Research Paper   Open Access

A Review of Intelligent Lock System

S. O. Anaza [1], J. D. Jiya[2] and Y. S. Haruna[2]

[1]*Research and Development department, Power Equipment and Electrical Machinery Development Institute, (PEEMADI) Okene, Kogi State, Nigeria*
[2]*Department of Electrical/Electronics Engineering, Abubakar Tafawa Balewa University, Bauchi-Nigeria.*

Abstract: *Threat to life and property necessitate the need for security (lock) systems which has evolved with technological advancement. Existing literature does not present first hand information to researcher to ascertain the research gap. This paper presents a review of some literatures in intelligent security lock systems, by presenting their concepts, the advantages and the drawback of such concept and the possible modification. Each of the literature reviewed is categorized into either single or multiple protocols depending on the number of security feature in the lock system. A single protocol system has one security feature while the multiple protocols have several security features. The approach produces a unique result which solves the problem of laborious literature survey.*

Keywords: *Security, Technology, Intelligent, Protocol, Lock System*

I.   INTRODUCTION

Security of human life and property is one of the paramount challenges facing any nation or any corporate organization (Oke et al, 2013). Security systems are necessary everywhere especially in Banks, Houses, Offices etc. As the technology is evolving every second, intelligent security systems have been developed and implemented to prevent illegal invasion. Getting access to previous literatures to ascertain previous research at a glance was hard to come by, there is the need to carry out a literature survey to provide important information to researchers. The aim of the paper is to make a review of some of the existing work on intelligent lock system by recognizing the authors along with their concept and theory, discuss the merit and demerit of such system and proffers possible modification. Depending on the "security huddle' before gaining access, they will be categorized into single and multiple protocol system.

II.   CONCEPT OF INTELLIGENT LOCK SYSTEM

First step towards security was Lock and key system. Security protocol followed in this system was "Single key for a single lock". Initially, this system was considered to provide utmost security. But this belief was soon proved wrong by the fact that multiple keys can be easily made for a single lock (Anubala et al., 2014). Vehicles follow the same trends where early modern vehicle uses non-electronic key in order to restrict open and start access. If the key matches, the vehicle user is able to turn it and is thereby authorized to start and drive the vehicle. This kind of security mechanism does provide some protection against theft, but can quite easily be exploited by duplication of keys (Fathima et al., 2015). These aforementioned limitations necessitate the need for an intelligent lock system.

A system is a small part of the universe that we are interested in (Sen, 2006), which in this case is a lock. One of the most critical aspects of a truly intelligent system is the ability to learn, that is, to improve its own functionality by interacting with the environment and exploring it (Tomaso and Luigi, 1992). A standard intelligent lock system must have the following basic features: (1) Provides environmental monitoring, access control and management system. (2) Prevents unauthorized access. (3) Allows doors to be opened using a proximity card, keypad or via a web interface. (4) Accommodates sensors to monitor temperature, humidity, smoke, presence of water or liquids, etc. (5) automatically generates an audio alert. (6) Records all the security information you need every time the door opened – who, where and when (Home Security and Automation, 2017). Standard intelligent lock uses different sensor for the three basic component of access control ie: identification, authentication and confirmation as shown in Figure 1.
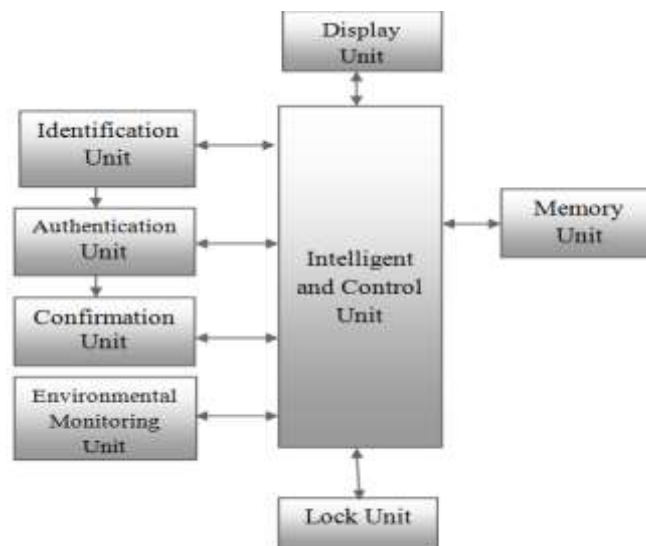
Figure 1: Block Diagram of Intelligent Lock

III.   REVIEW OF INTELLIGENT LOCK SYSTEM

There were several research works on intelligent lock system which were group into single protocol and multiple protocols depending on the number of security features. In this section, some of the authors along with the Concept and theory of their works will be highlighted. The advantages, disadvantage and possible improvement (research gap) were enumerated.

A.   Single protocol system

Geoffrey (2012), designed an RFID based automatic access control system. The USB serial communication was used to communicate with the host computer which is interfaced with the PIC 16f877A. Therefore, the graphic user interface program provides the functionalities of the overall system such as displaying live ID tags transactions, registering ID, deleting ID, recording attendance and other minor functions which were developed using visual basic 2010. Having feature for registering and deleting ID make the system more flexible but the system lack facilities for true user identification such as fingerprint scanner, camera etc. An improvement can be made on this system by RFID finger print scanner instead of Tag to rule the possibility of unauthorized access.

Srinivasa et al., (2013), worked on RFID based security system. The RFID module reads the data in the card and displays it on the LCD. The data in the card is compared with the data in the program memory and displays authorized or unauthorized messages. The RFID module actuates a buzzer whenever it reads the data from the RFID card. The system is simple and thus the failure rate is minimal. The system has no registration mode, no true user identification system and notification system in case of an intruder. An improvement can be made by adding more security features.

Hasan, et al (2015), designed a microcontroller based home security system with GSM technology. A mobile phone is interfaced with the microcontroller through a Bluetooth device in order to control the system. A manual keypad is another way to lock or unlock the system. It is a reliable security system because its bi-modal (parallel) nature, but the system lacks code registration mechanism and the microcontroller program lacks auto-generated code routine. Modifications can be made in the design by adding auto-generated code device and making the security features work serially, thus making it multiprotocol device.

Alagu et al., (2015), designed GSM based authorized access with separate user password door lock/unlock control system. SMS application sends data through GSM Modem. Another GSM device connected at the receiving end which is fed to the microcontroller. The microcontroller initiates a mechanism to open the door through a motor driver interface, if the sent data (password entered by the user) matches with the password stored in the microcontroller. This is simple and will give a good value for investment but the program in the microcontroller lacks auto-generated code routine. Improvement can be made by programming the microcontroller to generate codes.

Ushie et al., (2013), designed and constructed a prototype security door that can be remotely controlled. A GSM phone set acting as the transmitter and another GSM phone set with dual tone multi-frequency (DTMF) connected to the door motor through a DTMF decoder interfaced with microcontroller unit and a stepper motor. It provides an easy way of controlling a lock without physical contact, but the system lack true user identification system such as biometric and face detection facility. It also lacks notification and alarming system. An improvement can be made by adding another security feature to increase the security reliability.

Crystalynne et al., (2016), developed a microcontroller-based biometric locker system with short message service (SMS). The system scans fingerprint, match it with the saved pattern and unlock the locker. The global system for mobile (GSM) module was able to send text message containing the auto-generated pass code of the locker when an unrecognized fingerprint was encountered. It is a simple and reliable way of safeguarding a lock system, but the system has no registration mode mechanism to register finger pattern of new user. An improvement can be made by incorporating registration mode and adding another security features to increase the security reliability.

Nwankwo et al., (2013), designed security door that opened by pressing the keys of the assigned codes on the mobile phone, or by entering the corresponding code in a computer set interfaced with the system. The door opens automatically when the right code is entered and remains open for 10 seconds before closing back. The security system is affordable but lack auto-generation code and registration mode mechanism. An improvement can be made by adding biometric, auto-generation and registration mode mechanism.

Amit (2013), designed a GSM based automated embedded system for monitoring and controlling of smart grid. The device acquire the remote electrical parameters like Voltage, Current and Frequency from Smart grid and send these real time values over GSM network using GSM Modem/phone along with temperature at power station. It operates an Electromagnetic Relay. The Relay is used to operate a Circuit Breaker to switch off the main electrical supply. It is a good protective system but has no sensor and transducer for measuring environmental condition such as temperature, humidity etc. And improvement can be made by adding environmental condition measuring facilities.

Gowsalya et al., (2014), designed a system that work base on the principle of face recognition. If iris is matched, the door automatically will be opened otherwise it will remain close. Infrared sensor was used to detect the human in or out. It is a reliable security system but the system lacks other sensor(s) for sensing other parameters for physically impaired person (without iris). Modification can be made on the system by incorporating a biometric system to be used by such person.

Lia, et al. (2014), designed a system to simulate an electronic key, which is controlled through a Bluetooth-enabled smart phone. Controlling is conducted by sending a command via Bluetooth to the Arduino circuit that acts as an interface between the Android smart phone and solenoid. The security system is simple with low failure rate but lack notification system. Modification can be made by adding another security feature to increase the reliability of the security system.

Oke et al., (2013), developed a programmable electronic digital code lock system. In the design, a device is locked using a six digit code (password). The electronic code lock system was activated by switching to alarm mode when any wrong code is entered for four consecutive times and allows the user to stop it only when a proper 6-digit code is entered in the correct sequence. it is an affordable and simple security system, but the system lack notification facilities, registration mechanism to change the pass-code. Other security feature such as GSM system can be incorporated for notification information to dedicated person in case of any attempted intruder.

Anushri et al., (2015), designed a GSM based attendance monitoring systems which lock/unlock the door whenever the student sweeps the RFID tag near RFID Reader. The Student Details will be indicated on the LCD display and send through GSM SIM 300 Modem to parents to display whether the student is present or not. It is a reliable attendance base system especially with the feature of parent notification, but the system lacks registration mechanism and true identification system to alert the administrator of any manipulated intruder. The system can be improved further by adding registration mechanism, alarming mechanism and true identification system. Extending the system with Online Web based attendance system that can be made by providing the Student Database to the host Computer so that the Student's Record is to be updated automatically could also be feasible.

Anupriya et al, (2014), proposed a lock system that provides the MMS to identify intruder by sending MMS from transmitter phone to receiver phone. If anyone uses the system, image will be captured by using web camera. The captured image will be viewed in PC by using MATLAB and the image will be compared with the stored images, if it is matched with stored images the door will be automatically opened. If it is not matched, the image will be transmitted to mobile phone by using mobile data cable. After intruder detection the Alarm and Door Lock Gun will be activated by sending commands from receiver to transmitter. The main advantage of this technique is its high speed processing capability and low computational requirements, in terms of both speed and memory utilization but lack true identification system for a facially deformed user due to accident whose facial image was earlier captured. The system can be modified by providing another security feature to increase the security reliability of the system.

Lay et al., (2011), implemented a storage locker system. The system uses the technique of fingerprint recognition as the means to actuate the opening and closure of the lock. Biometric is a reliable security feature, but lack security feature for physically impaired person (amputee) and notification mechanism in case of an

intruder, An improvement can be made by adding another security feature(s) such as RFID system to take care of such people and to strengthen the security of the system.

B. Multiple protocol system

Komal and Dhiraj (2015) designed a Campus Access Management System based on RFID technology. The data from RFID reader is transmitted to a Centralized Remote Computer or Server located in the administrative office of the college through a RS-232 interface. The centralized server determines the authorization & access control rights. Access codes are entered through a Keypad. The entire program code was written in Microsoft Visual Basic 6.0 Software. This approach presents a highly coordinated attendance system, but the system lack secured security feature and alarming mechanism to notify the security. Modification can be made on this system by using biometric instead of RFID and alarming facility.

Ramani et al (2013), proposed a vehicle tracking and locking system based on GSM and GPS for car security system. These systems constantly watch a moving Vehicle and report the status on demand. When theft is suspected, the responsible person actuates the sending of SMS to the microcontroller, then microcontroller issue the control signals to stop the engine motor. The system will provide a good security system for vehicle, but is not linked to an online mapping system to give the exact location of the vehicle. The system can be improved further by extending the system with Online Web based monitoring system which should be linked to security agencies.

Hussaini et al., (2014), designed of a GSM-based biometric access control system. The Fingerprint Scanner automatically scans a finger placed on it, and compares it against its template. If a match exists, "Access Granted" is displayed on the LCD and the door is opened, otherwise, "access denied" is displayed. The GSM module is used in the acknowledgement mode to send an Access Request SMS to the Admin Phone (stating the user's unique 3-digit number), waits for the Admin to acknowledge the request. IF the admin acknowledges the request, the microcontroller opens the door and displays "access granted". If due to network errors or the admin refuses to reply for some time (30 seconds), the system automatically takes it as an access denied. Generally biometric system cannot be hacked easily but the system lacks an automated facility in the acknowledgement mode. This system can be enhanced by adding automated security facilities which acknowledge the user instead of admin personnel.

Raghu and Subhramanya (2013), designed and implemented a security lock based on RFID, Fingerprint, Password and GSM technology. The RFID reader reads the ID number from the passive tag and sends it to the microcontroller, if the ID number is valid, then it gives access to the fingerprint scanner otherwise it stops the process, if the fingerprint is matched then the microcontroller sends the password to the authenticated person mobile number then the authenticated person enters the passwords in the keyboard which was already given to the user and that received from the microcontroller. If these two passwords are matched then the locker will be opened otherwise the microcontroller sends a warning message to the authenticated person mobile number and it will be remain in lock position. The system is highly secured due the its multiple security features but the program in the microcontroller does not contain auto-code generation routine. An improvement can be made by making the microcontroller generates codes instead of predetermined passwords.

Gyanendra (2010), designs a digital door lock security system using the RFID technology. After receiving the tag information, the reader sends this information to the database for confirmation. If it holds, the information is stored for further operation. The central server queries to database and retrieve corresponding information after receiving the query from the reader. The reader computes timestamp (date, time) after receiving the reply form server and creates a log. Once the tag information is verified, the system generates a control signal through parallel port which controls the opening/ closing of door by means of stepper motor. Creating a log which contains information of the user is another vital security feature to the system, but it lacks notification and alarming facilities. The system can be improved by adding security feature(s) such as GSM module and buzzer.

Supraja, et al, (2014), designed a digital code lock system with a status display by using wireless communications RF technology and GSM technology. The wireless communications is established by using RF modules and a digital keypad interfaced to the controller. The authentication is provided through password for locking or unlocking the system and the status will be displayed using LCD module and the acknowledgement is provided to the user via the GSM technology. It is a highly secured system which is applicable to home security but program in the controller does not contain code generation routine and the system lack notification mechanism such as alarm. An improvement can be made by using camera to capture the image of the person entering the password. By applying "Digital Image Processing", the scanned photo gets compared with the predefined image of the authorized user in the system.

Prasanna and Hemalatha (2012), proposed an idea of solving problems arising in logistics management with the aid of wireless communication. The proposed system work as thus: If overloaded, a Buzzer is triggered. Vehicle starts to move from source to destination while GPS starts getting location and sending the details on Request. When the vehicle reaches destination the unloading of goods take place, also the RFID tag is read and

validation of tag takes place. If successful, user is allowed to access the goods, If not, SMS based indication will be provided. GSM will indicate the unloading details of goods on regular intervals. The misplacement of the goods is indicated with the help of a Buzzer. If misplaced goods are not reloaded into the vehicle, SMS will be sent to the base station and will not allow the vehicle to move. This approach is a secured way of guiding goods but system is not likened to an online Google map. An improvement can be made by considering misplacement of goods while unloading and the system should be linked to an online map for real time location.

Jaykrishan et al., (2014), designed a system in which the user unlocks the door using RFID system. If a wrong card is entered, then an SMS will be sent to the authorized person and an indication would be given to the security man by a buzzer, the SMS would be sent using GSM protocol. There would be a live streaming using a camera. DTMF is used to access the lock of the inside doors of the infrastructure using cell phone of the authorized person. It is a simple and affordable security lock system but the system lack no registration mode to allow for change of RFID ID number. Modification can be made by adding another security feature such as biometric system to increase the security reliability.

Srinivasan. And Krishnamoorthy (2015), designed a security system in which RFID reader reads the fingerprint from passive tag and sends it to the microcontroller, if the fingerprint is matched then microcontroller sends the password to the authenticated prisoner mobile number then the authenticated prisoner enters both passwords in the keyboard which was already given to the user and that received from the microcontroller. If these two passwords are matched then the locker will be opened otherwise the microcontroller sends a warning message to the authenticated prisoner mobile number. It is a secure way of guiding prison using multiple protocols. The system has no registration mode to allow for change of phone number and RFID number without altering the program in case of change of user. An improvement can be made on the system by incorporating registration mode and allowing the system to generate codes instead of using an established password

Prashantkumar et al., (2013), proposed a two wheeler vehicle security system in which the handle lock is operated by servo motor and controlled by the Remote Keyless System (RKS). The RKS has a transmitter and a receiver module. The receiver module is installed on the vehicle and the owner of the vehicle has the remote (transmitter module). The RKS remote could be used to lock/unlock the locking system (handle lock, fuel lock and rear wheel lock), switch ON/OFF the engine and to turn off the alarm. A Short Message Service (SMS) is sent to the registered SIM via the Global System for Mobile communication (GSM) module whenever the vehicle is unlocked using the RKS remote. Owner can in turn send a SMS to initiate the locking sequence, if he/she feels an unauthorized person has unlocked the vehicle. Global Positioning System (GPS) module is used to track the location and monitor the speed of the vehicle. Piezoelectric sensors are used as vibration sensors to detect any tampering with the vehicle. It is highly secured security lock for vehicle but the program used in the RKS is not Hopping code algorithm and the system is not linked to online mapping facilities to determine the exact location. Enhancement could be made on this system by using Hopping code algorithm in Remote Keyless System (RKS) for added security and an online mapping system linked to security agencies for easy detection in case of theft.

Sandeepet al. (2014), proposed a locking system for a cargo container. The electromechanical Lock is controlled by a Relay, which is locked after loading the consignment and the monitoring system gets activated. Once the door is locked, it will not get opened in any case until it reaches the destination. If in case it is tampered, the buzzer which is provided gets activated for alert. The monitoring system keeps sending status message to the vehicle to check and track the Cargo location. The monitoring front end was designed using VB.NET, interfaced with Google map for mapping the cargo. Once the vehicle reaches the destination, a message is sent to the monitoring system. If the coordinates matches then a password is sent to the person who is collecting the consignment. Once the password is entered, a LCD displays "swipe the RFID Card and enter password". Upon the card swiping and password entering, if these two parameters are accurate only then the door opens, otherwise the monitoring system gets a tampering message. This is highly secured means of guiding goods but the password generating mechanism is not automated. The password generating mechanism should be automated with auto-code routine. The reliability of the system can further be improved by hardware redundancy, effective design and code reviews

Priti and Zadem (2014), proposed a car security system that can add various images to database and with the help of face recognition technology. when any person enters into car then it compares image of that person with the existing images in the database, if the person is an authorized user, access will be granted and if not access to the car is blocked and the car owner will be informed about the unauthorized access with the help of Multimedia Message Services (MMS) by using GSM modem. Also it can provide password authentication in such case if the car owner wants to give emergency access to some user whose image is not in the database. In addition it can also perform accident detection in order to provide security to the users. In this case message will be sent to nearest police station or hospital. It is a highly reliable car security system but the system lack alarming facility

to alert a nearby person of an intruder. The system could be modified by adding an alarming system and using biometric system instead of face recognition to reduce the production cost.

Senthil and Praveen (2013), designed a lock system that is armed automatically when the driver moves away from the vehicle. It is disarmed only when a specific gesture is made in the hand-held wireless key fob. The 3D gesture is made in mid-air and can be reprogrammed by the user on the fly. The air gesture is recognized using a 3-axis MEMS Accelerometer that senses the gravitational force exerted upon it. A stolen key fob thus cannot be used to enter into the vehicle without performing the secret gesture. The password is stored in an external non-volatile memory. If the gesture is valid the key fob transmits a unique encrypted code that changes every time when this gesture is made. It is an intelligent approach to car security but lack notification mechanism such as short message services (SMS) and alarming system. Security feature such as notification mechanism and face recognition technology could be added serially to increase security reliability.

Manasee and Reddy (2013), designed an automation system based on wireless technologies. Door opening and closing is controlled by RFID, ZigBee and GSM. Temperature monitoring, gas detection and light controlling is developed using GSM. When user wants to enter the room he/she can place his/her valid RFID card on the reader. If valid RFID card is detected by the system, the gate opens and closes after some delay. If invalid card get detected alarm start ringing, so that we get information about invalid user. It is a highly secured system, but the system is not program to make the maximal use of the incorporated GSM technology. The system can be expanded with further security measures by sending information to the emergency call centre using GSM technology. Information about fire can be send to fire station; intruder detection information can be send to police station.

Mohan and Vinoth (2014), developed a home security system in which whenever the system notices human intrusion or senses leakage of raw gas, it immediately sends a Theft or Sensor alert message to the authorities via the GSM Modem and Passing alert messages to nearby ZigBee networked houses, and also the controller triggers the exhaust fan in the case of gas leakage. It has a password protected electromagnetic lock to open and close the house using GSM technology. In the case of owner's absence in the house, the system takes over the control of all the equipments, and saves the energy by turning-off unused electrical appliances. It is highly secured multipurpose system, but the program lack auto-generation routine (password). Modification can be made adding auto-generation routine in the program and adding another security feature in parallel (hard ware redundancy) to reduce the failure rate.

Fathima et al., (2015), proposed an intelligent security system for vehicles in which the manufacturer initializes the immobilizer and near field communication (NFC) tag with authentication key. The manufacturer also installs the smart secure mobile application in smart phone which is NFC enabled. The vehicle user reads the authentication key from NFC tag using NFC reader and stores the key in encrypted form. When it is necessary to unlock the vehicle, smart phone is placed closer to immobilizer. After placing, immobilizer reads the key and decrypts the key. Then immobilizer verifies the key with authentication key. If it is matched, it unlocks the vehicle; otherwise it sends an alert message. It provides more security to the vehicles using secure hardware, but lack vehicle location facilities and notification mechanism to notify the owner of an intruder. An improvement can be made by the combination of biometric, GPS and GSM technology, i.e. biometric for unlocking, GPS to locate the position of vehicle and GSM for notification.

IV.   CONCLUSION

A review of an intelligent security lock system is here presented by citing the authors along with their individual concept and theory. The merits and demerit of their respective approaches were enumerated and possible modifications were suggested. While it is impossible that any system can be made to guarantee absolute security, identifying the threats and assessing the risks are vital steps toward improving security.

REFERENCES

[1] Alagu L. R., Anandhajothi, A. & Selvakumari, P. (2015): GSM based authorized access with separate user password door lock and unlock control system, International Journal of Electrical And Electronics Engineers (IJEEE), Vol. 07 (01), pp 388-391.

[2] Amit, S. (2013): GSM Based Automated Embedded System for Monitoring and Controlling of Smart Grid, World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol. 7(12), pp 1748-1752.

[3] Anubala, B., Rahini, M. & Bavithra, T. (2014): Intelligent Door Locking System. International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 International Conference on Humming Bird, pp 50-53.

[4] Anupriya, S., Elakya, P., Kamatchi, B., Manasa, D. & Rohini, G. (2014): Advanced Entry Level Protection System for Theft. International Journal of Computer Networks and Communications Security, Vol. 2 (4), pp 125–128.

[5] Anushri J, Vijay L K & Barkha N (2015): RFID and GSM Based Attendance Monitoring System using door locking/unlocking system and Its Hardware Implementation, Journal of Management Engineering and Information Technology (JMEIT), Vol. 2 (3), pp 5-10.

[6] Crystalynne, D. C., Jaswinder, S. B., Jocelyn, R. H., Ditche, J. C. A., Melvie, S. D. C. & Jaira, C. I. (2016): Development of Microcontroller-Based Biometric Locker System with Short Message Service" Lecture Notes on Software Engineering, Vol. 4 (2), pp 103-106.

[7]   Fathima G. DivyaBarathi A, Jaya S & Manjushree R (2015): Intelligent Secure System for Vehicles, International Journal for Scientific Research & Development (IJSRD), Vol. 3 (02), pp 438-442,

[8]   Geoffrey, C. T. S. (2012): Automatic Access Control System using Student Identification Card Based on RFID Technology, Unpublished Undergraduate Project of Faculty of Electrical Engineering Universiti Teknologi Malaysia, pp 1-4.

[9]   Gowsalya, M., Sangeetha, M., Sri, D. K. K., Divya, N. & Devika, T. (2014): A Novel Approach Automatic Digital Door Opening and Closing Security System, International Journal of Innovative Research in Electrical, Electronic, Instrumentation and Control Engineering, Vol. 2 (2), pp 991-996.

[10]   Gyanendra, K. V. & Pawan, T. (2010): A Digital Security System with Door Lock System Using RFID Technology, international Journal of Computer Applications, Vol. 5(11), pp 6-8.

[11]   Hasan, R., Khan, M. M., Ashek, A. & Rumpa, I. J. (2015): Microcontroller Based Home Security System with GSM Technology, Open Journal of Safety Science and Technology, **5**, pp 55-62.

[12]   Home Security and Automation (2017): Intelligent Lock and IP Controlled Access, Retrieved on 18th April, 2017 from: https://cpisecurity.com/

[13]   Hussaini, H., Adamu, M. Z, Ajagun, A. S., Ijemaru, G. K. & Oresanya, B. O. (2014): Design of a GSM-Based Biometric Access Control System Control Theory and Informatics, Vol.4(8), pp 1-21.

[14]   Jaykrishan, P., Joyson, B., Ketan, P., Viral, P., & Ramanuj, G. (2014): Armoured Infrastructure using Multiple Protocols, International Journal of Computer Science and Information Technology Research, Vol. 2 (4), pp: 170-174.

[15]   Komal, K. M. & Dhiraj, G. A. (2015): Campus Access Management System via RFID, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Vol.4 (8), pp 23-27.

[16]   Lay, Y. L., Yang, H. J. & Tsai, C. H. (2011): Biometric Locker System, Proceedings of the World Congress on Engineering and Computer Science (WCECS) 2011, San Francisco, USA, Vol. I, pp 1-4.

[17]   Lia, K, Alfin, N. S. R, Mada S. W. S. & Edi, M. (2014): Door-Automation System Using Bluetooth-Based Android for Mobile Phone, Asian Research Publishing Network (ARPN) Journal of Engineering and Applied Sciences, Vol. 9 (10), pp 1759-1762.

[18]   Lynn, A. D & Anne, L. O. (2009): RFID and Application Security, Journal of Research and Practice in Information Technology, Vol. 41 (3), pp 209-221.

[19]   Manasee, P. & Reddy, S. R. N. (2013): Design and Implementation of Home/Office Automation System based on Wireless Technologies, International Journal of Computer Applications, Vol. 79 (6), pp 19-22.

[20]   Mohan, P. & Vinoth, K. M. (2014): Development of Individual Home Security System Using CAN and ZIGBEE Protocol, International Journal of Research in Engineering and Technology, Vol. 03 (07), pp 581-585.

[21]   Nwankwo, P. N., Nsionu, I. I. & Ezeilo, C. J. (2013): Design and Implementation of Microcontroller Based Security Door System (Using Mobile Phone & Computer Set), Journal of Automation and Control Engineering, Vol. 1 (1), pp 65-69.

[22]   Oke, A. O., Adigun, A. A., Falohun, A. S., & Alamu, F. O. (2013): Development of a Programmable Electronic Digital Code lock system, International Journal of Computer and Information Technology, Vol. 02 (01), pp 127-131.

[23]   Prasanna, K. R. & Hemalatha, M. (2012): Secure Logistic Management System Using Wireless Technologies, Research Journal of Applied Sciences, Engineering and Technology, Vol. 4 (12), pp 1785-1789.

[24]   Prashantkumar, R., Sagar, V. C., Santosh, S. & Siddharth, N. (2013): Two Wheeler Vehicle Security System, International Journal of Engineering Sciences & Emerging Technologies, Vol. 6 (3), pp 324-334.

[25]   Priti, K. P. & Zadem, G. N. (2014): Real time Car Antitheft System with Accident Detection using AVR Microcontroller; A Review, International Journal of Advance Research in Computer Science and Management Studies, Vol. 2 (1), pp 509-512.

[26]   Raghu, R. G. & SubhramanyaSarma, G. (2013): Locker Opening and Closing System Using RFID, Fingerprint, Password and GSM, International journal of emerging trends & technology in computer science (IJETTCS), Vol. 2 (2), pp 142-145.

[27]   Ramani, R., Valarmathy, S., Suthanthira, V. N., Selvaraju, S., Thiruppathi, M. & Thangam, R. (2013): Vehicle Tracking and Locking System Based on GSM and GPS, I. J. Intelligent Systems and Application, (IJISA.), pp 86-93.

[28]   Sandeep, S. R., Feroz, M., Sadiya, T. & Mohamed, N. S. (2014): Tracking and Checking Cargo Containers Pilferage Using Electronic Lock, International Journal of Technical Research and Applications, Vol. 2 (5), PP 113-116.

[29]   Sen, M. (2006): Lecture Notes on Intelligent Systems, Department of Aerospace and Mechanical Engineering University of Notre Dame, Notre Dame, IN 46556, U.S.A.

[30]   Senthil, K. T. & Praveen, K. (2013): Design of Next Generation Auto Theft Prevention System, International Journal of Scientific Engineering and Technology, Vol. 2 (3), PP 133-136.

[31]   Supraja, E., Goutham, K. V., Subramanyam, N. & Dasthagiraiah, A. (2014): Enhanced Wireless Security System With Digital code lock using RF &GSM Technology, International Journal of Computational Engineering Research (IJCER), Vol. 04 (7), pp 80-85.

[32]   Srinivasan, J. & Krishnamoorthy, M. (2015): Implementation of GSM Technology in Prison Locker System, International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), Vol. 12 (4), pp 15-18.

[33]   Tomaso, P. and Luigi, S. (1992): A Project for an Intelligent System: Vision and Learning", International Journal of Quantum Chemistry, Vol. 42, pp 727-739.

[34]   Ushie, J. O., Donatus, E. B. O. & Akaiso, E. (2013): Design and Construction of Door Locking Security System Using GSM. International   Journal   of   Engineering   and   Computer   Science,   Vol.   2   (7),   pp   2235-2257.