Novelty Journals

ISSN 2394-9678

International Journal of Novel Research in Electrical and Mechanical Engineering
Vol. 11, Issue 1, pp: (68-75), Month: September 2023 - August 2024, Available at: www.noveltyjournals.com

Design and Evaluation of a Code-Based Immobilizer System for Vehicle Anti-Theft Security

ILUNGA WA LUNDA ARIEL

Department of Electronics and Computer Science Institut Supérieur Pédagogique et Technique /Likasi (ISPT/Likasi)

DOI: https://doi.org/10.5281/zenodo.10473430

Published Date: 09-January-2024

***Abstract*: This paper focuses on the design and realization of an electronic immobilizer with an embedded system for the safety of vehicles without embedded security system. This study starts from the lack of reliability presented by the use of mechanical ignition keys as a vehicle safety measure. This measure is only a matter of keeping the ignition key safe from any threat given the speed at which a key can be reproduced nowadays. However, thanks to the advent of processors and microprocessors which can be easily integrated into any device, digital electronics today are capable of offering much more than a mechanical security measure based on a key. This paper therefore addresses the question of the security problem of vehicles from an electronic perspective, it is based on the flexibility of operation and the easy integration of programmable microcontrollers for the management of vehicle start authorization by electronic password authentication system. The result of this research shows that under certain conditions this system can improve vehicle safety but presents some flaws under other conditions.**

***Keywords*: immobilizer, anti-theft, embedded system, digital code system, security.**

I. INTRODUCTION

Nowadays, automobile safety has become one of the major concerns of vehicle manufacturers and owners. However, some vehicles on the automobile market are not equipped with sophisticated security systems for their safety. Some recent vehicle models are equipped with an immobilizer computer while others are not. Those that do not have immobilizer systems only have a mechanical security system based on the ignition key. Each vehicle launched on the market has its own unique key, and a vehicle is not supposed to be able to start with a key that is not its own under any circumstance. In theory this security measure is designed to be implemented flawlessly, but in reality this is not always the case according to the various cases of vehicle theft reported [1]. This gap between what is and what should be therefore raises an important question which is how to improve the safety of vehicles already launched on the market. Hence we propose this article which consists of designing and evaluating an immobilizer system for the security of vehicles that do not have an electronic security system.

Many researchers have studied automobile safety, they worked on geolocation systems (GPS trackers), anti-theft deterrent systems, remote engine cut-off by calling, etc. Their work was limited to designing and producing the security system without mounting it on a vehicle to test it in real (concrete) situation. Their tests simply consisted of using LEDs and other types of actuators replacing a real vehicle engine. In our case we are studying a code-based system with a secret digital code to be entered on a keyboard to secure vehicles. To do this, our investigation follows a methodological approach which is based on experimental data from the analysis of vulnerabilities of concrete vehicles without a security system before and after the production of our system (solution).

The objectives of this work are: (1) Analyze security vulnerabilities on vehicles without an immobilizer; (2) analysis of general aspects related to internal combustion engines by focusing on the common elements found on all engines in order to identify actions and strategic points for the location of our immobilizer; (3) Design a car immobilizer system to improve the safety of vehicles not equipped with an immobilizer; (4) Evaluate the system on a real vehicle under different scenarios to ensure its contribution to vehicle safety.

Novelty Journals

ISSN 2394-9678

International Journal of Novel Research in Electrical and Mechanical Engineering
Vol. 11, Issue 1, pp: (68-75), Month: September 2023 - August 2024, Available at: www.noveltyjournals.com

II. LITERATURE REVIEW

[2], [3] and [4] offer security systems based on GSM and GPS technologies for geolocation and sending alert notifications in the event of attempted theft of the vehicle. The difference between these 3 works is that [2] uses a barcode system to be scanned before starting the vehicle; thus, a bad barcode scanned triggers the sending of an alert notification to the owner by SMS, while a correct barcode authorizes the vehicle to start. [3] uses biometric fingerprint technology to gain access to startup; the fingerprints of the users authorized to start the vehicle are stored in the system memory. Thus, each time a fingerprint is scanned it is compared to the fingerprints recorded in the system, if recognized, the system authorizes starting, otherwise it sends an SMS alert to the owner as well as the geographical coordinates of the vehicle. And [3] offers mobile app-based startup access; only the person with the application can manage access to the starting system via Bluetooth connection. In the event of an attempt to start without having activated the system, the latter sends an SMS alert to the owner.

IoT being a key technology at the heart of the transmission and control of objects remotely via the Internet, [5], [6], [7] and [8] present systems based on IoT capable of stopping the engine remotely, control access to start, track the vehicle, etc. For their system they mainly proposed authentication based on RFID technology and digital code technology. For the case of RFID, the driver must first scan the appropriate RFID card on an onboard scanner in the vehicle. The system will send an access request notification to the mobile application of the owner and the latter will take care of grant or deny access. As for the password one it uses a keypad present in the vehicle to enter a password on the vehicle side and a mobile application to enter another password. The system can only be activated if the two passwords entered (on the phone and on the application) are correct.

Other researchers propose immobilizer systems using facial recognition [9], Fog Computing [10] and other technologies [11], [12]. Their systems are capable of controlling different components or parameters of the vehicle remotely such as the fuel pump, vehicle speed, doors, windows, etc. some of them are also able of taking videos, recording sounds inside the vehicle, as well as tracking, sending notifications and making calls.

As mentioned in our introduction, all this work is focused on the design of security systems using different technologies to protect vehicles against theft. The result of this research shows that it is possible to create vehicle immobilizer security systems with several different technologies. However, nothing in this work indicates the exact contribution of the proposed systems to improving security. Our article therefore focuses on the evaluation of the contribution of immobilizer systems to the anti-theft security of vehicles given that others have already proven that several technologies can facilitate the implementation of such a system.

III. METHOD/ APPROACH

This research was mainly based on the experimental method which consisted of analyzing the security aspect of vehicles without security systems as well as the operation of car engines. We analyzed the starting systems on two levels: With ignition key and without ignition key; subsequently we analyzed the importance of the key elements for the proper functioning of a gasoline engine.

3.1 Security analysis

3.1.1 Starting with ignition key

Starting with the ignition key is done by inserting the specific key of the vehicle into the Neiman in the “LOCK” position, then turning it to the “START” position clockwise as shown in Figure 1.

Figure 1: View of a car Neiman

Novelty Journals

ISSN 2394-9678

International Journal of Novel Research in Electrical and Mechanical Engineering
Vol. 11, Issue 1, pp: (68-75), Month: September 2023 - August 2024, Available at: www.noveltyjournals.com

This action is supposed to be possible only with the appropriate vehicle ignition key. To verify this, we used 4 vehicles of different brands on which we carried out starting tests with 3 different keys taken randomly illustrated in Figure 2.

Figure 2: Capture of keys used for vehicle starting test

1: Key of a TVS motorcycle 2: Key to a door lock 3: Key of a Suzuki Jimmy

The vehicles used to carry out this test are given in Figure 2.

Figure 3: Images of the vehicles used in the tests

3.1.2 Starting without ignition key

Apart from starting with an ignition key, we have also conducted experiments to see if a vehicle designed to be started with an ignition key can be started without a key by bypassing the key system. To do this we removed the Neiman ignition switch from its aluminum cylinder as shown in Figure 4 and then tried to start the vehicle directly from there without an ignition key.

Figure 4: Image of a disassembled Neiman contactor

3.2 Analysis of the components of an internal combustion engine

For the gasoline engine we analyzed the ignition circuit and the injection circuit. We analyzed the ignition circuit first by disconnecting one spark plug, then 2, 3 and 4 while trying to start the engine at each disconnection step. Then we analyzed the injection system by gradually disconnecting the injectors as shown in Figure 5, while trying to start the vehicle. In the same context we also removed the relay and the Fuel Injection fuse (FI).

Novelty Journals

ISSN 2394-9678

International Journal of Novel Research in Electrical and Mechanical Engineering
Vol. 11, Issue 1, pp: (68-75), Month: September 2023 - August 2024, Available at: www.noveltyjournals.com

Figure 5: View of the engine with 2 injectors disconnected

To the conducted analyzes above we added a study of some sensors present on a Suzuki M13A engine to find out if they have an impact on the starting of an engine. We disconnected the camshaft sensor (1), crankshaft sensor, throttle position sensor (2) and air flow sensor (3) in turn as shown in Figure 6.

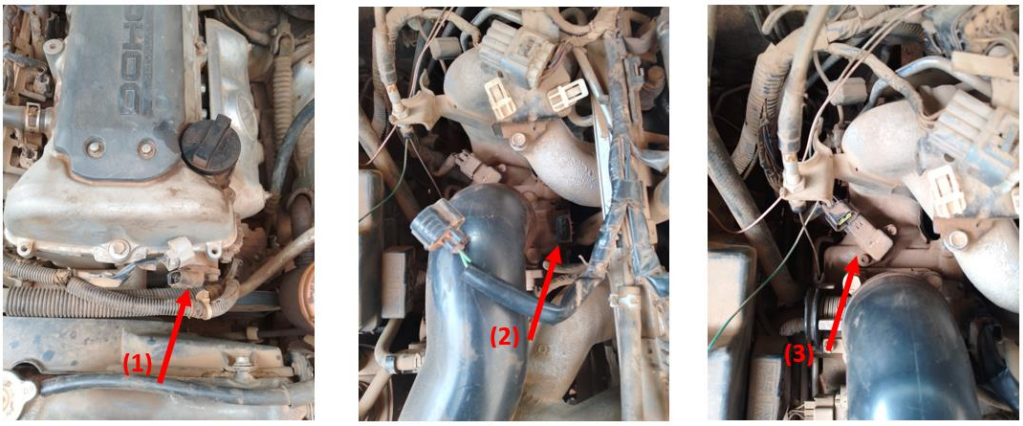

Figure 6: Pictures of 2004 Suzuki M13A engine with disconnected sensors

3.3 Design of the immobilizer

The block diagram of the system that we designed is given in Figure 7. This system has 4 main components which are: a keypad for entering the secret password, a processing unit, a display for interacting with the system and a relay module as pre-actuator.

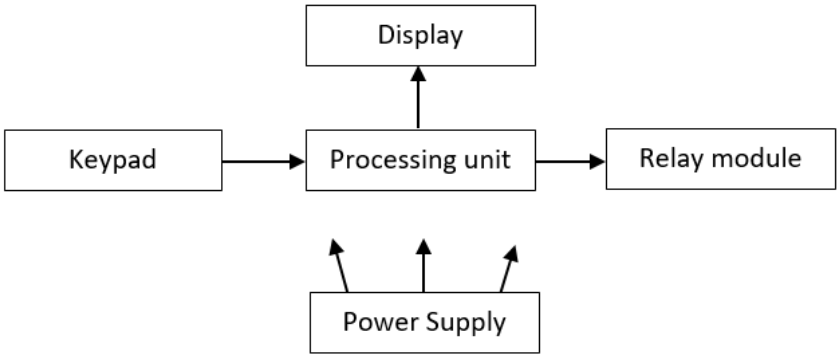

Figure 7: Block diagram of the proposed system

a. Keypad

We used the 4x4 matrix keypad given in Figure 8. We used 9 numeric keys to type the password, the “Ent” key as “OK”, the “F1” key as menu, the “Esc” key like “Cancel” and direction keys for navigation.

Novelty Journals

ISSN 2394-9678

International Journal of Novel Research in Electrical and Mechanical Engineering
Vol. 11, Issue 1, pp: (68-75), Month: September 2023 - August 2024, Available at: www.noveltyjournals.com

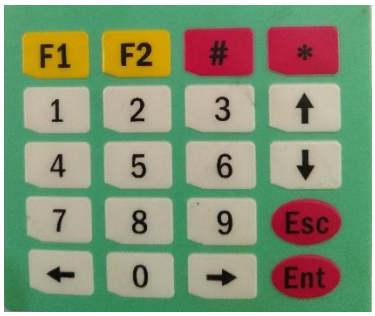

Figure 8: View of the Keypad used for the proposed system

b. Other components

Other components used in the implementation of our system are given in Table 1 below:

Table 1: List of key components used

N°	BLOCK	COMPONENT
1	Processing Unit	Arduino UNO
2	Relay module	8 Channels relay module
3	Display	16x2 LCD display with I2C module

The system operation algorithm is given in Figure 9 Below:

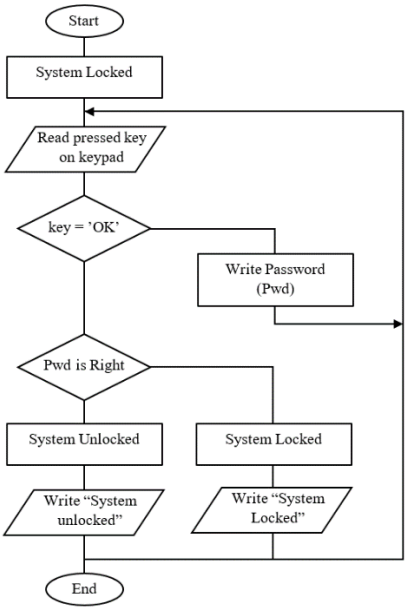

Figure 9: Operating algorithm of our immobilizer

Apart from the lock and unlock function, the system also includes the change password function and the alert function (for deterrence) in case of an attempt with a wrong password.

3.4 System evaluation

For the evaluation of our system we gave the vehicle on which we installed our system to 5 different persons including 2 drivers and 3 mechanics to whom we asked to start the car according to 2 scenarios: (1) by not telling them that there is a security system and the keypad is just a device for managing the vehicle's air conditioning; (2) by telling them the truth that the vehicle is equipped with a security system and that the keypad is an element that allows it to be activated or deactivated.

Novelty Journals

ISSN 2394-9678

International Journal of Novel Research in Electrical and Mechanical Engineering
Vol. 11, Issue 1, pp: (68-75), Month: September 2023 - August 2024, Available at: www.noveltyjournals.com

IV. RESULTS & DISCUSSION

4.1 Vehicle vulnerability

The ignition key start test revealed that security based on the key alone is not completely reliable. In fact, from the 4 vehicles used as sample, 2 started with all 3 keys, 1 with 2 keys and only 1 was unable to start. Table 2 gives us a summary of the result of this test.

Table 2: Summary of Neiman test

KEY	NISSAN	SUZUKI	TATA	TOYOTA
Key 1	✓	✓	X	✓
Key 2	✓	X	X	✓
Key 3	✓	✓	X	✓
STAT.	**3/3**	**2/3**	**0/3**	**3/3**

We note that 3 out of 4 vehicles can start with a key other than their own ignition key, i.e. 75%. We believe that wear of the contact cylinder is the cause of this fault in the starting system. We can therefore conclude that the wear caused can help a criminal to easily steal a vehicle.

Apart from using the flaw due to wear, our investigations also revealed that even without an ignition key, vehicles without an immobilizer system can easily be started. A thief can bypass the ignition key system by disassembling the Neiman under the steering wheel as shown in Figure 4. With the required equipment and knowledge thief needs less than 10 minutes to disassemble the Neiman and fraudulently starting the engine. Figure 10 gives the measured time required for disassembly of the Neiman by an expert on 4 vehicle brands.

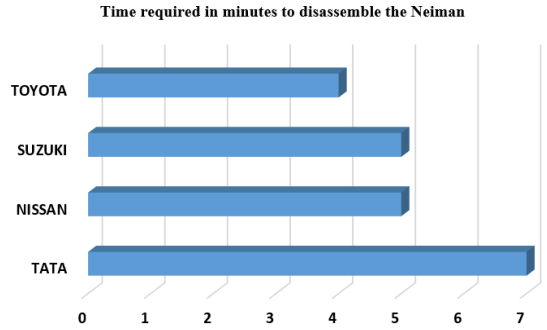

Figure 10: Measured time to disassemble the Neiman

Note that on the TATA brand although the Neiman was completely disassembled, the steering wheel still remained blocked by a mechanical steering wheel locking mechanism unlike other brands. With this, the engine can be started but the vehicle cannot be moved.

4.2 The engine and its components

Analysis of sensors and actuators revealed that certain components are imperative when starting an engine. Table 3 gives a summary of the behavior of the engine we studied according to different components.

Table 3 : Summary of the behavior of the Suzuki M13A engine depending on the state of the sensors and actuators

N°	COMPONENT DISCONNECTED	ENGINE
1	EFI Relay and/or EFI Fuse	Do not Start
2	One injector or one spark plug	Starts with abnormal engine speed
3	More than two injectors or two spark plugs	Do not Start
4	Camshaft sensor	Do not Start
5	Crankshaft sensor	Starts
6	Throttle sensor and Air flow sensor	Starts but no engine idle

Novelty Journals

ISSN 2394-9678

International Journal of Novel Research in Electrical and Mechanical Engineering
Vol. 11, Issue 1, pp: (68-75), Month: September 2023 - August 2024, Available at: www.noveltyjournals.com

Based on this result, our realization of the immobilizer system illustrated in Figure 11 was mounted on the injection circuit (relay and EFI fuse), ignition (on 2 spark plugs), camshaft sensor, as well as that of horn and hazard lights for deterrence.

Figure 11: Captures of the password-based immobilizer produced and mounted on a Toyota NOAH vehicle

4.3 Security test

During the evaluation we observed that when the participants who tested the vehicle were unaware that there was a security system installed and they tried to start the engine several times without success, they automatically thought that the engine had a problem and started looking into where it could be coming from. The security test (evaluation) result of our system is given in Table 4.

Table 4: Result of the evaluation of our system

N°	Participant	Automotive electronics skills	Diagnosis before being aware of the presence of the system	Result after becoming aware of the presence of the system
1	Driver 1	Medium	Spark plug issue	Failed to start (tried for over 2 hours)
2	Driver 2	Medium	None	Failed to start
3	Mechanic 1	Good	Ignition coil pack issue	Failed to start because of the Camshaft sensor
4	Mechanic 2	Excellent	Coil pack and pump issue	Succeeded to start after about 60 minutes
5	Mechanic 3	Excellent	wiring issue	Succeeded to start after about 50 minutes

V. CONCLUSION

At the end of this article, the investigations carried out revealed that 75% of vehicles without an immobilizer can be started with an inappropriate ignition key and 100% of vehicles can be started by dismantling the Neiman. After analysis and evaluation of the proposed system, we observed a considerable contribution to vehicle anti-thief security. For someone who does not have solid skills in automotive electronics or who is unaware that there is a security system installed on the vehicle, this system makes the vehicle impossible to be stolen; but for someone with knowledge of electronics and aware of the presence of the security system, this system allows to increase the time needed to start the vehicle fraudulently from less than 10 minutes to more than 45 minutes because we took care to hide our wiring. However, the presence of the keypad might reveal that there is a security system on board which can serve as a clue to locate all our wiring and reduce the time required for the bypass. As a result, the future researcher may consider eliminating the keypad using an infrared remote control system with all the buttons required to enter a password.

REFERENCES

[1] Méndez, C., Santos, L., Rosales, U., Santos, G., "Prediction Models for Car Theft Detection Using CCTV Cameras and Machine Learning: A Systematic Review of the Literature". International Conference on Computer Science, Electronics and Industrial Engineering (CSEI), vol. 678, 2023. DOI:10.1007/978-3-031-30592-4_14.

[2] Chetan, K., Yogesh, H., “An Approach of Anti-Theft Security System for Vehicles”, International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET), Vol. 5, Issue 5, May 2022. DOI:10.15680/IJMRSET.2022.0505041

[3] Akinwole, B., "Development of an Anti-Theft Vehicle Security System using GPS and GSM Technology with Biometric Authentication", International Journal of Innovative Science and Research Technology, Vol. 5, Issue 2, February 2020.

[4] Saima, S., Anwar, Z., Ajmal, K., Zeeshan, K., "ANDROID BASED VEHICLE TRACKING SYSTEM", Energy Web and Information Technology, Vol. 5, Issue 17, April 2018. DOI: 10.4108/eai.10-4-2018.154447

[5] Said, A., Raditya, A., Nur, S., Thomas, F., "IoT Based Vehicle Safety Controller Using Arduino", Engineering, MAthematics and Computer Science, Vol.5, Issue 1, pp: 1-6, January 2023. DOI: 10.21512/emacsjournal.v5i1.9251

[6] Husni, M., Ginardi, R., Gozali, K., Rahman, R., Indrawanti, A., Senoaji, M., "Mobile Security Vehicle's based on Internet of Things", Journal of Robotics and Control (JRC), Vol. 2, Issue 6, November 2021. DOI: 10.18196/jrc.26135

[7] Hamzah, M., Ali, I., Noorulden, B., "Design and Implementation of an Intelligent Safety and Security System for Vehicles Based on GSM Communication and IoT Network for Real-Time Tracking", Journal of Robotics and Control (JRC), Vol. 4, Issue 5, 2023. DOI: 10.18196/jrc.v4i5.19652

[8] Jorge, A., Jheyson, I., Laberiano, A., "Design of an Anti-theft Alarm System for Vehicles using IoT", International Journal of Advanced Computer Science and Applications, Vol. 12, Issue 12, 2021

[9] Shreya, B., Aniket, I., Nikita, J., Sristi, K., Rasika, N., "A review study on Vehicle Anti-Theft Immobilization System using Face Recognition", International Research Journal of Engineering and Technology (IRJET), Vol. 9 Issue 10, Oct 2022

[10] Eissa, J., "Introducing Fog Computing (FC) Technology to Internet of Things (IoT) Cloud-Based Anti-Theft Vehicles Solutions", International Journal of System Dynamics Applications, Vol. 11, Issue 3.

[11] Thair, A., Areej, M., "Design and Implementation of Anti-Theft Speed Control System Using Wi-Fi and Raspberry Pi 4 Technology", Open Access Library Journal, Vol. 9, 2022. DOI: https://doi.org/10.4236/oalib.1108882

[12] Jie, Z., Zhongmin, W., QingLi, Y., "Intelligent user identity authentication in vehicle security system based on wireless signals", Complex & Intelligent Systems, Vol. 8, pp: 1243–1257, 2022. DOI: https://doi.org/10.1007/s40747-021-00593-6