely, the RESTful Hyper-Text Transfer Protocol (HTTP) was used. A one-time password is developed and implemented in this environment to secure ignition key authentication. This password is timely generated on the user's request and expired based on the validity. The OTP used in this work adopts a cryptographic hashing algorithm that uses a one-way function for the arbitrary generation to a fixed-length message digest. The OTP begins the process with synchronization of input parameters, or secret key or PIN, runs the input functions through a one-way function, and to generates a fixed length of the password. The details process of generating OTP is illustrated in Figure 6, and the flowchart is presented in Figure 7.

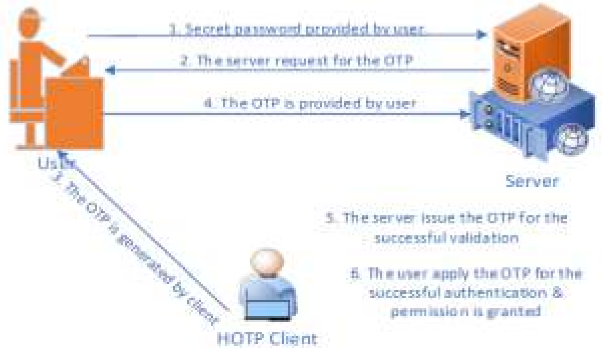
1. Secret password provided by user
2. The server request for the OTP
4. The OTP is provided by user
User
Server
3. The OTP is generated by client
5. The server issue the OTP for the successful validation
6. The user apply the OTP for the successful authentication & permission is granted
HOTP Client

Figure 6: Generation of OTP Architecture

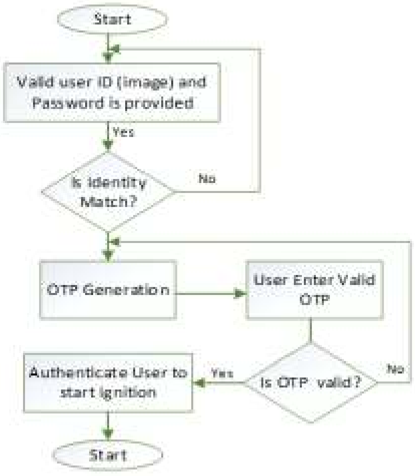

Figure 7: Flowchart of a Secured Ignition Car Key Using OTP

## 4. RESULTS AND DISCUSSION

The secured ignition and anti-theft vehicle detection are designed and implemented using an ESP32 microprocessor for the control of the system activities. Other discrete components and modules were tested individually to ascertain their design and workability before incorporating them into a single system unit. At each stage of a component interfaced with the microcontroller, a test was carried out to ensure the designed objective was achieved. The entire system was tested and it worked satisfactorily. Figures 8 and 9 illustrate the developed prototype of secured ignition and notification of anti-theft vehicle detection. However, during the system testing, it was observed that the secured ignition and notification of the anti-theft vehicle detection system were able to deny unauthorized users access from starting the ignition vehicle due to the wrong password provided. So, the ignition system of a vehicle cannot be started with the ignition key without undergoing the authentication processes. Also, the bi-factor authentication methods used based on the OTP and image were tested and they responded on time. The system captures and sends a picture of the insider to the authorized user during the password entry. The reviewed picture of the intended user/intruder gives a vehicle owner the idea of the person in charge of his or her vehicle. When an unauthorized person is found to have access to the vehicle, the owner can remotely turn off the vehicle and proceed to take appropriate security actions.

But, when an invalid password is entered, the system alerts the authorized users of an intruder attempt and allows a second attempt for valid password entrance. If the second attempt fails, the system alerts the authorized users again with the same message and triggers an alarm to call the attention of the public. However, when a valid user password is used, the system sends an OTP to the user's mobile phone and requested for the sent OTP to be entered. The stage of user password authentication forms the first-level user authentication. The second level of user authentication involves the system's request for a valid OTP. If a wrong or invalid OTP is entered, the system alerts the authorized users of an intruder and at the same time, triggers an alarm. The system response during testing was presented in Table 2.

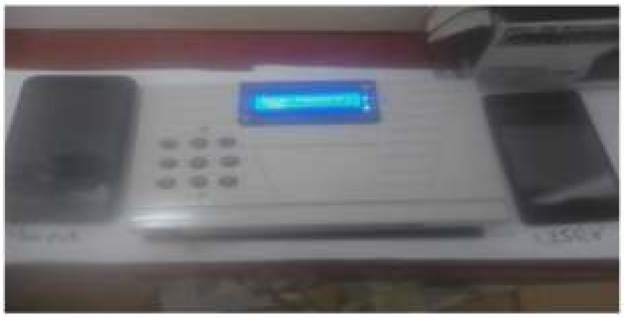

Figure 8: Secured Ignition and Notification of Anti-theft Vehicle Detection System Prototype

Figure 9: The Secure Anti-theft Vehicle Detection System Interface with Mobile Phone

**Table 2.** Secured Ignition and Notification of Anti-theft Vehicle System Response Information

| S/N | User's Action | System Response |
|---|---|---|
| 1. | Commencement of password entrance by an intended user | The system captured and sent the picture of the intended user to the vehicle owner |
| 2. | Valid password entered | OTP sent to the user's mobile phone via Bluetooth technology |
| 3. | Valid OTP entered | Insert the ignition key displayed on the LCD |
| 4. | The ignition switch turned to the ON position with the ignition key | The vehicle engine turned ON |
| 5. | Off SMS sent with a customized mobile phone | The vehicle engine turned off |
| 6. | The ignition switch turned to the ON position with the ignition key | Enter the password displayed on the LCD |
| 7. | Invalid user password entered once | The system alerts all authorized users of an intruder attempt |
| 8. | Invalid user password on two attempts or wrong OTP entered | The system alerts all authorized intruder detection and triggers an alarm. |

## 5. CONCLUSION

The secured ignition and notification of an anti-theft vehicle detection system are developed using ESP 32 microcontroller system to coordinate the system activities. This controller system was interfaced with the 4 by 4 keypad to allow users input a password. The GSM module and Bluetooth-technology module were integrated for remote communication and users' notification about the vehicle status. Also, the buzzer is integrated for public alertness and awareness about vehicle theft activities. Therefore, the OTP embedded as a security measure plays a significant role to caution unauthorized users to attempt vehicle stealing through the ignition of the car. Several modules integrated were tested and they functioned properly with a fast response time. However, the developed anti-theft vehicle detection system demonstrated the capabilities of securing vehicle ignition from unauthorized users, and notifying users, and the public about unauthorized users' access through system alarms and SMS. The performance of the developed anti-theft vehicle detection system will greatly discourage the theft of vehicles, in our society.

## REFERENCES

Ahmed, A. I., Sharf, S. H., Salama, R. A., Mekky, M. A., Salama, M. A., & Badawy, W. (2022, March). A Reliable Secure Architecture for Remote Wireless Controlling of Vehicle's Internal Systems based on Internet of Vehicles using RF and Wi-Fi. In 2022 5th International Conference on Computing and

Informatics (ICCI) (pp. 257-262). IEEE.

Ajao, L. A., Kolo, J. G., Adedokun, E. A., Olaniyi, O. M., Inalegwu, O. C., & Abolade, S. K. (2018). A smart door security-based home automation system: internet of things. *SciFed Journal of Telecommunication*, 2(2), 1-9.

Ajao, L. A., Abisoye, B. O., Jibril, I. Z., Jonah, U. M., & Kolo, J. G. (2020, August). In-vehicle traffic accident detection and alerting system using distance-time-based parameters and radar range algorithm. In *2020 IEEE PES/IAS PowerAfrica* (pp. 1-5). IEEE.

Aliyu, S., Yusuf, A., Abdullahi, U., Hafiz, M., & Ajao, L. A. (2019, September). Smart Protection of Vehicle using Multifactor Authentication (MFA) Technique. International Engineering Conference (IEC).

Alsayaydeh, J. A. J., Indra, W. A., Khang, W. A. Y., Shkarupylo, V., & Jkatisan, D. A. P. P. (2019). Development of vehicle ignition using fingerprint. *ARPN Journal of Engineering and Applied Sciences, 14*(23), 4045-4053.

Balakrishnan, B. Suryarao, P. Singh, R. Shetty S. & Upadhyay, S. (2022). Vehicle Anti-theft Face Recognition System, Speed Control and Obstacle Detection using Raspberry Pi. 1-5, doi: 10.1109/ROMA55875.2022.9915691.

Bukola, A. (2020). Development of an anti-theft vehicle security system using GPS and GSM technology with biometric authentication. *International Journal of Innovative Science and Research Technology. 5*(2). 1250 – 1260.

Chaudhari, C. Jahagirdar, S. & Bagwan, S. (2016). Vehicle Theft Control System. *International Journal of Engineering Science and Computing*, 6(4), 4602 - 4603.

Circo, G., & Scranton, A. (2020). Did Connecticut's "Raise the Age" Increase Motor Vehicle Thefts? Criminal Justice Policy Review, 31(8), 1217-1233.

Dang, T., Gupta, V., Wadia, D. S., Kohli, P., & Chahal, R. K. (2021, March). Face Ignition: An automatic anti-theft and keyless solution for vehicles. In 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 248-253). IEEE.

Das, D., Banerjee, S., Ghosh, U., Biswas, U., & Bashir, A. K. (2021). A decentralized vehicle anti- theft system using Blockchain and smart contracts. Peer-to-Peer Networking and Applications, 14(5). 2775–2788. doi:10.1007/s12083-021-01097-3

Dixon, A., & Farrell, G. (2020). Age-period-cohort effects in half a century of motor vehicle theft in the United States. Crime science, 9(1), 1-17.

Hodgkinson, T., & Andresen, M. A. (2020). Show me a man or a woman alone and I'll show you a saint: Changes in the frequency of criminal incidents during the COVID-19 pandemic. *Journal of criminal justice, 69,* 101706.

Inalegwu, O. C., Maliki, D., Ajao, L. A., & Abu, A. D. (2018). Fingerprint-based driver's identification system. 2nd International Conference on Information and Communication Technology and Its Applications (ICTA 2018).

Jimoh, O. D., Ajao, L. A., Adeleke, O. O., & Kolo, S. S. (2020). A vehicle tracking system using greedy forwarding algorithms for public transportation in urban arterial. *IEEE Access*, *8*, 191706-191725.

Lokol, A. Z., Bugaje, A.I. & Abdullahi, U. (2015). Microcontroller Based Smart Card Car Security System. *International Journal of Engineering Trends and Technology*, 29(3), 150 - 153.

Omer, S., Sohelrana, K., Tamkeen, A., & Rasheed, M. A. (2020, March). Real time application of vehicle anti-theft detection and protection with shock using facial recognition and iot notification. In 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1039-1044). IEEE.

Mendosa, O.F. (2017). Microcontroller Based Vehicle Security System with Tracking

Capability using GSM and GPS Technologies. *Asia Pacific Journal of Multidisciplinary Research.* 5(2). 114-120.

Sawant, N., Sutar, S., Ghumare, G., & Itole, M. D. (2021). Fingerprint-based car ignition system using arduino and rfid. *International Journal, 6*(5).

Patane, P., & Nandgaonkar, M. (2020). Multipoint laser ignition system and its applications to IC engines. Optics & Laser Technology, 130, 106305.

Ramesh, M., Akruthi, S., Nandhini, K., Meena, S., Gladwin, S. J., & Rajavel, R. (2019, November). Implementation of vehicle security system using gps, gsm and biometric. In *2019 Women Institute of Technology Conference on Electrical and Computer Engineering (WITCON ECE)* (pp. 71-75). IEEE.

Singh, D. N., & Tejaswi, K. (2013). Real time vehicle theft identity and control system based on ARM 9. *International Journal of Latest Trends in Engineering and Technology,* 2(1), 240 - 245.

Singh, P., Sethi, T., Biswal, B.B. & Pattanayak, S. K. (2015). A Smart Anti-Theft System for Vehicle Security. *International Journal of Materials, Manufacturing,* 3(4), 249 - 254.

Stadler, A., Wessoly, M., Blochum, S., Härtl, M., & Wachtmeister, G. (2019). Gasoline-fueled pre-chamber ignition system for a light-duty passenger car engine with extended lean limit. *SAE International Journal of Engines, 12*(3), 323-340

Sundt, J. (2022). Clarifying the effect of California Realignment on motor vehicle theft: results of an interrupted time series. *Journal of Experimental Criminology, 1-9*.

Umar, B. U., Olaniyi, O. M., Ajao, L. A., Maliki, D., & Okeke, I. C. (2019). Development of A Fingerprint Biometric Authentication System for Secure Electronic Voting Machines. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 115-126.

Virmani, D., Agarwal, A., & Mahajan, D. (2019). Smart anti-theft system for vehicles using mobile phone. Smart Innovations in Communication and Computational Sciences: Proceedings of ICSICCS 2017, Volume 1. 265-278.

Zhu, S., Akehurst, S., Lewis, A., & Yuan, H. (2022). A review of the pre-chamber ignition system applied on future low-carbon spark ignition engines. Renewable and Sustainable Energy Reviews, 154, 111872.