OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Smart Security System for Vehicles using Internet of Things (IoT)

VIJAYKUMAR H NAYAK
SELECTION GRADE LECTURER (CSE)
GOVERNMENT POLYTECHNIC LINGASAGUR
vknayak146@gmail.com

ABSTRACT
Vehicle security systems (VSS) will become smart systems in the future due to the increasing development of smart technologies, which will have many advantages. The internet has become a necessary component of daily life due to its constant advancements; the newest and most cutting-edge technology, known as Internet of Things (IoT), has completely revolutionized the way people see the world. Every day, the Internet of Things expands from tiny devices to massive machines that can exchange data and carry out tasks while people are engaged in other activities. The primary goal of the article is to use the Internet of Things (IoT) to develop a smart vehicle security system. This involves converting a traditional vehicle security system (CVSS) into a smart vehicle security system (SVSS), which allows users to access and manage automobiles remotely using a smartphone. Intelligent Anti-Theft Tracking Systems (iATTS) is another term for SVSS. Our specific goal is to create a wireless smart vehicle security system that is lightweight, affordable, expandable, and flexible through the Internet of Things (IoT). To do this, we will integrate various technologies such as radio frequency identification (RFID), cloud networking, wireless communication, GPS, GSM, and fuzzy algorithm for decision trees. This intelligent system is designed to notify the car owner of information about the vehicle, including location, time, and alarm, using a mobile application or Short Message Service (SMS). When combined, the technologies may function as a smart vehicle security key that allows users to operate their car from a distance (by using an app or SMS to open or lock it). The whole system is made with all different kinds of cars in mind. It is easy to install and simple enough to give high protection for automobiles. The SVSS will be used to prevent, detect, and countermeasure vehicle robberies.

Keywords: Smart vehicle security systems; Automation; Internet of Things; IoT; Radio frequency Identification; RFID; Global Positioning System; GPS; Global System for Mobile communication; GSM; Short Message Service; SMS; cloud networking; fuzzy algorithm.

I. INTRODUCTION

The widespread theft of automobiles is evidence that the security setup for automobiles, especially those with two wheels, is still inadequate. Having an additional security structure in place is seen to be crucial for keeping cars at a strategic distance from potential burglaries. Owners of vehicles must carefully consider vehicle security under such circumstances. A strong security framework is required in the present situation for all kinds of vehicles. According to a recent report, India has the biggest two-wheeler industry in the world, selling close to 17.7 million vehicles in 2016—nearly 48,000 of which are sold per day. The second-biggest market for two-wheelers is China. Taiwan, Vietnam, Indonesia, Pakistan, and other Asian nations came next. The danger of theft increases when there are more motorcycles on the road. As to the National Crime Records Bureau (NCRB) statistics, 211,844 two-wheeler vehicles were reported stolen in India in only the year 2016. There is an increase from reports from 2010 to 2015, yet only 46,436 automobiles were recovered, meaning 78% of the vehicles were left unrecovered.

Two-wheelers are usually taken directly from apartment parking lots or roadways. Wheel clamping, sometimes known as vehicle clamping, and towing services are other methods used to steal vehicles. The cars are either disassembled or sold at cheap rates by the time the police are called, which may be several hours after the crime, leaving almost no evidence. Due to the difficulty in recovering the automobiles, both the owner and the police are unable to hold the thief accountable. In the worst situation, cars are taken by a towing company that has been given permission by a police officer without the owners' knowledge.

It's interesting to note that reports of car theft cases worldwide are rising at a startling pace, and the situation is the same everywhere else in the globe. The majority of car security systems are designed specifically for four-wheelers. Over the years, several security systems have been suggested; nonetheless, almost all of the most recent cutting-edge security systems are created specifically for automobiles. The two-wheeler security measures that are now in place have significant drawbacks.

A smart car security system is a tool that lets people operate cars intelligently and autonomously in a local or worldwide setting. Many well-known and current frameworks for car security systems rely on different technologies, however they are insecure and don't fully support people. Several security features, whether they are basic or make use of modern technology, have been created in cars in response to the portrayal of car thefts. Typical security features, such alarm systems for four-wheel cars and keys for two-wheel vehicles, have previously been added by developers to automobiles. In the current technological age, security mechanisms [1] offered by the developers are less reassuring; further protection is necessary if it is to be genuinely safe. Using a microprocessor, Nasir and Mansor [2] created an automated key for a two-wheeled vehicle. Sehgal et al. [4] were successful in creating a security system that uses SMS to monitor missing two-wheel cars, whereas Tang et al. [3] produced security systems for four-wheeled vehicles utilizing wireless sensor network technology. The digital mobile telephone technology known as GSM is extensively used in Europe and other regions globally. Of the three digital wireless telecommunication systems (TDMA, GSM, and CDMA), GSM is the most frequently used and uses a form of time division multiple access (TDMA). After data has been digitalized and compressed, GSM delivers it along a channel along with two additional user data streams, each in a separate time slot. It uses the 900 MHz or 1800 MHz frequency range to function.

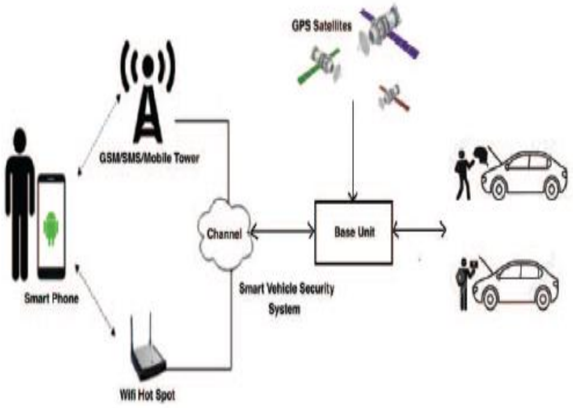

Figure No. 1: The concept of the Wireless Vehicle Security System (WVSS) using IoT.

The Very Important Person (VIP) security paradigm is seen in many created products. It is composed of many levels, such as the first secure point, second secure point, and so on. Two levels of security are used in this research to ensure the safety of the vehicles: point positioning for the second secure point and authentication technique for the first. Whereas the Point Positioning method is one of the techniques used in GPS, the authentication method has been extensively used in several computer security systems. [5] employed the authentication technique for a wireless network security system, and the researchers compared the accuracy of GPS-online data processing from a few GPS data processing services using the Point Positioning method. The process of accessing certain systems, such as those that need a password [6], fingerprint [7], retinal [8], facial recognition [9], ID number (unique number), and others, is known as the authentication method's concept. The initial stage in these investigations is the authentication of the ID number; thanks to RFID technology, there won't be any ID number duplication or sharing. The fundamental GPS approach, known as the point positioning method [10], seeks to determine a location in real-time with a high degree of precision. It is also referred to as the absolute method. The security system is described as follows: in order to switch on the car, the rider must first enter his ID number using the authentication method. The initial safe point employs a normal security system. In contrast, the second security point employs the Point Positioning technique in conjunction with GPS to monitor the location of the equipment.

II. LITERATUCRE REVIEW

One single component—the microcontroller—will operate all systems, and radio frequency identification serves as this component's control (RFID). The vehicles will be more secure when the authentication and point positioning methods are used, as only one ID number will be recognized and able to unlock the handlebar and start the engine on two-wheel vehicles. The rider must authenticate their ID number in order to unlock the handlebar. Another benefit of this system is its real-time location tracking capability, which is made possible by the Point Positioning method's high degree of precision in real-time position identification. If the bikes are stolen, the two techniques included in the vehicles will cause the engine to shut off automatically.

The design of the car security system uses an Arduino microcontroller as the primary controller; it is noteworthy that this controller can send brief message alerts that convey information in the form of warnings and the location of the vehicle. It is anticipated that the system will be a cutting-edge vehicle security system that uses a variety of communication technology combinations to create interactive security systems. Since building IoTs has contributed a new dimension to the evolution of information and communication technologies, it has advanced significantly in the last few years. The term "Internet of Things" (IoT) refers to a relatively new paradigm for communication that envisions a near future in which everyday objects will be equipped with microcontrollers, phones for computerized communication, and the necessary protocols to enable them to communicate with users and each other, becoming an essential component of the Internet. The development of information and communication technology has been measured in a new way by the Internet of Things (IoTs).

By 2020, 50 billion things or gadgets are expected to be linked to the Internet, according to CISCO [11]. The Internet of Things (IoT) promises to make the Internet much more ubiquitous and immersive. Moreover, the Internet of Things (IoT) will promote the development of numerous applications that utilize the potentially enormous amount of data produced by such a system to provide new services to various organizations, individuals, and other service-oriented sectors by enabling simple access and interaction to a wide range of devices, such as home electrical appliances, sensors, CCTVs, etc. [12].

Fig. 1 illustrates the Wireless Vehicle Security System (WVSS) idea leveraging IoT. This framework improves car security systems by enabling smart, intelligent, and autonomous vehicle control over the internet from anywhere in the world using PCs, smartphones, and/or mobile devices. Among many other loT applications, smart security systems are crucial to the global realization of smart cities.

III. PROPOSED SYSTEM

Problems with modern technology: There are several problems with the sophisticated security system that is in place right now.

- using image processing technology (biometric methods, such as face detection, voice recognition, and fingerprint detection systems) – these security systems are expensive, complicated, and unsuitable for use with two-wheelers. The only two functions that existing car security systems can do are disable the engine and activate a loud alarm, which is a severe restriction.
- Expensive: The security mechanisms that are in place now are quite costly. Car makers will not be able to install security systems unless they are fairly priced, since doing so would result in a significant rise in the vehicle's total cost. The cost of non-recurring engineering (NRE) may be decreased if the security system is designed to work with most car manufacturers and classes.
- Power usage: Another important factor is power usage. The vehicle's 12V battery serves as the security system's supply, thus there should be less power used overall.
- Space Utilization: Since two-wheelers provide very little room for installing security modules, one of the main limitations is area. The need is to create a system that fulfills essential functions, is easy to use, economically priced, and compact enough to fit beneath a car seat. The module's small size makes it possible to install it under the car's seat without requiring any structural modifications to the car.
- Automobile Insurance firms: Due to the concerningly high incidence of theft, insurance firms face substantial costs. Rates for SMS/Data Pack Subscriptions: To get frequent theft SMSs and access to the mobile app, users must pay a monthly or annual subscription fee.

The only way out of this situation is to create a low-cost, low-complexity, strong, and trustworthy security/theft control system that enables people to monitor and totally lock their cars. The police officers may then promptly get the information that the owner of the car has captured. The primary goal of the article is to use the Internet of Things (IoT) to develop a smart vehicle security system. This involves converting a traditional vehicle security system (CVSS) into a smart vehicle security system (SVSS), which allows users to access and manage automobiles remotely using a smartphone. Specifically, we want to use the Internet of Things (IoT) to design a low-cost, flexible, extensible wireless smart vehicle security system that integrates wireless communication, cloud networking, radio frequency identification (RFID), GPS, Global Positioning System (GPS), and Global System for Mobile communication (GSM). This intelligent system is designed to notify the car owner via a mobile application or Short Message Service (SMS) of various vehicle information, including location, time, and alarm. The technologies work together to provide a smart car security key that allows users to remotely manage their vehicle via an SMS or app, allowing them to lock or unlock it. This whole system is made with all kinds of cars in mind, offering a straightforward, efficient installation process that gives cars the highest level of protection.

IV. DESIGN AND IMPLEMENTATION

Figure 2 lists the basic characteristics of the smart security system for automobiles.

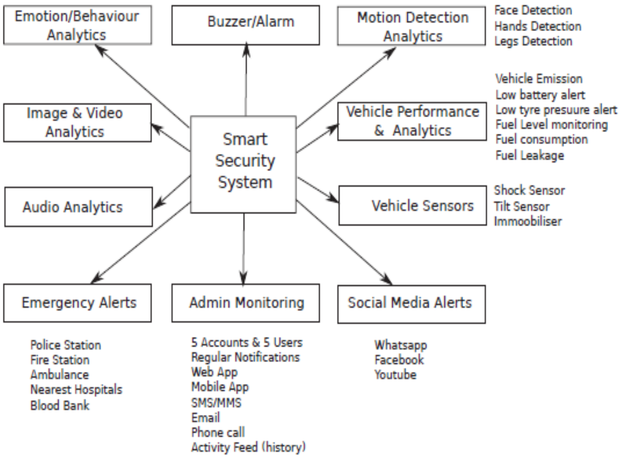

Figure No. 2: Features of the Smart Security System for Vehicles using IoT

The planned vehicle type, namely the motor made with a big enough storage box, will be fitted with the RFID-based double security system design. An open-loop control system, the double security system on RFID-based cars refers to the detection output results given by the RFID detection system; no feedback is delivered back to the rectification process. The block diagram of a complete smart car security system is shown in Fig. 3. The identification, detection, controllers, and output subsystems make up an interactive double security system for cars based on RFID. subroutines.

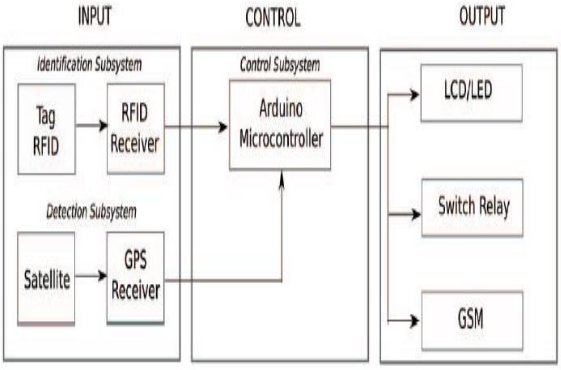

Figure No. 3: Block diagram of an overall smart vehicle security system

Identification Subsystem: An input subsystem includes the identification subsystem. RFID tags, an RFID reader, and the primary Arduino Uno R3 microcontroller make up the RFID detection subsystem. RFID Reader: This device reads RFID tag identifying data and sends it to the Arduino Uno R3 microcontroller, which functions as a controller. Detection Subsystem: The main controller, an Arduino Uno R3, satellites, and a GPS receiver make up the GPS detection subsystem. The satellite will communicate data in Global Positioning System Fix/Accuracy Data (GGA) and National Marine Electronics Association (NMEA) format when it detects the presence of a GPS receiver. Next, the Arduino Uno R3 microcontroller receives the data.

- Minimum Output, Relay Action, and GSM Communication subsystems make up the Output subsystem. On Minimum Output Subsystems, there are LED and buzzer indicators that show the input, and a 16x2 LCD that shows the output of the data reader. Action subsystem, a subsystem that connects the cars by acting as a breaker/ignition circuit, may be accomplished by employing relays as automated switches.

- Control Subsystem: The Arduino Uno microcontroller may trigger the relay to turn on the motor circuit ignition systems by producing an initial output of 5 volts (high condition). To prevent the vehicle ignition system from turning on until the ignition relay and the necessary conditions are met, the circuit is linked to the key switch on the car. The GSM communication subsystem facilitates communication between the owner of the vehicle's mobile phone and microcontroller.

The Linksprite ATWIN GSM Shield module, compatible with the Arduino Uno R3 microcontroller, is used to create the communication subsystem. Since the GSM module needs the ATcommand protocol to operate, the Arduino microcontroller's software code needs to provide a description of it.

Additionally, our own mobile application "Find my Vehicle" may be used to track the whereabouts of automobiles via the security system installed in them. Therefore, our software will assist users in finding the device on a map, locking it remotely, playing music, displaying a message, and/or receiving driving instructions to the location of the car. The position information is obtained by the satellite station, which may then display it in Google Maps. In this system, the base station and the satellite station function as a master and slave pair, with the base station giving the satellite stations the orders they need to find their positions. An Android smartphone serving as a client controls the system, and data is delivered using socket programming. The software offers an interface that allows users to remotely operate and monitor each of the three stations (think of it as a "find my iphone app"). In case the internet is unavailable for updates from the system, there is an additional communication module known as the GSM module.

V. RESULT ANALYSIS

Tests on tools and components, tests on subsystems, and tests on the whole system were all carried out in phases.

5.1: Test on Component/Tools Function

To prevent mistakes brought on by one or more of the tools or devices not working, tests were performed on the components, devices, and tools. Digital multimeter measuring instruments and software for every device were used in the test.

- Test of the Voltage Source: The purpose of the test was to ascertain if the voltage source could provide the voltage required by the system. The voltage sources are linked to the voltage regulator circuit, which is made up of the ICs 7805, 7809, and 7812, among other parts. This is being done to modify the system's voltage needs. The error numbers were derived from the voltage source's test results using:
- Test using Tags and RFID Reader: Three RFID tag units were utilized in this test. RFID Tester software was used to conduct the test. An RFID minimal circuit was attached to a single ACER 4752G research portable computer unit. RFID minimal circuit uses a USB to Serial RS232 interface to send the data on the RFID tag serially to the computer unit. The card number 8803460 (tag1) is used to acquire data for the first RFID tag test. With the card number 8803459 (tag2), data are acquired for the second RFID tag test. Using the card number 7206252 (TAG3), data is acquired for the third RFID tag test.
- The purpose of the Main Controller Microcontroller, Arduino Uno R3 Test is to ascertain whether the Microcontroller Arduino Uno R3 is in excellent working order. The software IDE (Integrated Development Environment) 1.0.5 Arduino was used to test the primary controller, microcontroller Arduino Uno R3. By connecting the Arduino Microcontroller to a computer and using the Arduino IDE software to upload a sample program to the Arduino Uno R3, one may ascertain the Arduino Microcontroller's circumstances.

5.2: Subsystem Test

To make sure the subsystem could carry out its duties in accordance with the requirements of the system, a test was undertaken. Tests are run on the output, control, and detection subsystems, and the results are compared to see whether the system produced the desired outcomes.

- Test on Identification RFID Subsystem: The test uses an Arduino Uno R3 microcontroller unit, an RFID reader ID-12 LA unit, several minimal output systems, and software Arduino IDE 1.0.5. The purpose of this test was to determine the RFID reader's capacity to scan RFID tags, transfer ASCII data to the Arduino Uno R3 microcontroller, and display the data on an Arduino IDE 1.0.5 software monitor.

- Test for GPS Detection Subsystem: The test uses a U-box GPS Receiver CN-06 unit, an Arduino Uno R3 microcontroller unit, PCs, Arduino IDE 1.0.5 software, and U Center GPS Evaluation Software. The Global Positioning System (GPS) is used to get latitude and longitude data at random intervals across the Bangalore, India, region.
- Examine the Action Relay Subsystem. The test makes use of a 12-volt power supply, a relay circuit Activator, an Arduino Uno R3 microcontroller, PCs, and Arduino IDE 1.0.5 software. Based on the instructions provided by the Microcontroller Arduino Uno R3's primary control, the test was carried out to ascertain how well the circuit functioned as a switch linking relay movers and breaker. The character input that is received from the computer via USB-based serial connection influences the command. The characters "1" and "0" cause the relay to switch back to the connected position, turning on the LED lights, and "0" to turn off the LED lights, respectively.
- Test on GSM Communications Subsystem: The test used the following components: an Arduino Uno R3 microcontroller, a Link sprite ATWIN Quadband GPRS/GSM Shield module, a computer, a mobile phone, and software: Arduino IDE 1.0.5 and SSCOM32E. The purpose of the test was to confirm that the Link sprite ATWIN Quadband GPRS/GSM Shield module could indeed facilitate communication between the Arduino microcontroller and the mobile device.

An Arduino Uno R3 microcontroller may be used with the Link sprite ATWIN Quadband GPRS/GSM Shield communication module. GSM service is supported by the module.

SMS in text format and PDU (binary) are supported by the Link sprite Quadband GPRS/GSM Shield. The 900 MHz frequency of the Link sprite ATWIN Quadband, GPRS/GSM Shield is ideal for usage in India.

5.3: System Test

A system test is carried out after the integration of the current subsystems into a single system. This step counts the time delay that the system experiences. It is evident that certain of the actions taken in reaction to certain situations feeding into the system have a temporal delay. Getting Ready A temporal delay happens when a newly installed system is switched on. Relay On time delay is the amount of time needed to ensure that the RFID tag input criteria are met and that the key is turned on to activate the relay. The amount of time needed for the motorcycle's key to be turned off and the relay to become inactive is known as the delay time relay Off 1. Relay time relay Off 2 is the amount of time that must pass before the GSM character input requirements are satisfied and the relay is turned off. After receiving power from a voltage source, the system had an average 5.6-second setup delay. With an average time, delay of 1.6 seconds, the system is capable of responding to input circumstances.

If the data from the RFID tag is suitable, the microcontroller Arduino Uno R3 performs the function by connecting the relay. If the data from the RFID tag matches and the car is turned on, the following step is to contact the registered phone number. A brief message with the vehicle's position is sent to the specified phone numbers as the other system action.

VI. DISCUSSION

The system's functioning has allowed for the findings that have been acquired based on the identification, detection, actions, and communication tests that have been conducted. The system can recognize an RFID tag's object as an access key to the vehicle engine based on ASCII data stored in the tag, and it can then connect several vehicle engines. Similarly, the system can recognize an incoming SMS's character through the Linksprite GSM Shield module as input character, and it can then respond to the SMS with the vehicle position information so that it can connect with the owners' mobile devices.

Serial communication is necessary between the systems' identification, detection, and communication processes and the Microcontroller Arduino Uno R3 primary data processor. The primary data processor, Microcontroller Arduino Uno R3, has two serial communication pins, one for the data transmitter (Tx) and one for the data receiver (Rx). It can only communicate with one process at a time while receiving data. This results in the inability to meet the requirements of the system, which comprises three serial communication processes (RFID identification, GPS detection, and GSM communications). With the use of the software code libraries "SoftwareSerial" and "AltSoftSerial," the requirements are satisfied by using two pairs of fake pin serial addition. Pin serial connection operates at the same 9600 Baud Rate. The functioning principle of the fake pin serial is identical to that of the actual serial pin on the Arduino Uno R3, although there is a little chance of delay time accumulation since the pins operate alternately quickly.

The test results demonstrate that the system is experiencing a delay in operation. Several variables contribute to the time delay, including the impact of time delay programs and external factors like weather and building development that might interfere with data transmission signals. Building construction that obstructs radio waves between the GPS receiver and satellites has a significant impact on the GPS receiver's ability to receive data from satellites and transmit it to the Arduino Uno R3 microcontroller. Receiving calls or brief messages when there is a signal outage also has an impact on GSM Shield's functionality. One of the main causes of the system's time delay is the program's upload time to the Arduino Uno R3 microcontroller.

VII. CONCLUSION

The test results and discussion lead to the conclusion that an interactive double security system has been implemented on vehicles that can distinguish an RFID tag based on ASCII data stored to turn the vehicle on and provide the vehicle's location. The vehicle's machine may be turned off when it is taken thanks to an emergency safety function included into the security system that uses GSM connection. The system's latency and the surrounding environment both have an impact on information accuracy. With an average preparation delay time of 5.6 seconds and an average delay time of 1.6 seconds, the system's overall time delay may be accepted for its efficacy. Error acquisition 4.067% on the voltage source indicates that the voltage source system is functioning properly.

The proposed system's concept is to replace traditional security systems with the Internet of Things (IoT), wherein automobiles are networked to the internet and accessible from any location via an Android smartphone that can establish a wireless network connection. A thorough assessment and a useful description of the component testing will be carried out to enhance the job. Additionally, we want to provide an integrated assessment that contrasts the current CVSS with our suggested SVSS. This will help us achieve our main objective.

Future work will mostly focus on the interaction that is introduced between fuzzy algorithms and cloud networking methodology. Vehicles may have developed smart security systems fitted to track the whereabouts of the vehicle using our own "Find my Vehicle" mobile application. Therefore, our software will assist users in finding the device on a map, locking it remotely, playing music, displaying a message, and/or receiving driving instructions to the location of the car. The position data is obtained by the satellite station, which then displays it on Google Maps. Additionally, the system may store vehicle status information and geographical and temporal data on the Thing speak cloud platform. Graphs are used in the mobile application to display the saved data. Users of the system may examine and track the whereabouts of vehicles at any time and from any place. Our Internet of Things (IoT)-based smart security system has been successfully shown via experiments with connected cars, which are readily managed remotely or wirelessly over the internet. The use of blockchain technology and artificial intelligence in fleet management and vehicle monitoring will be crucial.

REFERENCE

[1]. V. Govindraj, M. Sathiyanarayanan, and B. Abubakar, “Customary homes to smart homes using internet of things (iot) and mobile application,” in Smart Technologies for Smart Nation (SmartTechCon), 2015 International Conference On. IEEE, 2017, pp. 1059–1063.

[2]. M. M. Nasir and W. Mansor, “Gsm based motorcycle security system,” in Control and System Graduate Research Colloquium (ICSGRC), 2011 IEEE. IEEE, 2011, pp. 129–134.

[3]. V. W. Tang, Y. Zheng, and J. Cao, “An intelligent car park management system based on wireless sensor networks,” in Pervasive Computing and Applications, 2006 1st International Symposium on. IEEE, 2006, pp. 65–70.

[4]. Z. Yihua, “Vip customer segmentation based on data mining in mobile-communications industry,” in Computer Science and Education (ICCSE), 2010 5th International Conference on. IEEE, 2010, pp. 156–159.

[5]. S. A. Hameed, S. Abdulla, M. Ershad, F. Zahudi, and A. Hassan, “New automobile monitoring and tracking model: Facilitate model with handhelds,” in Mechatronics (ICOM), 2011 4th International Conference On. IEEE, 2011, pp. 1–5.

[6]. B. Gurung, P. Prasad, A. Alsadoon, and A. Elchouemi, “Enhanced virtual password authentication scheme resistant to shoulder surfing,” in Soft Computing and Machine Intelligence (ISCMI), 2015 Second International Conference on. IEEE, 2015, pp. 134–139.

[7]. T. R. Borah, K. K. Sarma, and P. H. Talukdar, “Retina recognition system using adaptive neuro fuzzy inference system,” in Computer, Communication and Control (IC4), 2015 International Conference on. IEEE, 2015, pp. 1–6.

[8]. C. C. Queirolo, L. Silva, O. R. Bellon, and M. P. Segundo, “3d face recognition using simulated annealing and the surface interpenetration measure,” IEEE transactions on pattern analysis and machine intelligence, vol. 32, no. 2, pp. 206–219, 2010.

[9]. Y.-Q. Gui and J. Zhang, “A new authentication rfid protocol with ownership transfer,” in ICT Convergence (ICTC), 2013 International Conference on. IEEE, 2013, pp. 359–364.

[10]. N. M. Raharja, O. Wahyunggoro, A. I. Cahyadi et al., “Altitude control for quadrotor with mamdani fuzzy model,” in Science in Information Technology (ICSITech), 2015 International Conference on. IEEE, 2015, pp. 309–314.

[11]. M. Sathiyanarayanan and K. S. Kim, “Multi-channel deficit roundrobin scheduling for hybrid tdm/wdm optical networks,” in Proc. Of the 4th International Congress on Ultra-Modern Telecommunications and Control Systems (ICUMT 2012), St. Petersburg, Russia, Oct. 2012, pp. 552–557.

[12]. M. Sathiyanarayanan and B. Abubhakar, “Dual mcdrr scheduler for hybrid tdm/wdm optical networks,” in Proc. of the 1st International Conference on Networks and Soft Computing (ICNSC 2014), Andra Pradesh, India, Aug 2014, pp. 466–470.

[13]. M. Sathiyanarayanan and B. Abubakar, “Mcdrr packet scheduling algorithm for multi-channel wireless networks,” in Proceedings of 3rd International Conference on Advanced Computing, Networking, and Informatics. Springer, 2015, pp. 125–131.

[14]. M. Sathiyanarayanan, S. Azharuddin, and S. Kumar, “Four different modes to control unmanned ground vehicle for military purpose,” vol. 2, no. 3, pp. 3156–3166, 2014.

[15]. M. Sathiyanarayanan, V. Govindraj, and N. Jahagirdar, “Challenges and opportunities of integrating internet of things (iot) and light fidelity (lifi),” in 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). IEEE, 2017, pp. 137–142.