International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Finger Print and NFC Base Secure Authentication for Safe Lock

N. Nivetha

Assistant professor, Dept of Electronics and Communication Engineering, Unnamalai Institute of Technology, Tamil Nadu, India

Abstract

This paper proposes an idea on developing a Near Field Communication (NFC) Smart Lock System that utilizes a smart phone's on-board NFC chip as a method to unlock a door. Access is regulated using a NFC Smart Card which runs a simple user interface that allows an Administrator to grant or deny entry to any particular user. The goal for this project was to give access to particular user. Access will be given to the user by using NFC Smart Card. Every NFC Smart Card contains Unique Identification (UID) Number, by using UID we grant or deny entry to user. It is working on NFC door lock that will be available to the general public at an affordable price. The goal of this project is to create a more convenient way to unlock your door than the traditional key. In the key's place is an NFC tag that will unlock the door by proximity. However, the improvements of this NFC door lock must outweigh the complications of implementation. The list of customer needs (in the Requirements and Specifications section) was constructed with that fundamental goal in mind. The design consists of two components. The first component is the actual door lock that must be installed in the door frame. This will be controlled by a magnetic lock and will need to be powered. The second component is a relatively small module that you can install anywhere near the door. This module is responsible for the NFC sensing.

Keywords: Identification, proximity, NFC, Smart card, Magneticlock.

1. Introduction

Near Field Communication (NFC) is a technology for contactless short-range communication. Based on the Radio Frequency Identification (NFC), it uses magnetic field induction to enable communication between electronic devices. The number of short-range applications for NFC technology is growing continuously, appearing in all areas of life. Especially the use in conjunction with mobile phones offers great opportunities. One of the main goals of NFC technology has been to make the benefits of short-range contactless communications available to consumers globally. The existing radio frequency (RF) technology base has so far been driven by various business needs, such as logistics and item tracking. While the technology behind NFC is found in existing applications, there has been a shift in focus most notably, in how the technology is used and what it offers to consumers. With just a point or a touch, NFC enables effortless use of the devices and gadgets we use daily.

NFC works on the principle of sending information over radio waves. Near Field Communication is another standard for wireless data transitions. This means that devices must adhere to certain specifications in order to communicate with each other properly. The technology used in NFC is based on older RFID

(Radio-frequency identification) ideas, which used electromagnetic induction in order to transmit information.

This marks the one major difference between NFC and Bluetooth/Wi-Fi. The former can be used to induce electric currents within passive components as well as just send data. This means that passive devices don't require their own power supply. They can instead be powered by the electromagnetic field produced by an active NFC component when it comes into range. Unfortunately, NFC technology does not command enough inductance to charge our smartphones, but QI wireless charging is based on the same principle.

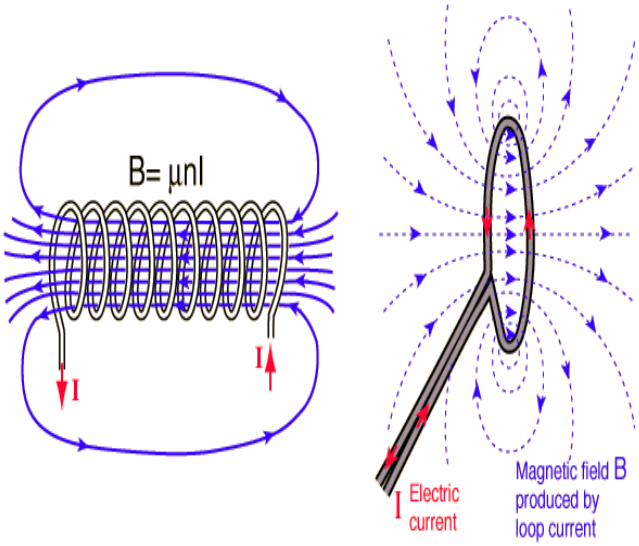

Fig 1.1 Electromagnetic field

Electromagnetic fields can be used to transmit data or induce electrical currents in a receiving device. Passive NFC devices draw power from the fields produced by active devices, but the range is short.

The transmission frequency for data across NFC is 13.56 megahertz. You can send data at 06, 212, or 424 kilobits per second. That is quick enough for a range of data transfers from contact details to swapping pictures and music.

To determine the sort of information will be exchanged between devices, the NFC standard currently has three distinct modes of operation. Perhaps the most common use in smartphones is the peer-to-peer mode. This allows two NFC-enabled devices to exchange various pieces of information between each other. In this mode, both devices switch between active when sending data and passive when receiving.

Read/write mode, on the other hand, is one-way data transmission. The active device, possibly your smartphone, links up with another device in order to read information from it.

1.1 Comparisons with Bluetooth

NFC compare with other wireless technologies. We might think that NFC is a bit unnecessary, considering that Bluetooth has been more widely available for many years. However, there are several important technical differences between the two that gives NFC some significant benefits in certain circumstances. The major argument in favor of NFC is that it requires much less power consumption than Bluetooth. This makes NFC perfect for passive devices, such as the advertising tags mentioned earlier, as they can operate without a major power source.

However, this power-saving does have some major drawbacks. Most notably, the range of transmission is much shorter than Bluetooth. While NFC has a range of around 10 cm, just a few inches, Bluetooth connections can transmit data up to 10 meters or more from the source. Another drawback is that NFC is quite a bit slower than Bluetooth. It transmits data at a maximum speed ofjust 424 kbit/s, compared to 2.1 Mbit/s with Bluetooth 2.1 or around 1 Mbit/s with Bluetooth Low Energy.
But NFC does have one major advantage: faster connectivity. Due to the use of inductive coupling, and the absence of manual pairing, it takes less than one-tenth of a second to establish a connection between two devices. While modern Bluetooth connects pretty fast, NFC is still super handy for certain scenarios namely mobile payments

1.2 Development of NFC Technology

The introduction of Near Field Communication (NFC) technology, the mobile phones already had several types of communication options with the external environment .When the mobile phones were introduced, the primary need was to setup voice communication, it was primarily provided by Global System for Mobiles (GSM) which has other services such as SMS, MMS and even internet access. Later Bluetooth technology was introduced that connects peripherals with computing devices including mobile phones In present days, a new communication technology known as NFC is becoming popular in mobile smart phones. This technology needs two NFC compatible devices placed very near to each other (less than 4cm) in order to communicate. NFC operates at 13.56 MHz and can transmit information up to a maximum rate of 424 Kbits per second. In an NFC communication, two devices are needed. First device is called the initiator which is an active device and is responsible for starting the communication, whereas second device is called the target and responds to the initiator's requests. The target device may be active or passive. The communication starts when the active device gets close to the target and generates a 13.56 MHz magnetic field and powers the target device.

2. PROPOSED SYSTEM

The proposed system utilizes Near Field Communication (NFC) technology which on interfacing with the locker provides access to the locker. This method provides advanced level of safety and security rather than a digital pass code or fingerprint scanner.

1. **Fingerprint used to open bureau**

- Biometric door locks or smart locks are devices that allow us to unlock your door with the combination of a fingerprint and PIN. Smart locks typically cost a few hundred dollars and allow you to authorize several people to unlock your door.
- It operates by scanning and converting your fingerprint data into a numerical template. Once you place your finger onto the scanner for the first time the conversion into numerical data takes place, and the fingerprint template is saved.

2. **SMS verification done by approved number**

- Click on the "SMS Phone Number" button. Next, click on the "Get SMS Token" button. A 6-digit code will be sent to your cell phone number to ensure you have access to the cell phone number you entered.
- SMS verification is a common way to add a second form of verification to apps. By sending an SMS message containing a one-time-code like "1234" or "481236" to the user's phone number, they can then enter the code into your app to confirm that they received the SMS message.

3. HARDWARE MODULE

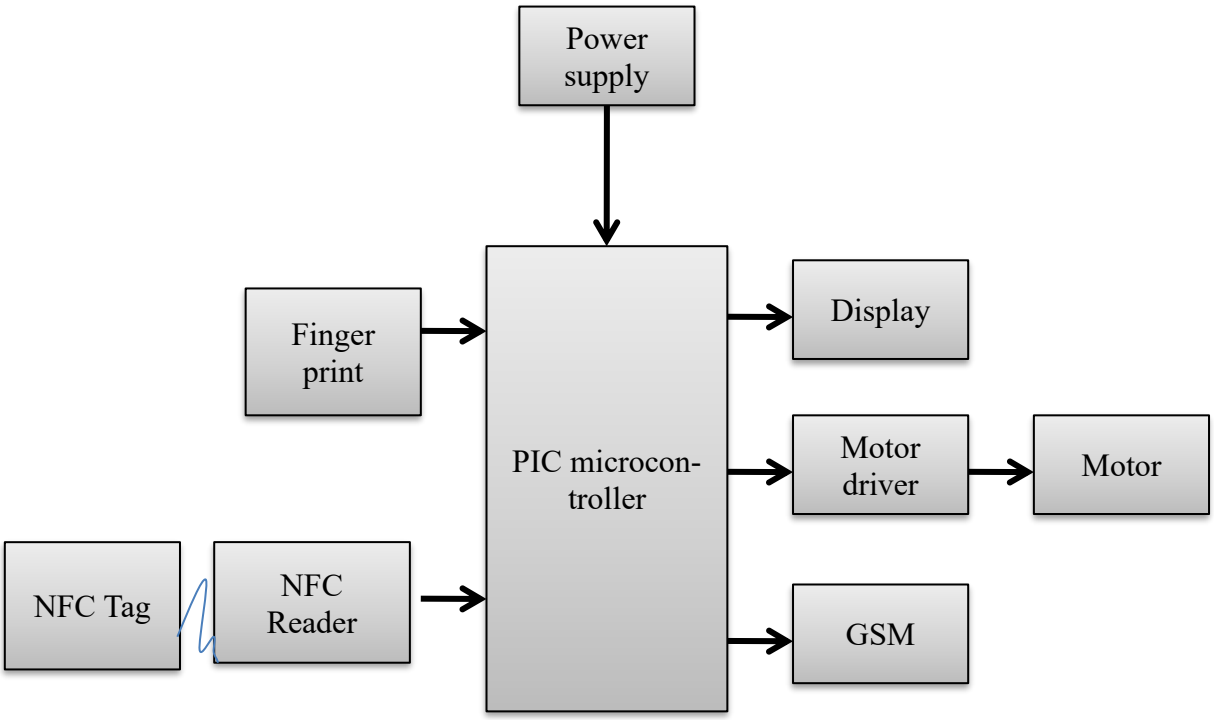

Fig: 4.1 Block Diagram for Fingerprint and NFC Base Secure

3.1 PIC Microcontroller

Microcontrollers with Harvard architecture are also called "RISC microcontrollers". RISC stands for Reduced Instruction Set Computer. Microcontrollers with von-Neumann's architecture are called 'CISC microcontrollers'. Title CISC stands for Complex Instruction Set Computer. Since PIC16F877 is a RISC microcontroller, that means that it has a reduced set of instructions, more precisely 35 instructions. All of these instructions are executed in one cycle except for jump and branch instructions. PIC16F87 usually reaches results of 2:1 in code compression and 4:1 in speed in relation to other 8-bit microcontrollers in its class.

3.2 Fingerprint

It is an impression left by the friction ridges of a human finger. The recovery of partial fingerprints from a crime scene is an important method of forensic science. Moisture and grease on a finger result in fingerprints on surfaces such as glass or metal.

3.3 NFC - Near Field Communication

It is a technology that allows devices to exchange information simply by placing them next to one another. Smart phones use NFC to pass photos, contacts, or any other data you specify between NFC-enabled handsets. Just like Bluetooth and Wi-Fi, and all manner of other wireless signals.It works on the principle of sending information over radio waves. Near Field Communication is another standard for wireless data transitions. Passive NFC devices draw power from the fields produced by active devices, but the range is short.

3.4 NFC tags

Tags are passive devices, which mean that they operate without a power supply of their own and are reliant on an active device to come into range before they are activated. In order to power these NFC tags, electromagnetic induction is used to create a current in the passive device.

3.5 GSM Module

It is mainly used for mobile communication. GSM module is connected to microcontroller for sending and receiving of messages. It is used that supports communication in 9000MHz band. This GSM module requires a 12V power supply. The block of GSM modules are enabled by interfacing GSM modem to PCB and giving outputs for RS232. The data can be feed from GSM module to PIC microcontroller through the output pins.

3.6 GSM - Global System for Mobile communication

GSM could be a mobile communication modem; it's stands for world system for mobile communication (GSM). GSM is employed for transmission mobile voice and knowledge services. They're operated at the 850MHz, 900MHz, 1800MHz and 1900MHz frequency bands that are an open and digital cellular technology. Standing indicator can flashes unceasingly whenever the decision arrives otherwise it's left ON. Network junction rectifier can blink each second that indicates that the GSM module isn't connected to the mobile network. The LED blink continuously for every 3 seconds, when the connection is established and in off state when the connections aren’t established.

Fig:3.2 GSM Module

3.7 GSM SIM 800C

SIM800C is a widely used GSM Module with a serial interface modem which runs in between 3.4V-4.4V Voltage level. SIM800C is a Quad-band GSM/GPRS Module which is used in embedded applications where the remote data transfer is required. SIM800C works on 850/900/1800/1900MHz. It can also receive & transmit Voice Call, SMS with low power consumption. The module is controlled by using AT

commands. It supports one SIM card interface and has UART (TX &RX) pins along with one RS232 Serial Protocol that can be used to interface with different microcontrollers in embedded applications.

3.8 LCD – Liquid Crystal Display

LCD includes some microwatts for show compared to some mill watts. Liquid Crystal Display could be a combination of 2 states of matter, the solid and therefore the liquid. Liquid is employed to provide a comprehensible image in liquid crystal display. The liquid crystal display works on the principle of obstruction lightweight. When compared to LED and cathode ray tube, LCD is thinner. Blocking light principle is used for the working of LCD. This is used to display the weight of the gasoline content.

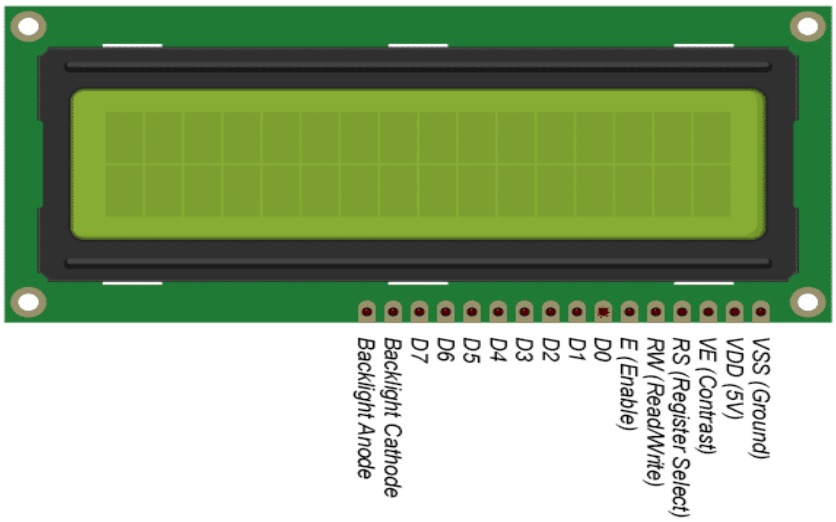

Fig 3.3 LCD Display

3.9 DC MOTOR

The DC motor is a machine that transforms electric energy into mechanical energy in form of rotation. Its movement is produced by the physical behavior of electromagnetism. It has inductors inside, which produce the magnetic field used to generate movement A DC motor is used to drive a mechanical load. In this lab, a separately excited DC generator provides the load. The load on the motor is adjusted by varying the generator field current. By increasing the field current of the DC generator, the load on the DC motor increases and thus the armature current increases. In general, DC motors are characterized by their torque-speed curves as shown in Figure. Since the measuring equipment for shaft torque is not available in the lab it is necessary to use alternative means of characterizing the DC motor. One alternative is to plot shaft speed versus armature current since torque is directly proportional to the armature current ($T = K_a \phi_d I_a$) with a constant field current supplied to the motor. Shaft speed is also a function of the field current in a DC motor while maintaining a constant armature voltage ($E_a = K_a \phi_d \omega$) as field current is directly proportional to the direct axis flux produced in the machine.

3.9.1 Construction

The stator of the dc motor has poles, which are excited by dc current to produce magnetic fields. In the neutral zone, in the middle between the poles, commutating poles are placed to reduce sparking of the commutator. The commutating poles are supplied by dc current. Compensating windings are mounted on

the main poles. These short-circuited windings damp rotor oscillations. The poles are mounted on an iron core that provides a closed magnetic circuit. The motor housing supports the iron core, the brushes and the bearings. The rotor has a ring-shaped laminated iron core with slots. Coils with several turns are placed in the slots. The distance between the two legs of the coil is about 180 electric degrees. The coils are connected in series through the commutator segments. The ends of each coil are connected to a commutator segment. The commutator consists of insulated copper segments mounted on an insulated tube. Two brushes are pressed to the commutator to permit current flow. The brushes are placed in the neutral zone, where the magnetic field is close to zero, to reduce arcing. The rotor has a ring-shaped laminated iron core with slots. The commutator consists of insulated copper segments mounted on an insulated tube. Two brushes are pressed to the commutator to permit current flow. The brushes are placed in the neutral zone, where the magnetic field is close to zero, to reduce arcing. The commutator switches the current from one rotor coil to the adjacent coil; the switching requires the interruption of the coil current. The sudden interruption of an inductive current generates high voltages. The high voltage produces flashover and arcing between the commutator segment and the brush.

4. Working Principle

An NFC reader/writer is connected to a Microcontroller which reads the details of the user from the NFC smart phone. The Microcontroller then checks if the d is an owner d or a guest d. If it is a guest d, it verifies it with the code provided to the GSM module. For this and the previous condition, if the NFC smart d code matches with the required data. It will send a signal to the servo motor to rotate to either locked or unlocked state.When the servo motor is in the locked state, a red LED will be on and the LCD screen will display that the door is locked, and when the servo motor is in the unlocked state the green LED will be on and the LCD screen will show that the door is unlocked. Android provides an adaptive app framework that allows you to provide unique resources for different device configuration.

5. REQUIREMENTS

5.1 Hardware Requirements

- PIC Microcontroller
- Power Supply
- Microcontroller
- GSM
- Display
- Motor

5.2 Software Requirement

Embedded System

6. Result Analysis

The result has been analysed based on the connection in kit for Fingerprint and NFC base secure authentication for bureau lock are shown in figure. So the process is completed by connecting the kit for Fingerprint and NFC base secure authentication for bureau lock and getting the data for analyzing.

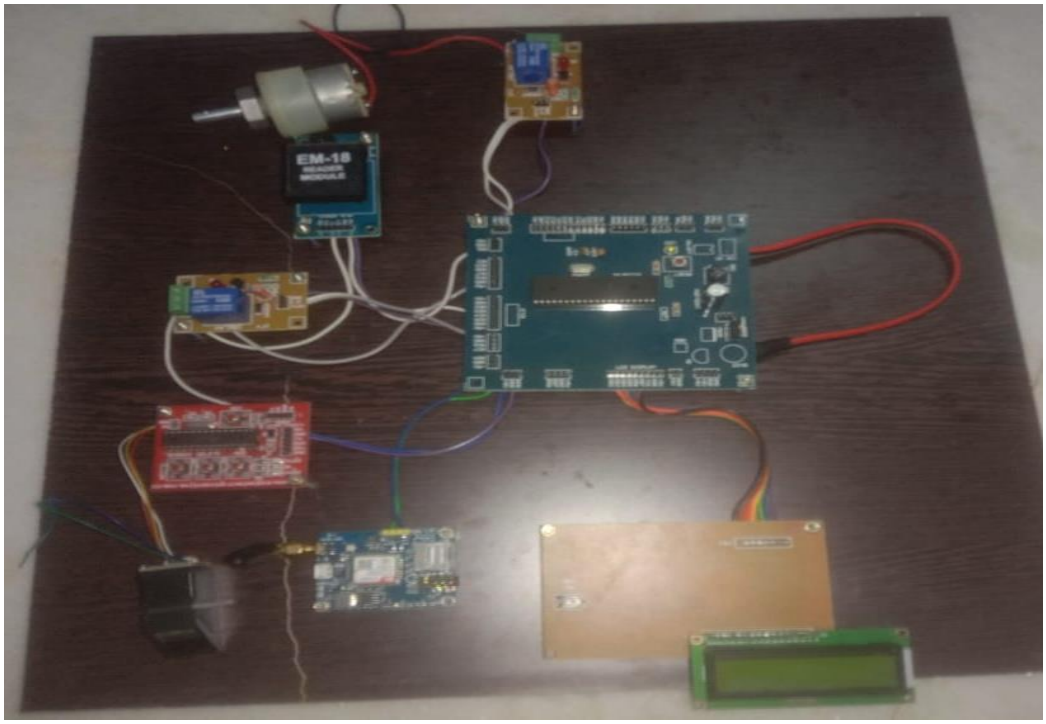

Fig 6.1Total connection of Fingerprint and NFC base secure authentication for bureau lock .

7. CONCLUSION AND FUTURE SCOPE

7.1 Future Scope

- Fingerprints keep the customer information safe.
- Security analysis and threat modelling shown in this work highlights the security strength of the system during authentication.
- As a future work, we will expand this project to even control home appliances, which in turn, will improve the lifetime of the home appliances (high efficiency)since the human intervention is minimal and also provides good safety and security.

7.2 Conclusion

Finally, the NFC based door locker system has been designed. This system provides high reliability and enhanced security for the lockers. If this system is practically put into use, it will work efficiently and gives more protection. It will also relieve the tension of all the people about the safety in the lockers. NFC technology can be used in many other applications. NFC can also be used to control home appliances. This project concludes, allow only access granted user and stop the access deny user. It works based on Door Security using NFC Technology. By using NFC tags, we control the access to user. NFC based security and access control system is more secure and fast responded as compared to the other system like biometric. The advantage of the NFC system is contact-less and works without-line-of-sight.

References

1. Peng-Loon Teh, Huo-Chong Ling, Soon-Nyean Cheong, “NFC Smartphone Based Access Control System Using Information Hiding,” IEEE Conference on Open Systems (ICOS), December 2013.
2. HasooEun,“Conditional Privacy Preserving Security Protocol for NFC Applications,” IEEE Transactions on Consumer Electronics, Vol. 59, No. 1, February 2013.

3. Muhammad QasimSaeed, Colin D.Walter, “Offline NFC Tag Authentication,” The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012).
4. EskoStrömmer, Marko Jurvansuu, TuomoTuikka, ArtoYlisaukko-oja, HarriRapakko, JarmoVesterinen, ”NFC-enabled Wireless Charging,” 4th International Workshop on Near Field Communication,2014.
5. JukkaRiekki, Ivan Sanchez, MikkoPyykkönen,”NFC-Based User Interfaces,” 4th International Workshop on Near Field Communication, 2014.
6. Charl A. Opperman,Gerhard P. Hancke,” Using NFC-enabled Phones for Remote Data Acquisition and Digital Control,” IEEE Africon 2011 - The Falls Resort and Conference Centre, Livingstone, Zambia, 13 - 15 September 2011.
7. B. Beny,A. Vilmos,K. Kovacs, L. Kutor,”The Design of NFC Based Applications,” International Conference on Intelligent Engineering Systems ,29 June - 1 July, 2007.
8. AA Hussein, and AA Mohammad, "Near Field Communication (NFC)," International Journal of Computer Science and Network Security,vol. 12(2),pp. 93-100,Feb. 2012.
9. J.Christian, J.Scharinger, and Gerald, "NFC Devices: Security and Privacy," in Proc. of the 2008 Third International Conference on Availability,Reliability and Security,pp. 642- 647,2008.
10. D.Bhattacharyya, R.Ranjan, F.Alisherov, and M.Choi, "Biometric Authentication: A Review," International Journal of Science and Technology,pp. 13-16,Sept. 2009. [11] S Malhotra, “Banking Locker System With Odor Identification & Security Question Using Rfid&Gsm Technology”, 30 September, 2014.
11. F. Aloul, S. Zahidi, and W. El-Hajj, "Two Factor Authentication Using Mobile Phones," in IEEE/ACS International Conference on Computer Systems and Applications, vol. 6, pp. 641-644, May 2009.
12. AA Hussein, and AA Mohammad, "Near Field Communication (NFC)," International Journal of Computer Science and Network Security, vol. 12(2), pp. 93-100, Feb. 2012.
13. J. Christian, J. Scharinger, and Gerald, "NFC Devices: Security and Privacy," in Proc. of the 2008 Third International Conference on Availability, Reliability and Security, pp. 642-647,2008.
14. C.H. Dubin, "Get Smart About Access Control," International Journal of Electronics Applications, vol. 2,p p. 112-115, Oct. 2011.
15. S. Narayana, and G. Prasad, 'Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions," International Journal of Signal and Image Processing, vol. 1(2), pp. 60-73, Dec. 2010.
16. C.H. Hung, Y.W. Bai, and J.H. Ren, "Design and implementation of a door lock control based on a near field communication of a smartphone," in 2015 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), June 2015, pp. 45-46.
17. Prof.Benazir.H.M Dept. of ECE, Nisha S. Kalpathri, ChandralekhaSunagar, Shaikh Collage of Engineering and Technology, Belagavi, India “Fingerprint Authentication Smart Locking System Using OTP”, International Journal of Advance Research in Engineering, Science & Technology, vol 4, Issue 6, June-2017.
18. Mr.PatilBhushan S, Mr.Mahajan Vishal A, Mr.SuryawanshiSagar A, Mr.PawarMayur B, Prof.Mr.U.R.Patole, “ Automatic Door Lock System using PIN on Android Phone”, International Research Journal of Engineering and Technology, vol 05, Issue 11, November 2018.
19. Sri Prakash N, Venkatram N. “Establishing efficient Security scheme in home IOT device through biometric finger print technique”. Indian Journal of Science and Technology, 2016 May