ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue I, January 2025

Keyless Entry System Using a Smartphone for Vehicle: A Development of Vehicle Security Performance

Richard M. Pabelona Jr., DIT[1], Joe Marie D. Dormido, DIT[2]

[1]College of Industrial Technology, Carlos Hilado Memorial State University

[2]College of Computer Studies, Carlos Hilado Memorial State University

DOI : https://doi.org/10.51583/IJLTEMAS.2025.1401012

Received: 23 January 2025; Accepted: 27 January 2025; Published: 05 February 2025

Abstract: This study involves developing a keyless entry system using a smartphone for vehicles. The system comprises a mobile application and apparatus with main and secondary modules. The main module comprises a mini-computer, Bluetooth Low Energy module, NFC module, ultrasonic sensor, and control circuit installed inside the vehicle. Connected to it is the Secondary module comprising a Car Battery voltage reader circuit, EFI and Fuel Pump control circuit, and a microcontroller located inside the vehicle hood. The mobile application connects to the apparatus wirelessly and acts as a key. A chip-enabled card is a backup key in case the Smartphone is unavailable. It can activate the application by tapping the chip-enabled card through the Smartphone's NFC. The participants of the study are the vehicle owners and are determined through purposive sampling, which is important in examining the subject characteristics involved in the study. Experts evaluated the system using the ISO/IEC 25010:2011 Systems and Software Quality Requirements and Evaluation Questionnaire. The level of acceptability of the Keyless Entry System using Smartphones in terms of functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, and portability was "Excellent". Upon Overall, the system performed its intended function and extended a vehicle's safety features.

Keywords: keyless entry, smartphone, module, microcontroller, mini-computer, Bluetooth LE, NFC, wireless, sensor, vehicle authentication.

I. Introduction

Personal cars have been increasingly important for day-to-day transportation due to its convenience and better mobility as compared to public transport. Vehicles, however, poses a security vulnerability for its owner. Models vary accordingly in terms of performance, features, and price. Security and convenience are two features that come with a cost. Although theft deterrence technology are employed, not all vehicle models are alike and some are using old technology (Xie et al., 2023). With differing systems amongst carmakers, it can be an expensive upgrade just securing your vehicle better (Donlon, 2016). Keyless entry systems have been available with most modern cars today using a transponder/key-fob/remote device (Haodudin Nurkifli & Hwang, 2023; Xie et al., 2023). The said systems are limited in terms of features, dependent on the transponder/key-fob/remote device, battery-operated, and prone to mechanical damage and radio frequency (RF) interference and other security risks (Haodudin Nurkifli & Hwang, 2023; Xie et al., 2023). Biometric authentication with a push to start inside cars has been made available to high-end cars and limited models and is implemented differently by car manufacturers and can be expensive (Xie et al., 2023). Other cars implement keyless entry using a mobile device but are limited to locking and unlocking the car based on proximity and may use older transmission protocols (Ashworth et al., 2023). Furthermore, the implementation of this system does not incorporate a secondary authentication to verify the driver/owner using the smartphone. Implementing most modern systems usually focuses on the vehicle's locking mechanism and does not have an engine control. Engine control varies according to the brand/model of a vehicle and will be restricted to the use of a particular application to utilize it fully. As examined from the prior arts related to the said system, the researcher found out that the solution did not incorporate two-way authentication and incorporated engine immobilization.

Thus, the researcher designed and developed a universal system that is capable of being implemented in vehicles regardless of brand and model that extends a vehicle's convenience and security features. The solution comprises an apparatus installed in the vehicle which co-exists in the existing alarm or security system and adds an ingenious solution to immobilize the engine when an unauthorized user is detected and a mobile application for authentication and communication to the apparatus.

Objectives of the Study

This study aims to design and develop a Keyless Entry System using a Smartphone.

Specifically, this study aims to:

1. Design and develop a system for keyless entry in a vehicle using a Smartphone.

2. Evaluate the system's acceptability using the standard instrument of ISO/IEC 25010:2011 System and Software Quality Requirements and Evaluation in terms of Functional Suitability, Performance Efficiency, Compatibility, Usability, Reliability, Security, Maintainability, and Portability.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue I, January 2025

Framework of the Study

Fig. 1 describes the Input -Throughput-Output of the system. The requests listed in the INPUT are vital requirements for all system operations to function. The list of requests comes from the Mobile Application and the chip-enabled card. The application uses the phone's built-in fingerprint reader, Bluetooth Low Energy (LE), and Near Field Communication (NFC). The chip-enabled card contains a key as an alternative authentication in the absence of a mobile phone. As for the THROUGHPUT, the main module controls the hardware components and performs logical operations of the system to process all requests. The result of the process is then forwarded to the mobile application, which gives the user valuable information. Lastly, the evaluation of the software and firmware of the apparatus adopts the ISO/ IEC 25010:2011 System and Software Quality Requirements and Evaluation instrument for evaluation to determine that the "Keyless Entry System using Smartphone" satisfies the objectives of this study, as shown in the OUTPUT of the conceptual model. The researcher believes that feedback during the development of the system is part and parcel of the system's success in the actual implementation and real-world scenarios it may encounter during operation.

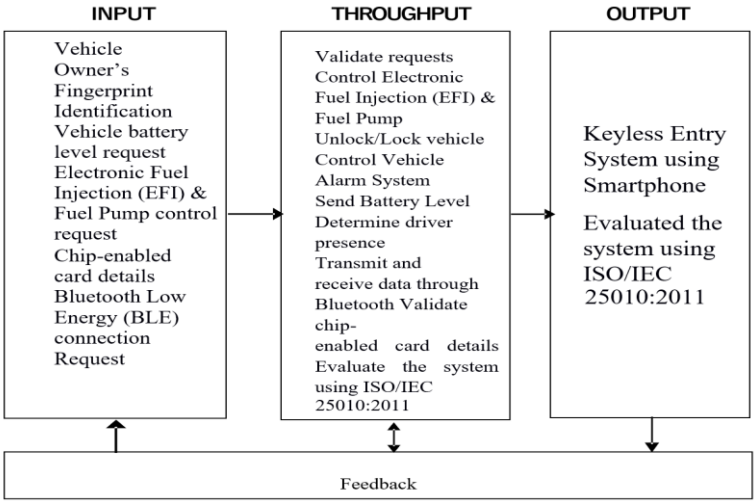


Fig. 1 Conceptual Framework of the Study

Significance of the Technology

The technology of this study applies to embedded systems that combine electronics, electrical, and programming into a single device. Embedded systems use microcontrollers, which use minimal power to run and can perform as a standalone device with less supervision. Its extendability is far superior to most computer systems due to the wide selection of modules that can be integrated and utilized. The system uses the Raspberry Pi module, a minicomputer running on Debian Linux, and comprises a General- Purpose Input/ Output (GPIO) port to develop and integrate external modules. The modules comprising an ultrasonic sensor, Near Field Communication (NFC), a voltage reader circuit, a relay-triggered fuse circuit, and a microcontroller are all vital to the system. For mobile application development, Android was the platform of choice for its openness and availability of documentation in biometrics and Bluetooth. The communication medium of the mobile application and the main module uses Bluetooth Low Energy (BLE), which consumes less power and transfers faster than the previous version. The researcher's "Keyless Entry System using Smartphone" took advantage of the said technologies presented to create a device that extends the security feature of a vehicle and provides a convenient means of access to the owners' vehicle through the mobile application. The system is compatible with most vehicles having at least a central lock and fuel injection regardless of manufacturer and model. The technology presented in this study is extendable and applicable to other areas, not only in vehicles.

Scope and Limitation

This system was intended for vehicle owners who want to extend the security feature and means of accessing their vehicles. This system comprises an apparatus comprising a main and secondary module and a mobile application. The device will extend the feature of the existing security system of a vehicle by adding another layer of security through the use of a mini-computer with Bluetooth Low Energy (BLE) Near Field Communication module, a control circuit for a car alarm, battery level sensor, and Electronic Fuel Injection (EFI) & Fuel Pump control circuit. The system allows a chip-enabled card to authenticate the driver by tapping it into the device's Near Field Communication (NFC) module as an added convenience feature for the owner. The system communicates to the owner wirelessly and does not distract the vehicle's functionality. It can install the system in any vehicle model regardless of manufacturer or brand.

The system requires a direct battery supply for continuous runtime. The system must authenticate the driver through their registered fingerprint using the smartphone's fingerprint scanner to start the vehicle successfully. The mobile application's Bluetooth range cannot exceed more than 10 meters for detection. The system is not capable of creating an NFC tag. The system cannot remotely trigger the vehicle if not in range. The system requires a vehicle with Electronic Fuel Injection (EFI).

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue I, January 2025

II. Literature Review

The concepts, studies, patents and utility model related to the researcher's study is presented, this enabled the researcher to identify key features and gaps in the existing technologies presented. The feature presented disclosed in China Patent No. CN205149794U "use cell-phone fingerprint identification's intelligent vehicle security system" and US Patent No. US20140282931A1 "system for vehicular biometric access and personalization" uses the mobile phone's fingerprint scanner to unlock and lock a vehicle, however the prior art does not employ secondary verification using Near Field Communication (NFC) and backup card solution. On the other hand, WO Patent No. WO2002048485A1 "fingerprint recognition key, lock, and control method" provided a fingerprint recognition key for locking and unlocking the vehicle door, start the engine, and uses a mobile device as an alternative key, however, it does not incorporate a method to control the Electronic Fuel Injection (EFI) & Fuel Pump control of the vehicle wirelessly. In another prior art US Patent No. US20050184855A1 "fingerprint vehicle access system" disclosed, it presents a biometric sensor physically attached to the vehicle and does not make use of a mobile phone's fingerprint scanner. As for the CN Patent No. CN101890932A "intelligent anti-theft device of automobile based on in-vehicle communication system" utility model, it provides GSM and GPS capability that prevents car theft through location tracking and gsm based control, however it does not incorporate a Bluetooth Low Energy (BLE) connectivity to determine driver distance, an ultrasonic sensor that detects driver inside the vehicle, and a fingerprint authentication using mobile phone which adds another layer of security for the vehicle. Lastly, the US Patent No. US20130317693A1 "rental/car-share vehicle access and management system and method" utility model utilizes barcode, Near Field Communication (NF), and a mobile application. The downside of the prior art is its reliance to a network server and is not a standalone device for the vehicle and is not for personal use but for business. Thus, the present invention seeks to address the gap in the prior arts provided by developing a universal device and mobile application that is compatible to any brand or model of vehicle provided it qualifies to the requirements of the system.

III. Methodology

This study follows the System Development Life Cycle (SDLC) for the development of the system for both the mobile application and the apparatus's firmware. Specifically, the "Modified Waterfall Model" was the model of choice by the researcher as it is suited for the system since it incorporates an incremental approach which is needed due to the nature of the study, which requires testing of individual components before integration and afterward implementation. It is supported by Morse (2016), which describes the model as a logical progression of steps taken throughout the software development life cycle (SDLC), much like the cascading steps down an incremental waterfall. While the popularity of the waterfall model has waned over recent years in favor of more agile methodologies, It cannot deny the logical nature of the sequential process used in the waterfall method, and it remains a common design process in the industry (Morse, 2016).

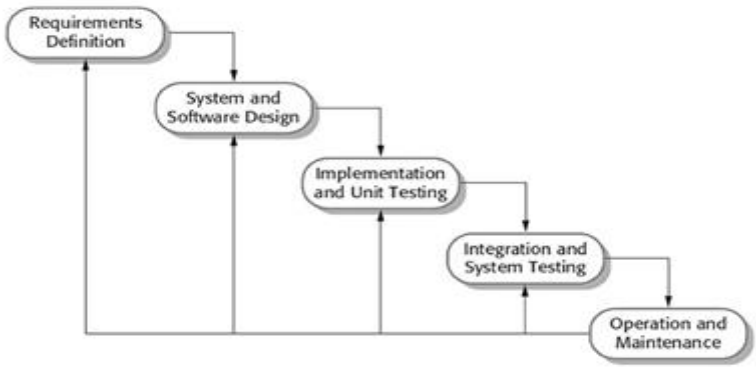


Fig. 2 Modified Waterfall Model

Participants of the Study

The population of the study was determined using purposive sampling with five participants according to their field of expertise related to the study, comprised of a Mechanical Engineer/Automotive, Electronics/Communications Engineer, Computer Engineer, and Information Technology Professional. It was supported by Edralin (2002), who mentioned that "the selection of key informants based on a predetermined set of criteria. These people are considered to be the most appropriate source of data in terms of the objectives of the study". It is to determine whether the participant was an expert, and a profile was gathered for each.

Data Gathering Procedure

The survey questionnaires was reproduced according to the number of respondents for actual administration here in Negros Occidental. The researcher adapted ISO/IEC 25010:2011 Systems and Software Quality Requirements and Evaluation questionnaire. The researcher installed the device on a vehicle and the application on a mobile device. To guide the system's flow, the researcher demonstrated each functionality and feature stated as the objectives of this study to the identified group of experts. As mentioned above, The researcher surveyed five technical experts in the field. An individual evaluated the system to the expert to ensure all features were described and could be evaluated at the pace of the expert. Inspection of the hardware was made and

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue I, January 2025

will then be verified through the mobile application. The data were tabulated and processed electronically upon retrieving the survey questionnaires.

Data Analysis

To interpret the survey results, the researcher used a statistical tool to generate the results, which was then interpreted meaningfully to answer the research problem posed at the beginning of the investigation (Edralin, 2002). The researcher selected the most appropriate statistical tool for data analysis to describe the study's result best.

Data Analysis

The mean of each criterion on the data gathered was computed carefully. A scale of 1 to 5 was made where 1 being the lowest and 5 being the highest. Table 1 was used to interpret the mean score.

Table I: The 5-point scale, its mean range, and verbal interpretation

Mean Range	Verbal Interpretation
4.21 – 5.00	Excellent
3.41 – 4.20	Very Satisfactory
2.61 – 3.40	Satisfactory
1.81 – 2.60	Fair
1.00 – 1.80	Poor

The Technology

Referring to Fig. 3, the System Architecture is described. It is divided into three main parts; the hardware module, the vehicle, and the smartphone. Embedded technology was the choice in developing the system as it can be designed to be stand-alone, power efficient, extendable, and portable. The system uses wireless technology using the power-efficient Bluetooth Low Energy (BLE) and Near Field Communication (NFC). The application was developed for Android and took advantage of the operating system's openness. The programming language for the mobile application is Java which is object-oriented and widely used. The operating system of the main module is Linux based, which is open source. The scripting language used for the main module, Node.js, is because of its wide availability of libraries for the sensors and input-output operations of the system. The system, therefore, is well placed in electronics, electrical, and computer systems.

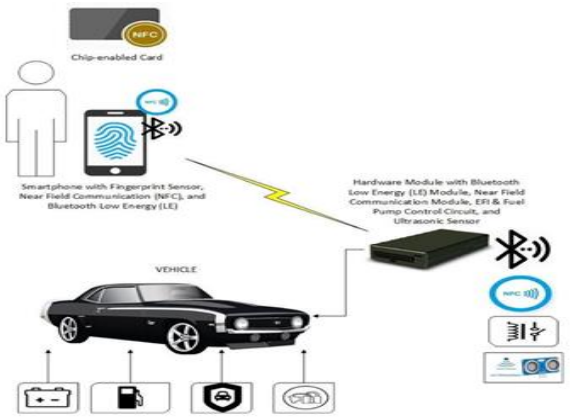


Fig. 3 System Architecture

IV. Results

Table II shows the evaluation of the system, ISO/IEC 25010:2011 System and Software Engineering – Systems and Software Quality Requirements and Evaluation (SQuaRE)- Systems. According to ISO (2011), it is a

Table II The 5-point scale, its mean range, and verbal interpretation

ISO/IEC 25010:2011 Systems and Software Quality Characteristics		**Mean**	**Description**
	GRAND MEAN	**4.55**	**Excellent**
A.	**Functional Suitability (as a whole)**	**4.47**	**Excellent**
	a.1 Functional Completeness	4.40	Excellent

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue I, January 2025

	a.2 Functional Correctness	4.60	Excellent
	a.3 Functional Appropriateness	4.40	Excellent
B.	**Performance Efficiency (as a whole)**	**4.33**	**Excellent**
	b.1 Time Behavior	4.00	Very Satisfactory
	b.2 Resource Utilization	4.40	Excellent
	b.3 Capacity	4.60	Excellent
C.	**Compatibility (as a whole)**	**4.70**	**Excellent**
	c.1. Co-existence	4.80	Excellent
	c.2 Interoperability	4.60	Excellent
D.	**Usability (as a whole)**	**4.57**	**Excellent**
	d.1 Appropriateness Recognizability	4.80	Excellent
	d.2 Learnability	4.40	Excellent
	d.3 Operability	4.60	Excellent
	d.4 User error Protection	4.40	Excellent
	d.5 User Interface Aesthetics	4.40	Excellent
	d.6 Accessibility	4.80	Excellent
E.	**Reliability (as a whole)**	**4.30**	**Excellent**
	e.1 Maturity	4.20	Very Satisfactory
	e.2 Availability	4.80	Excellent
	e.3 Fault Tolerance	4.20	Very Satisfactory
	e.4 Recoverability	4.00	Satisfactory
F.	**Security (as a whole)**	**4.60**	**Excellent**
	f.1 Confidentiality	4.60	Excellent
	f.2 Integrity	4.60	Excellent
	f.3 Non-repudiation	4.60	Excellent
	f.4 Accountability	4.40	Excellent
	f.5 Authenticity	4.80	Excellent
G.	**Maintainability (as a whole)**	**4.64**	**Excellent**
	g.1 Modularity	4.60	Excellent
	g.2 Reusability	4.60	Excellent
	g.3 Analysability	4.60	Excellent
	g.4 Modifiability	4.80	Excellent
	g.5 Testability	4.60	Excellent
H.	**Portability (as a whole)**	**4.80**	**Excellent**
	h.1 Adaptability	4.80	Excellent
	h.2 Installability	5.00	Excellent
	h.3 Replaceability	4.60	Excellent

product quality model composed of eight characteristics (which are further subdivided into sub-characteristics) that relate to software's static properties and the computer system's dynamic properties. The model applies to both computer systems and

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue I, January 2025

software products. It means that the evaluation tool is appropriate for the Keyless Entry System using Smartphones to ensure that it will evaluate all the areas of the system objectively and accurately.

The following are the findings of the study:

1. The level of functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, and portability of the Keyless Entry System using Smartphone when taken as a whole is "Excellent".

2. The level of performance efficiency of the Keyless Entry System using Smartphone when classified according to time behavior is "Very Satisfactory".

3. The level of reliability of the Keyless Entry System using Smartphone when classified according to maturity and fault tolerance is "Very Satisfactory".

4. The level of reliability of the Keyless Entry System using Smartphone when classified according to recoverability is "Satisfactory".

V. Conclusion

Based on the findings of the study, the following conclusions were formulated:

The overall results of the Keyless Entry System using Smartphone in all Systems and Software Quality Characteristics of the ISO/IEC 25010:2011 is "Excellent" which means that the system performed accordingly and extended the safety and convenience features by providing two-way verification, Smartphone fingerprint authentication, engine immobility, and Bluetooth Low Energy (BLE) based keyless entry.

References

1. Akinsanmi, O., Usman, A. D., Abdulraheem A., et. al. (2015). "Two Factor Authentication Based Automobile Keyless Entry System". International Journal of Engineering and Applied Sciences (IJEAS), 2, 102-106.
2. Amit, A., Sarthak S., Shivam, G., et. al. (2014). "Ignition Based on Fingerprint Recognition". International Journal of Scientific Research and Management Studies (IJSRMS), 2, 66-71.
3. Ashworth, J., Staggs, J., & Shenoi, S. (2023). Radio frequency identification and tracking of vehicles and drivers by exploiting keyless entry systems. International Journal of Critical Infrastructure Protection, 40, 100587. https://doi.org/10.1016/j.ijcip.2022.100587
4. Burchette, R. (2004), US Patent No. US20050184855A1, US, US: U.S. Patent and Trademark Office.
5. Chen C., Alfayez, R., Srisopha, K., (2017). "Why Is It Important to Measure Maintainability and What Are the Best Ways to Do It?". Retrieved on May 31, 2018, from https://ieeexplore.ieee.org/document/7965364/.
6. Dipak A., Mhaske, Katariya S. S., Kadlag, S. S. (2013). "Review of Various Functions Controlling of Vehicle by Using Mobile Bluetooth". International Journal of Computer Technology and Electronics Engineering (IJCTEE), 3, 48-52.
7. Donlon, R. L. (2016). "5 things you need to know about keyless ignition systems". Retrieved on June 1, 2018, from https://www.propertycasualty360.com/2016/02/24/5-things-you-need-to-know-about-keyless-ignition-s/?slreturn=20180501030521.
8. Enev, M., Takakuwa, A., Koscher, K, Kohno, T. (2015). "Automobile Driver Fingerprinting". Proceedings on Privacy Enhancing Technologies, 1, 34-51.
9. Haodudin Nurkifli, E., & Hwang, T. (2023). Provably secure authentication for the internet of vehicles. Journal of King Saud University - Computer and Information Sciences, 35(8), 101721. https://doi.org/10.1016/j.jksuci.2023.101721
10. Hashim, N. M. Z., Basri, H. H., Jaafar, A., et. al. (2014). "Child In Car Alarm System using Various Sensors". ARPN Journal of Engineering and Applied Sciences, 9, 1653-1658.
11. ISO. (2011). "ISO/IEC 25010:2011". Retrieved on May 31, 2018, from https://www.iso.org/standard/35733.html.
12. Jefferies, J. E., DeMay, R. W., Lachinyan, G. L. (2012). US Patent No. US20130317693A1, US, US: U.S. Patent and Trademark Office.
13. KEYENCE Corp., (2016). "What is an Ultrasonic Sensor".Retrieved on June 9, 2018, from https://www.keyence.com/ss/products/sensor/sensorbasics/ultrasonic/info/.
14. Kiruthiga N., Latha L. (2014). "A Study of Biometric Approach for Vehicle Security System using Fingerprint Recognition". International Journal of Advanced Research Trends in Engineering Technology (IJARTET), 1(2), 10-16.
15. Kiruthiga, N., Latha, L., Thangasamy S. (2015). "Real Time Biometrics Based Vehicle Security System with GPS and GSM Technology". Procedia Computer Science, 47, 471-479.
16. Koo, H. (2000), WO Patent No. WO2002048485A1, WO, WO: World Intellectual Property Organization.
17. LinkLabs, (2011). "Bluetooth Vs. Bluetooth Low Energy: What's the Difference?". Retrieved on June 9, 2018, from https://www.link-labs.com/blog/bluetooth-vs-bluetooth-low-energy.
18. Mooney J. D., (2004). "Developing Portable Software". Retrieved on May 31, 2018, from https://link.springer.com/content/pdf/10.1007%2F1-4020-8159-6_3.pdf.
19. Morse, E. (2016). "Waterfall Model". Retrieved on May 29, 2018, from https://airbrake.io/blog/sdlc/waterfall-model.
20. Pabelona, R. M., (2014). "Acceptability and Capability of Energy Consumption Monitoring System: Basis for Efficient Energy Saving Scheme". GRCAD 2014 Conference Proceedings, 1, 109 - 126

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue I, January 2025

21. Pan, J. (1999). "Software Reliability". Retrieved on May 31, 2018, from https://users.ece.cmu.edu/~koopman/des_s99/sw_reliability/.
22. Protopapas, M. E. (2012), US Patent No. US8937528B2, US, US: U.S. Patent and Trademark Office.
23. Qixin, C., Weidong, L., Li, Z., Jianmei W. (2015), China Patent No. CN205149794U, CN, CN: China Patent and Trademark Office.
24. Rana, T., Shah, A., Rana, P., Chandak, S. (2017). "Smart Vehicle Security". International Journal of Engineering Science and Computing, 7(4), 10264-10266.
25. Rouse, M., (2012) "Microcontroller". Retrieved on June 9, 2018, from https://internetofthingsagenda.techtarget.com/definition/microcontroller.
26. Sakhare, M., Ganer, S., Mulchandi, M. (2015). "Car Remote Locking Via Bluetooth using Android". International Research Journal of Engineering and Technology (IRJET), 2, 766-767.
27. Secondes, A., (2018). "Adaptive Centralized Communication Management System". Unpublished dissertation. Iloilo Science and Technology University, Iloilo, Philippines.
28. Seffah, A., Donyaee, M., Kline, R.B. et al. (2006). "Usability measurement and metrics: A consolidated model". Retrieved on May 31, 2018, from https://doi.org/10.1007/s11219-006-7600-8.
29. Simmons, M. S. (2013), US Patent No. US20150048927A1, US, US: U.S. Patent and Trademark Office.
30. Square Inc., (2017). "Near Field Communication". Retrieved on June 9, 2018, from http://nearfieldcommunication.org/about-nfc.html.
31. Techopedia, (2018). "Fingerprint Scanner". Retrieved on June 9, 2018, from https://www.techopedia.com/definition/29808/fingerprint-scanner.
32. Xiaolei, L., High release. (2010), CN Patent No. CN101890932A, CN, CN: China Patent and Trademark Office.
33. Xie, X., Jiang, K., Dai, R., Lu, J., Wang, L., Li, Q., & Yu, J. (2023). Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3. Proceedings 2023 Network and Distributed System Security Symposium. Network and Distributed System Security Symposium, San Diego, CA, USA. https://doi.org/10.14722/ndss.2023.24082