Development of Vehicle Door Security using Smart Tag and Fingerprint System

Jamil Abedalrahim Jamil Alsayaydeh, Adam Wong Yoon Khang, Win Adiyansyah Indra, J. Pusppanathan, Vadym Shkarupylo, A K M Zakir Hossain, Saravanan S/O Saminathan

Abstract: Research and development advancements in the area of Vehicle Door Security using Smart Tag and Fingerprint System. Fingerprint biometric is one of the popular, ubiquitous, reliable, economical and efficient biometric technologies. Due to its versatility, fingerprint biometric is applicable. Fingerprint is popular because of its universality, uniqueness, permanence, acceptability, performance [1]. The Arduino as a controller between RFID Sensor, Fingerprint Sensor, Buzzer, LCD, LED and Relay. This research implemented for security purpose to protect the safety of vehicle from vehicle theft or burglary. It is very useful and important for alert the people who have vehicle to protect it from theft. This is a very important system to be implemented at the main door of vehicle. The system started to work when the user access either than one system fingerprint or smart tag to lock and unlock the door. The fingerprint system only user can access their fingerprint whereas the smart tag system can access by user or user's intimate relative when they borrow the vehicle for emergency. The vehicle door cannot be opened when unmatched fingerprint is access or incorrect smart tag is access. Once the incorrect smart tag is access by unauthorized person, the buzzer will be activated and produce a high level of alarm sound to alert the user. The Arduino Uno microcontroller is controlled by the entire system of the project. Hence, it is easy to implement and available to use because it has a simple function, so this system can be enhancing with modern technology so it can be applying into vehicle part for secure the vehicle.

Keywords:Camera-Ready Format, Arduino Uno, Paper Specifications

Jamil Abedalrahim Jamil Alsayaydeh, Center for Advanced Computing Technology, Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik (FTKEE), UTeM, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.

Adam Wong Yoon Khang, Center for Telecommunication Research and Innovation, Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik (FTKEE), UTeM, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.

Win Adiyansyah Indra, Center for Telecommunication Research and Innovation, Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik (FTKEE), UTeM, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.

Vadym Shkarupylo, Department of Computer Systems and Networks, National University of Life and Environmental Sciences of Ukraine, Heroyiv Oborony str., 15, 03041, Kyiv, Ukraine.

A K M Zakir Hossain, Center for Telecommunication Research and Innovation, Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik (FTKEE), UTeM, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.

Saravanan S/O Saminathan, Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik (FTKEE), UTeM, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.

Jaysuman Bin Pusppanathan, Senior Lecturer, School of Biomedical Engineering & Health Sciences, Faculty of Engineering, Universiti Teknologi Malaysia.

I. INTRODUCTION

Vehicle especially car is an automobile and most important transport for human.

As the term of statistics, there are many cases or reports due to the vehicle burglaries and theft and it keep increase time by time. The crime statistical reports state that vehicle burglary is increasing dramatically around the world [2].

This issue has created fear among the people. In this way, there are many ways that have been taken via vehicle owner to more secure the car from burglaries or theft. Hence, every vehicle it is important to have or install a security system. In era of globalization, security system assumes as essential element to prevent unauthorized person that cannot be entry at secured place without approved from owner. In general, lock was simple device that can be hacked by unauthorized person. The lock system was fake functional used in security system. An elective strategy is expected to increase the scope of effectiveness and the proprietor will have better security notification if their vehicle. Development of Vehicle Door Security using Smart Tag and Fingerprint System. These two systems can provide a protection for vehicle from theft and also for the security purpose. The smart tag system is using for access the tag which have security password by user to unlock the vehicle door. Besides, the fingerprint system is high performance security technique using for access user's fingerprint to unlock the vehicle door. In this system, user can access either than one of these two systems allow to open the vehicle door. The fingerprint system only user can access their fingerprint whereas the smart tag system can access by user or user's intimate relative when they borrow the vehicle for emergency. In the case that the smart tag is missing or stolen by unauthorized person, the user can block their tag immediately for cannot to be access again because the tag has security password. Moreover, the vehicle door cannot be opened when unmatched fingerprint is access or incorrect smart tag is access. Otherwise, the buzzer will be activated and produce a high level of alarm sound to alert the user when any unauthorized person could have attempt to theft. In addition, the entire system of this project is controlled by Arduino Uno to achieve the aim in this research. Nowadays, vehicle theft is a kind of assets crime that frequently occurred in the world [3].

By the quick advancement of technology and development of many innovation, the quantity of this crime still can't be reduced. This incident is happened because of minimum standard of security system is installed by vehicle manufacturers such as alarm system. However, this system is not effective enough for security because of low limitation range between vehicle and its owner. By this way, theft can attempt easy to deactivate the security system in the several seconds. Other than that, the insurance agencies have higher pressure as they need to pay the claims made by the clients. As a result, the insurance agencies need to improve the insurance premium. For this situation only a small percentage of people could manage the cost of a good insurance premium. The rise of the insurance premium is causes of installed the shortage of security system to the vehicle. Within this system, the vehicle door security using smart tag and fingerprint systems were developed to prevent the vehicle burglary. Even though, the cost must be affordable and the owner could keep their vehicle with full safety.

Longman, M. stated that vehicle burglary has advanced from people easily burglary from another for their very own use to a highly complex criminal undertaking. Vehicle theft is clearly a crime of property, however it is more suitable to recognize it as a financial crime and recognize that it turns into a hybrid crime when violence is occurred, for example, on case of carjacking. Thus, car makers should always develop security includes and outfit their vehicles with more expensive and reliable anti-theft system. Insurance companies need to deal with an incredible amount of vehicle burglaries, which diminishes their profitability and increases their premiums [4].

Based on (Teh Boon Sung, 2013), the statistic on stolen private cars shows that the quantity of private cars theft was decrease every year from 1980-1995. However, the quantity of private cars theft expanded pointedly after year 2000. The average number of private cars theft is 5,958 every year in 1980-1995. In 2005-2009, this number quite increased more than 3.5 times to 21.501 private cars theft every year [5].

Types of Vehicle Theft
A. Carjacking
Peter Tran revealed that Carjacking is an uncommon occurrence as encounter with another individual frequently requires large amounts of power which normally results in violence. Violence in a minor crime such as burglary stretches the discipline of imprisonment if caught and the crime of theft develops into burglary. Yet, lot of criminals turned out to be progressively desperate as technology and security in vehicles is improved. Hence, the grand vehicles frequently contain security systems that limit the offender's capacity to learn or to execute a vehicle theft. Otherwise, carjacking is one method for vehicle burglary with the most risk from a suspect's point of view others may prefer to use their broad effort through control rather than force [6].

B. Joyriding
Longman stated that vehicles are like stolen basically as a method for brief transportation, frequently referred as a joyriding. Suspects abandon the vehicle when they get to the expected goal as well as when they feel that they may get captured. They may theft another vehicle to get to the following destination, and this cycle proceeds as long as transportation is required. Joyriders are generally youths being age under 18. They drive at rapid that will closes in danger like crashes, killing and mutilating themselves and travelers and people in different vehicles. Besides, joyriding is carried out as vehicle theft crime. This is an excitement with companions or within youngsters. Generally, the stolen vehicle is left after use however the majority of the joyriding thieves are getting included with auto burglary rings. Hence, vehicle thief is a serious crime, but joyriding is minor crime [4].

Ways to Protect Vehicles from Vehicle Theft
RJdrive.vegas stated that gives some tips on how to protect vehicle from vehicle theft; first way is lock the vehicle door. This way should be a head- slapper, yet a lot of thieves are crimes of chance, and a locked vehicle is harder and more open to enter. Approximately 60 percent of all vehicles stolen were left unlocked. The next way is don't left the vehicle key. This way is important that This way describe locked or unlock, keys dangling in the start on the rush or even secreted in the visor make it easier and more probable for vehicle to be snatched. Plus, nearly 80 percent of all vehicles stolen had the keys in them [7].

Dobrian revealed that some tips to protect vehicle from vehicle theft including anti-theft devices. Alarms and visual devices can deflect theft by pointing out somebody attempting to steal or break into the vehicle. These unmistakable or capable of being heard obstacles include vehicle alerts, flashing lights, steering wheel locks, and window scratching. In addition, immobilizing device as anti-theft device that keep thieve from bypassing the vehicle fuel and ignition systems. Hence, a few systems use computer contributes ignition keys while others disable the flow of power or fuel to the engine [8].

Arduino
Louis stated that Arduino is an open source microcontroller which can be effortlessly programmed, erased and modified at any moment of time. The Arduino platform introduced in 2005 was designed to give a reasonable and simple path for specialists, students and experts to create devices that collaborate with their environment using sensors and actuators. According to the simple microcontroller board, it is an open source registering platform that is used for building and programming electronic devices. It also capable for acting as a mini PC simply like different microcontrollers by taking input and controlling the outputs for an assortment of devices. The most used are Arduino Uno and Arduino Mega. Arduino IDE is used to program an Arduino and to straight version of C++. The product is great with a wide range of working system like Windows and Linux. Besides, components of Arduino Board can divide into two categories: hardware and software [9].

On the basis of smart home domain-related usage scenarios, the obtained results have shown that, from corresponding time costs viewpoint, the proposed model is recommended to be applied during the designing of IoT infrastructures. The TLA+ specifications, created with respect to the proposed model, can be characterized as transparent, scalable and

easily reconfigurable solutions that can be applicable in different applicability domains and/or subdomains [10].

Fingerprint Based Anti-Theft System for Vehicle Safety

N.Pooja et al., briefly discussed about developed the security system of vehicle against the theft. Besides, fingerprint is a main role of this project help to developed of security system. A fingerprint of each person is one of a kind even identical twins don't have a similar fingerprint. This is because of fingerprint recognition method that can destroy fear of losing keys. In addition, fingerprint recognition method permits accessing to just those fingerprints that are put away in the library. If vehicle theft occurred, the GPS technology is used for identify or track the vehicle. Hence, this paperwork is based on how to overcome the alcoholic and drive situation. For this way the alcohol sensor is used which recognizes the liquor focus in our breath. Otherwise, the system catches the picture and will create a layout when the user enters the finger print. That produced layout is checked with the filtered confirmed users. On the off chance that it is matched, at that point the vehicle starts. At that point the system will check the alcohol sensor limit value. Although, the system analysis whether the vehicle theft is occurred or not when the fingerprints are unmatched. It can be common by using vibration sensor at lock area. The system will convey the message automatically with the destination by GPS to the vehicle user or owner by GSM [11].
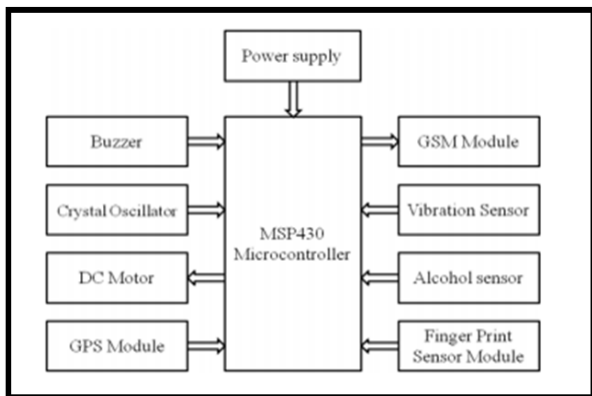
Fig. 1. Block diagram for Fingerprint Based Anti-Theft System [11]

Microcontroller Based Smart Card Car Security System

Loko, A. Z. et al, described that this paperwork focuses on the outline and its implementation with call interruption alert capacity. The PIC167877A microcontroller, RFID reader, RFID card and a GSM modem were used for the effective usage of the system. In addition, the PIC16F877A microcontroller was used to fill in as the whole part of the system which holds the remarkable RFID card number and controls the electromagnetic relay and the GSM MODEM.

The main control section was built with the PIC16F877A microcontroller IC. The PIC16F877A microcontroller belongs to the Microchip Company, which is an 8-bit microcontroller with up to 8 channels built in A/D converter built in transmitter-receiver module and 40 I/O pins.

The Electromagnetic relay filled in as the mechanical apparatus that secures the car start system, and the GSM modem was used to alert the car user at whatever point there is an interruption attempt. Thus, with this sort of system displayed in this paperwork, the security of cars can be more

sensitive in order to secure and ensure the cars more from any interruption and robbery in an electronic based approach. The system planned was tried under various case situations to confirm its reliability.

His paper presented a technical overview on the implementation of a microcontroller based smart card car security system with call intrusion capability. The system has proven to be more advanced than the conventional keyless remote control security because one has to scan the right card before the car ignition starts and also it calls the owner on his cellular phone whenever the car is started or whenever there are intrusion attempts in case of wrong card scanned [12].
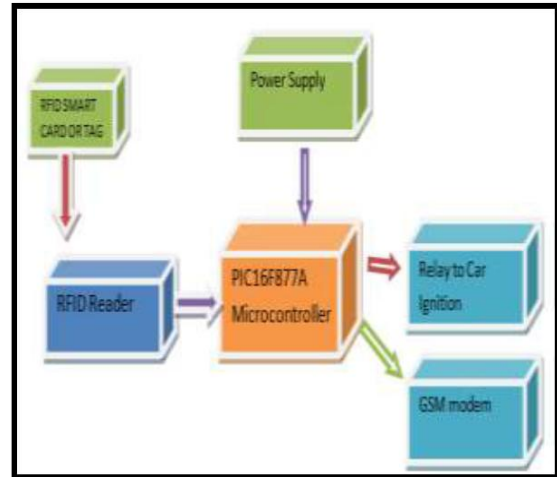
Fig. 2. Block diagram of connection hardware and software [12]

II. METHODOLOGY

Methodology refers to the theoretical analysis of the suitable methods in the field of study or particular principles follow in all fields of knowledge. In defining the problem, it ensures that each work on the project can be completed accurately and perfectly in order with the method prescribed production and maintenance. The study methodology is related with the appropriateness of methods used that determine research in the field of engineering.
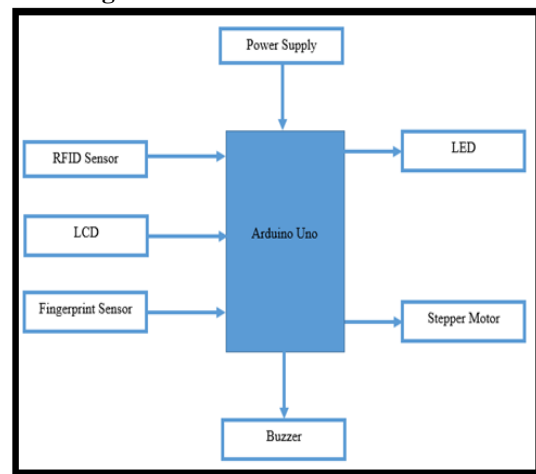
A. Block Diagram

Fig. 3. Block diagram of Vehicle Door Security using Smart Tag and Fingerprint System

There are eight important elements are plays to execute this project successfully which are RFID sensor, fingerprint sensor, Arduino Uno, LCD, Stepper motor, power supply, LED and buzzer. RFID sensor, fingerprint sensor and LCD act as input as well as Stepper motor, LED and buzzer act as output of this project. When user accessing, the microcontroller will receive information from inputs and it will interpret the information. Then, the information will be transmitted to output. For example, when user access the RFID tag, the security code will receive by Arduino Uno to interpret whether it is correct tag or not. Once, the information is conveying to lit up the LED and the stepper motor acts to lock or unlock the door as an output. The buzzer will activate when wrong input is accessing.

B. Flowchart of Smart Tag System
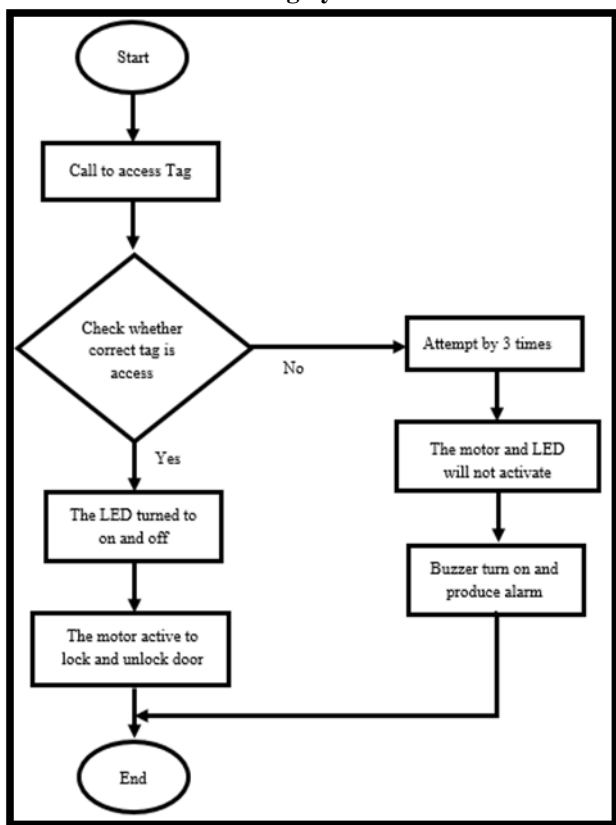
Fig. 4. Flow chart of Smart Tag System

There are two kind of requirement analysis which is functional requirement and non-functional requirement. The functional requirement is defining as what the system should do to achieve or the way it will need to perform the function. The application of this system will allow unlocking the vehicle door as an output of this project when user access the matching fingerprint and smart tag that contain a correct security code. Otherwise, the non-functional requirement is describing as requirement that how the system should perform its characteristic and the limitation that are on its functionality. The user should to understand the overall function of the system to know how to handle it when need to use many times with manually. In addition, the user should decide each parts of system either the software or hardware of the system.

C. Flowchart of Fingerprint System

Fingerprint Authentication has been studied for well over a century. However, its use has truly become widespread and mainstream only in the last few decades due to development of automated fingerprint recognition systems. The ever-increasing demand for reducing the error and failure rates of automated fingerprint recognition systems and the need for enhancing their security have opened many interesting and unique research opportunities that encompass multiple domains such as image processing, computer vision, statistical modeling, cryptography, and sensor development. Our preliminary analysis shows that fingerprints have been proven to be an excellent if not the best biometric and its potential has not yet been fully realized. But still, issues such as fingerprint authentication at a distance, real-time identification in large-scale applications with billions of fingerprint records, developing secure and revocable fingerprint templates that preserve accuracy, and scientifically establishing the uniqueness of fingerprints will likely remain as grand challenges in the near future [13].
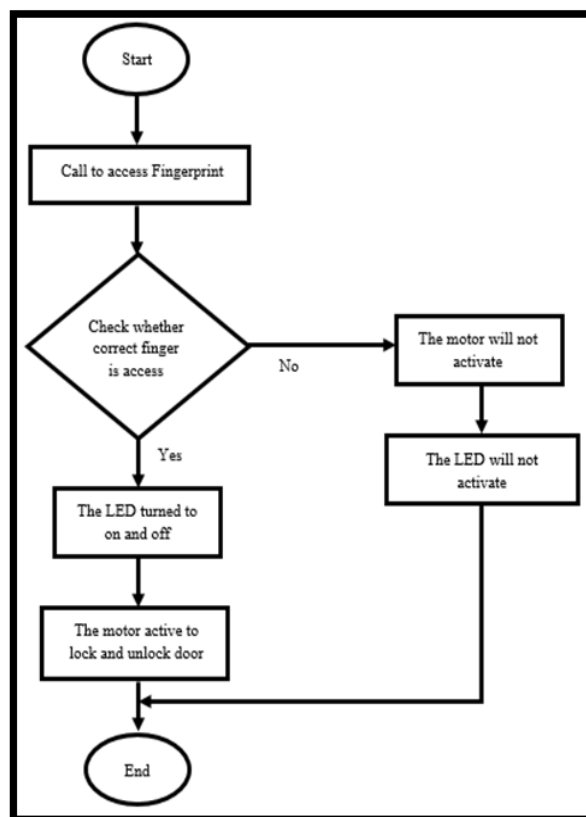
Fig. 5. Flow Chart of Fingerprint System

III. RESULTS

The system has been tested to demonstrate the project delivery's functionality as in presented design. The combination of the software applications and hardware components has enabled the application operating as planned or labelled on the designed interface. A program was composed into Arduino IDE, then it is uploaded into Arduino Uno controller. Other than that, some component also tested with simulation by using Proteus 8.6 software.

3111

After the component is tested, the code program for the project is created and need to verify to ensure it is zero error. At that point, the hardware component is connected dependent on the code program such as the declaration, the input and output. The project work same as expected after the hardware is done connected and the coding is uploaded. The analysis is done to demonstrate the result.

Fig. 6. Prototype of Vehicle Door Security using Smart Tag and Fingerprint System
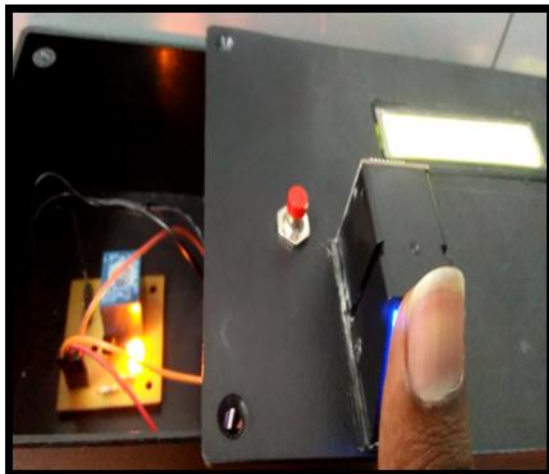
Fig. 7. The project function when correct fingerprint is access
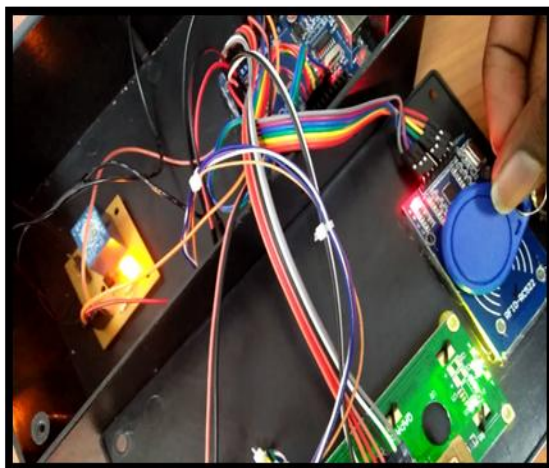
Fig. 8. The project function when correct tag is access

Fig. 9. The motor will function to lock and unlock the door

IV. ANALYSIS

Based on the fingerprint sensor detect, the 'confidence' is a score number which range from 0 to 255 bytes that indicates how better of a match the fingerprint. In this part, calculate the average score number with access of five times the fingerprint by five different fingerprint IDs. The table below shows the average score number of fingerprint match against 5 different fingerprint IDs.

Table 1 The average score number of fingerprint match against 5 different fingerprint IDs

Number of Fingerprint ID	Average value of score number
1	107.2
2	159.8
3	114.8
4	207.8
5	222.6
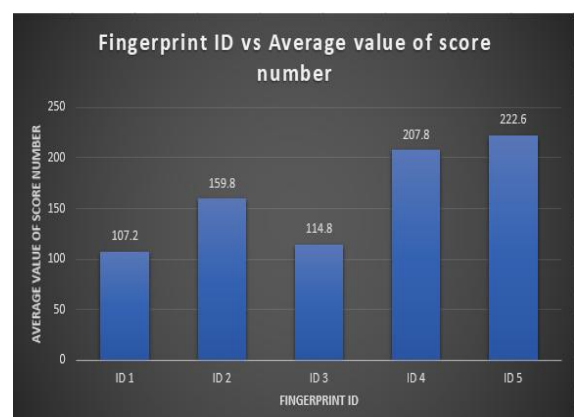
Fig. 10. Bar chart on the five different fingerprint ID versus the average value of score number

From the bar chart above, it can be seen that the score number is range value from 0 to 255 bytes. It will give score number depends on the how range the fingerprint detect in fingerprint sensor.

Adam Wong Yoon Khang was born in Miri district of Sarawak, Malaysia, in 1982. He completed his B. Communication Engineering from University Malaysia Perlis, Malaysia in year 2006. He received his Master degree in Telecommunication Engineering from University Teknologi Malaysia based at Kuala Lumpur Malaysia, in year 2012. In 2012 also, he continues his PhD study in Telecommunication Engineering at Skudai, Johor Bahru of Universiti Teknologi Malaysia and had successfully completed it in year 2018. He then joined Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka (UTeM) in year 2018 also as Senior Lecturer position. At UTeM, he is a research member at Center for Telecommunication Research and Innovation. His current research interest are Internet of Things, Hybrid Optical Wireless, simulation optimization, ad hoc network and passive optical network but not limited to the mention topic here. Currently he supervised some postgraduate students as co-supervisor and is a reviewing member of various reputed journals including Melaka International Conference on Social Sciences, Science and Technology 2019 (MIC3ST 2019). He also as a Professional Technologists for Malaysia Board of Technologists (MBOT).

Win Adiyansyah Indra was born in Sumbawa, Indonesia in 1977. He completed his B. Communication Engineering from Telkom University, Indonesia in year 2001. 10 years of working experience in Telco area, including Nokia. He received his Master degree from International Islamic University Malaysia, in year 2013, sponsored by Yayasan Khazanah Nasional. He then joined Universiti Teknikal Malaysia Melaka in year 2013 as Lecturer. His current research interest is Wireless Communication, Transmission, Radio Frequency Energy Harvesting.

Jaysuman Bin Pusppanathan his Ph.D. degree from Universiti Teknologi Malaysia in 2016. He is currently a Senior Lecturer in the School of Biomedical Engineering & Health Sciences, Faculty of Engineering, Universiti Teknologi Malaysia. His current research interests are electrical tomography for both process industry and biomedical applications, sensors and drone technology. He actively publishes research articles and receives several research grants from both the government and private sectors, university and international collaboration.

Vadym Shkarupylo received M.S. degree from the Department of Computer Systems and Networks in Zaporizhzhia National Technical University, Ukraine, in 2010, and Ph.D - in Pukhov Institute for Modelling in Energy Engineering, Kyiv, Ukraine, in 2014. From 2015 to 2018, he worked as the Assoc. Prof. at the Department of Computer Systems and Networks in Zaporizhzhia National Technical University. From 2018 till present he is the Assoc. Prof. at the Department of Computer Systems and Networks in National University of Life and Environmental Sciences of Ukraine, Kyiv. His research interests include formal methods, web services, Internet of Things.

A K M Zakir Hossain was born in Rajshahi, Bangladesh, in December 1983. He received the B.Sc. from Rajshahi University of Engineering and Technology (RUET) in February, 2007and M.Sc. degrees in Electronics and Telecommunications from the University Gavle, Gavle, Sweden in 2013. He has completed his Doctor of Philosophy (Engineering) from the International Islamic University Malaysia (IIUM), Malaysia in December 2017. He worked as a Post-Doctoral Research Fellow from February 2018 to April 2019. Currently, he is working as a Senior Lecturer in the Faculty of Electrical and Electronics Engineering Technology, University Technology Malaysia Melaka (UTeM). From 2014, he is a student member of the Institute of Electrical and Electronics Engineers (IEEE). He is also a certified engineering technologist in the Board of Engineers Malaysia (BEM) from January 2019. His research interests are Passive RFID, Antenna and Engineering, Electromagnetics, Passive Microwave Devices, and Analog & Digital Electronic System Design.

Saravanan S/O Saminathan was born in Bidor, Perak in 1994. He completed his diploma in Electronics Engineering from Politeknik Shah Alam in year 2015. In the same year, he continued his degree in Bachelor of Computer engineering technology (computer system) with honours from Universiti Teknikal Malaysia Melaka,Utem and currently doing internship for 6 month. His research interest includes wireless networking and Internet of things (IoT).

Retrieval Number: E7468068519/2019©BEIESP
DOI: 10.35940/ijeat.E7468.109119

3114

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication