IOT based EMF data transfer for Electronic Locking System

Project report submitted in the fulfilment of the requirement for the degree of Bachelor of Technology

in

Information Technology

By

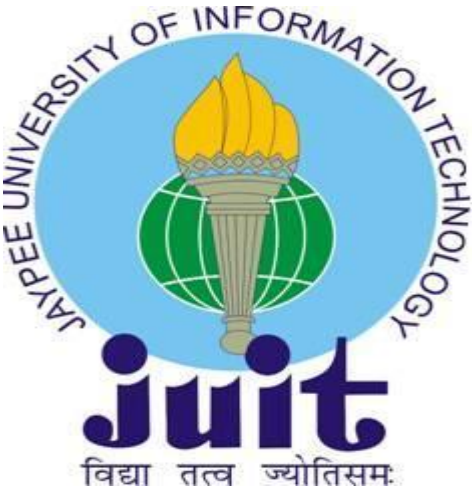
Diksha (131410)

Divyanshu (131411)

Under the supervision of

Dr. Punit Gupta

to



Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh

Candidate's Declaration

I hereby declare that the work presented in this report entitled **"IOT based EMF data transfer for Electronic Locking System"** in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology Waknaghat is an authentic record of my own work carried out over a period from January 2017 to May 2017 under the supervision of **Dr. Punit Gupta** (Designation and Department name).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

(Student Signature)

Diksha, 131410

Divyanshu Goel,131411

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

(Supervisor Signature)

Dr. Punit Gupta

Assistant Professor (Grade II)

Department of Computer Science Engineering,

Date: May 1,2017

ACKNOWLEDGEMENT

Every project big or small is successful largely due to the effort of a number of wonderful people who have always given their valuable advice or lent a helping hand. We want to sincerely acknowledge the guidance; support and inspiration of all those people who have been involved in making this project a success.

We are highly indebted to Dr. Punit Gupta for his constant supervision and guidance as well as for providing all the necessary information regarding this project & also for his support in completing the project.

We would also like to thank our parents &the member of JUIT for their kind co-operation and encouragement which help us in the completion of this project.

We would like to thanks the University Faculty for giving us such time and attention.

My thanks also go to my classmates and people who helped me with their capabilities in developing this project.

Diksha(131410)

Divyanshu(131411)

Date: May 1,2017

Table of Contents

List of Abbreviations

	ABBREVIATON
EMF/emf	Electromagnetic Field
IoT	Internet of Things
I/O	Input or Output
&	And
Chars	characters
i.e.	that is

List of Figures

List of Tables

Abstract

Recently, door locks have been used, as a part of the Internet of Things (also called as IoT) digital. However, the opening or closing of door locks by invalid visitors to enter illegally in homes and offices, many times media has been reported these issues. In this project, an EMF based door locking system that is working with the IoT environment has been proposed. Basically to enhance security and convenience of the authorized users, this project has been proposed and implemented.

There is a necessity for cost efficient EMF data transfer electronic door locking system to be designed because this project is able to provide much more security than the other ordinary mechanical door locking systems. Keeping all these problems in mind, this project is working on **IOT based EMF data transfer for Electronic Locking System**. We want to apply the electronic technology to develop a fully customized and integrated IOT based electronic locking system at low cost. We believe that this project will be effective in keeping unwanted persons or thieves and other kind of dangers away. Through the use of this system, the doors can be locked/unlocked by using pre-defined password, which will increase the security level to protect the houses from any unauthorized locking or unlocking. If in any case the user doesn't remember the password or its combination, this system will give the user a flexibility to reset the password. The thing that cannot be denied is the efficiency of this locking gadget. To design an Electronic Door Lock with Arduino Technology is one more purpose of this project. In this project, the most important work undertaken is to sense the correctness of a secret code i.e. the password with the help of Arduino technology. When the correct password is entered through mobile application, a small solenoid starts operating, which when powered, then can transfer the password or secret code to other solenoid and that code is checked from the server, if correct the door lock or unlock as selected by the user.

Chapter-1

INTRODUCTION

This chapter gives a concise introduction about the work, which defines all the components namely Electro-mechanical Door Lock, Arudino platform. Followed by the design of unlocking of Electro-mechanical Door Lock by Arudino Technology using EMF. Locks for doors are exactly considered to be as the basic modes of the day to day household door and also keeping this in mind, locks hold an huge importance for the protection of doors from illegal or unauthorized unlocking. Efficiency of the electronic locking gadget can definitely not be denied. The main aim of the task undertaken in this paper is to check the correctness of the password using the Arduino technology on server only. When the correct code or password is entered with the help of mobile application, a small solenoid starts operating, which when powered, then can transfer the password or secret code to other solenoid and that code is checked from the server, if correct the door lock or unlock as selected by the user.

1.1 Introduction

EMF:

An electromagnetic field (also called EMF) is the physical field which is being produced by electrically charged objects. This science of electromagnetism was developed by many workers. One of the most important workers for this was Michael Faraday. Another was, James Clerk Maxwell, who put the laws of electromagnetism in the same form as one knows them today. That laws are called Maxwell's equations and also plays the same role in the electromagnetism as Newton's laws of motion in the mechanics.

Maxwell described that in nature light is electromagnetic and its speed can be found by making electric and magnetic measurements purely. Thus, the optics science was informally connected with the electricity and the magnetism. Electromagnetic field has been extended indefinitely throughout the space and also describes the electromagnetic interaction.

This EM field can also be viewed as the combination of the magnetic field and the electric field. This force is one of the four fundamental forces of nature that are gravitation, strong interaction and weak interaction.

Throughout the course of history of electromagnetism, from a classical perspective the EM field can be thought as a continuous, smooth field, propagated in wave manner; whereas from the prospect of quantum field theory, this field can be seen as a quantized, which is supposed to be composed of individual particles. For Maxwell's equation scope is remarkable,

because it covers the fundamental principle of electromagnetic on large scale and optical devices, like motors, computer systems, cyclotrons, radio, microwave radar, TV(television), microscope and the telescopes. The behaviour of charged objects is affected by EMF in the vicinity of the field. In short, Maxwell's equations as well as Lorentz force laws defines the way how current and charge interact with the help of EMF.

Electromagnetism takes two forms. Maxwell's equations are being used continually and universally in solution of vast variety of problems that are practical, at the level of application of engineering. There is a progressing effort to enhance its scope in a way that electromagnetism is reported as the special case of a general theory, at the level of the theory foundations.

A point function is the continuous function of the position point in the region of space. A field is a region of space where it stipulates a physical quantity. Fields like these are restricted into two groups that are:

The Scalar field: This is defined as the region of space, where each point is connected with a scalar point function, that is, the continuous function which delivers the value of physical quantity which is connected by means of surfaces known as level or equal surfaces.

The Vector field: This is specified by the continuous vector point functions which have the magnitude and the direction, two of which change from one point to another point, in a given region of the field. Method of a presentation of the vector field is known as lines of surfaces or vector lines. Tangent at the vector line gives direction of the vector at a point.

The electromagnetic field may be categorized in two distinct ways: a discrete structure or a continuous structure.

Continuous structure

Electric and magnetic fields produce smooth motion of the charged objects. Here, continuously energy is transferred through the EMF between any two places. Examples of smooth motion can be charges that are oscillating produces electric as well as magnetic fields that can be seen as in wavelike trend, smooth and continuous.

Discrete structure

The EMF can be in a more 'coarse' way. In some of the situations electromagnetic energy transfer can be described in a quite better way as being carried in the form of packets called quanta (in this case, photons) with a fixed frequency which is revealed from the Experiments. Planck's relation is the link between the energy E of a photon and its frequency ν through the equation.

$$E=h\vartheta$$

where h = Planck's constant

ν = the frequency of the photon

This quantum picture of the electromagnetic field given the rise to quantum electrodynamics, and has been proven to be very successful, a quantum field theory describes the interaction of electromagnetic radiation with charged matter.

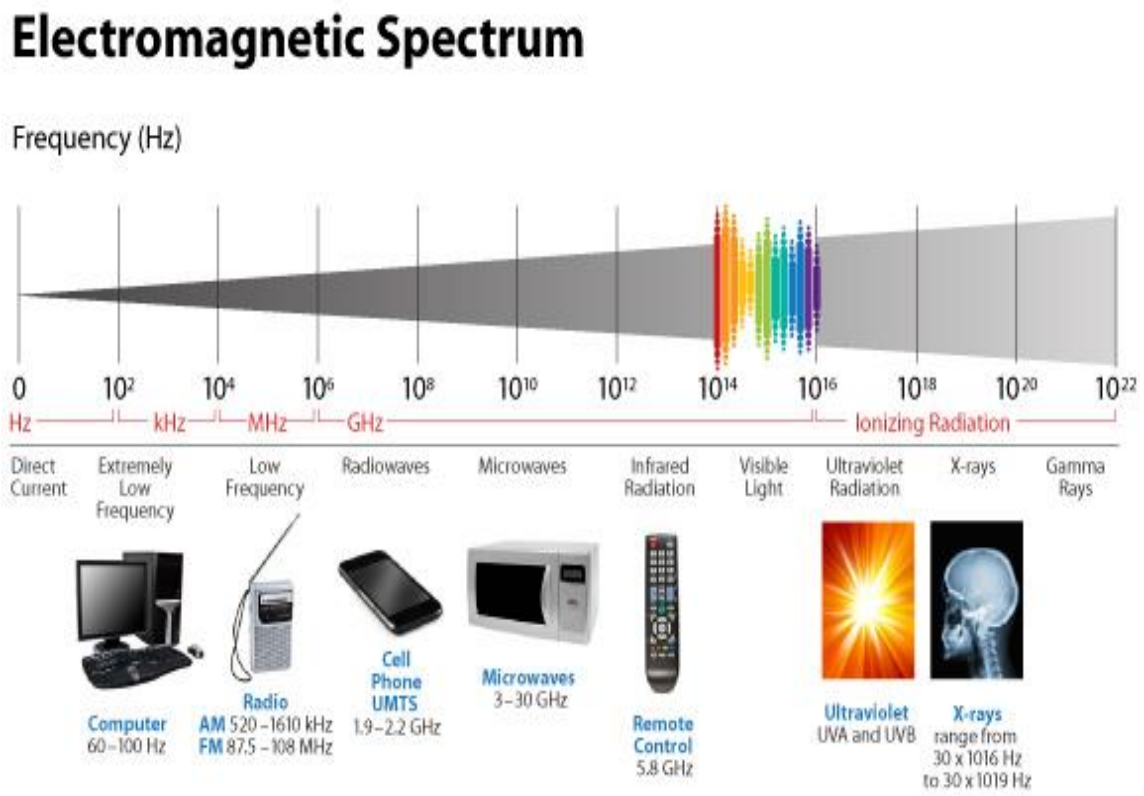


Fig 1.1 Electromagnetic Spectrum

Arduino

Arduino microcontroller can be used in design and art as an open source programming tool to create various interactive works. It is able to drive motors, sensors, LEDs, and various other components. The Microcontrollers are small systems for computing and are used for various purposes like for low memory as well as for low power. A microcontroller has a microchip on the circuit board with various read-write capabilities, inputs, outputs and memory. Microcontrollers also had a presence in arts and design for decades, an Arduino microcontroller is made up of the first microcontroller which is specifically designed for the designers and the artists.

It has a license which allows everyone to improve Arduino, build or expand Arduino. This licence drove to a popular platform with some of its extensions. The authentic Arduino with its development environment was launched in 2005 in Smart Projects company in Italy. After one year, this project won the award at Prix Ars Electronica. Several clones were made that usually contains some of the improvements and also are compatible with Arduino as well as with its development

environment. These clones were not allowed to carry the name i.e. Arduino, but e.g. FreeDuino (a name that everyone can use), Boarduino, Roboduino (calculated for the designing of the robots) and few others were allowed. Microcontroller correlates to an ATmega family which was manufactured by the company Atmel in Norway.

There are various flavours of Ardunio that are Arduino BT, Arduino LilyPad, Arduino Uno, Arduino Mega, Arduino Leonardo, Arduino Mini, Arduino Nano, Arduino Mini Pro. But we are using **Intel Galileo Gen 2.**

An Intel Galileo is basically a microprocessor hardware-compatible, software-compatible, and pin-compatible with having a large range of the Arduino Uno* R3 shield. It come up with the previously installed operating system like Linux and is also able to boot from a custom build Linux version which is installed on the micro-SD card. With this Intel Galileo the user is able to use either an Arduino IDE or can enable ssh and is able to use the command line in order to run the programs in of her own choice programming languages, like C or Python. An evident distinction between Gen 2 Intel Galileo and Gen 1 Intel Galileo is basically the power supply which it requires. An Intel Galileo Gen 2 needs 12 Volt power supply on the other side an Intel Galileo Gen 1 works with only 5 Volt power supply.

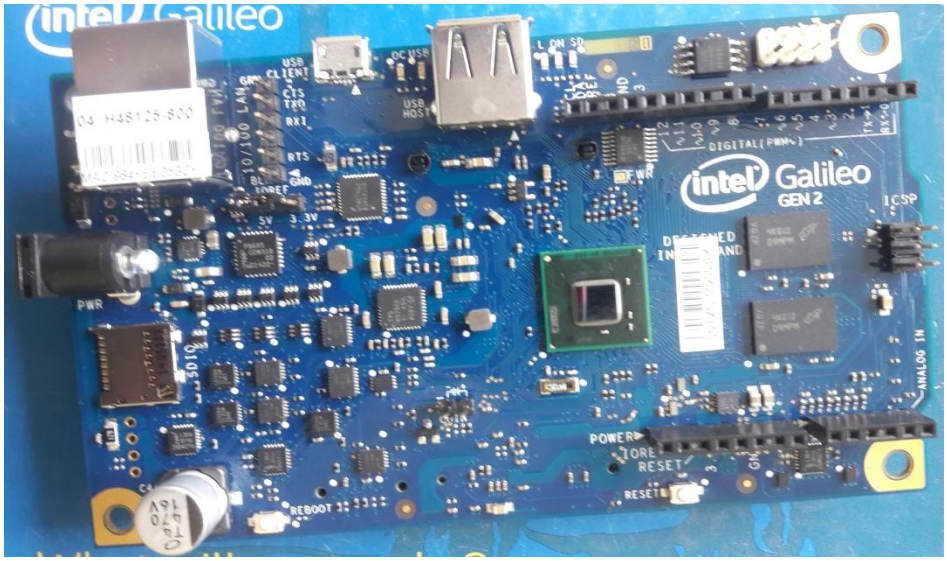


Fig 1.2. Arduino

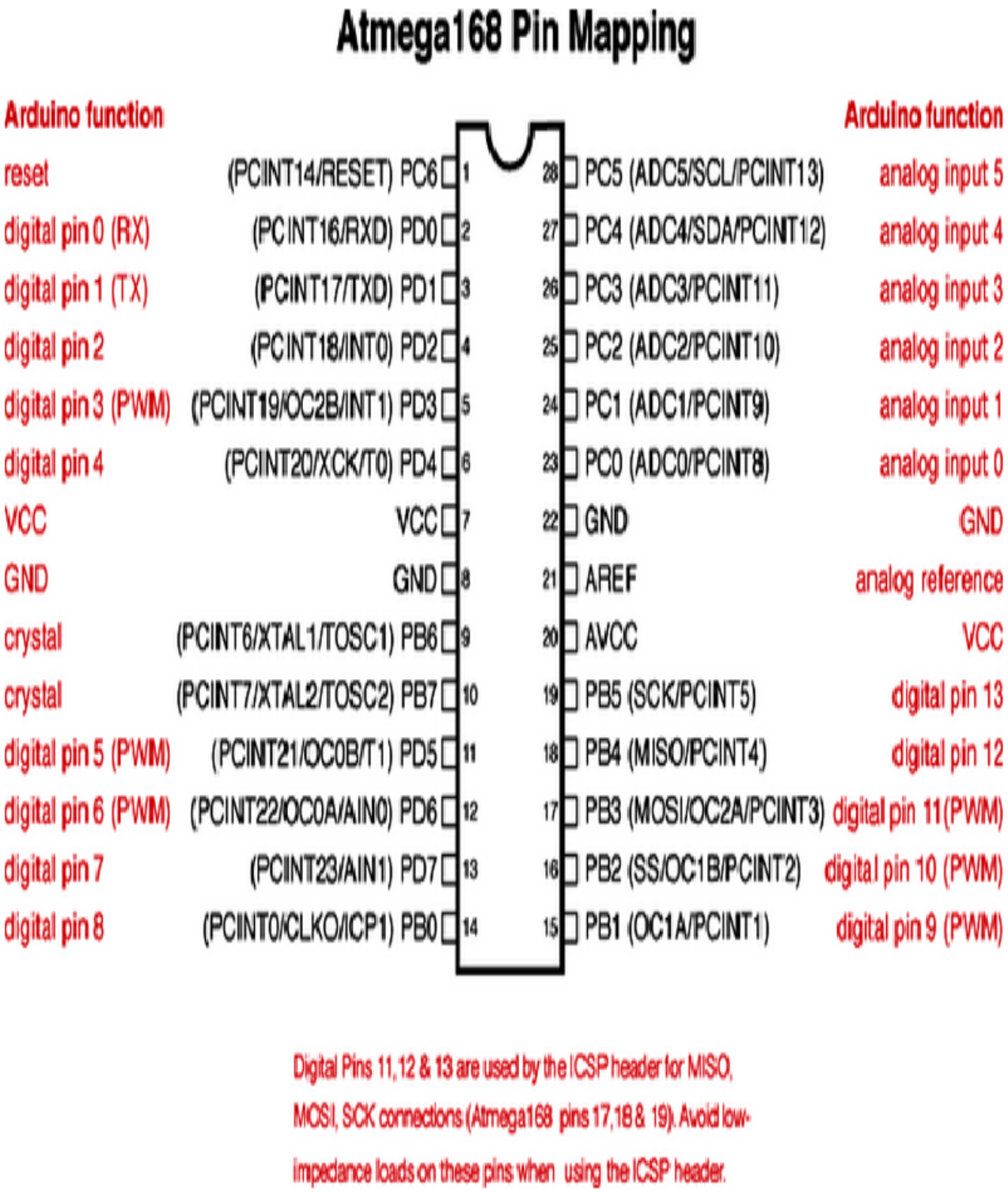


Fig1.3 Arduino pin mapping

Various steps to use Intel Galileo Gen 2

Install and then Open Arduino IDE.

Go to the Tools firstly and then to the Board menu, now select Intel Galileo Gen 2

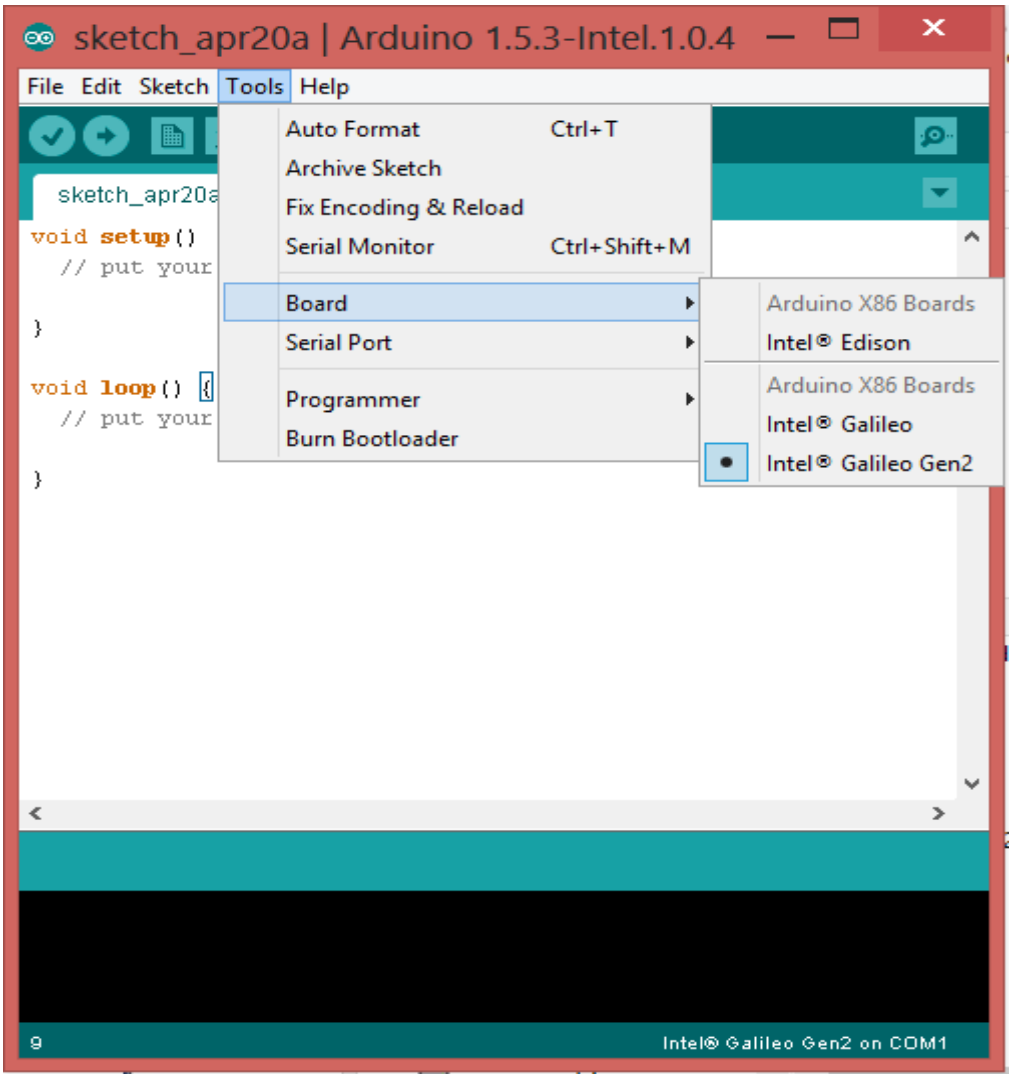


Fig1.4 screenshot of selecting board

Secondly go to the Tools and then to Serial Port, now select the COM number in that on which Intel Galileo Board was appeared to be connected in the Device Manager Ports Section (COM5 here in our case)

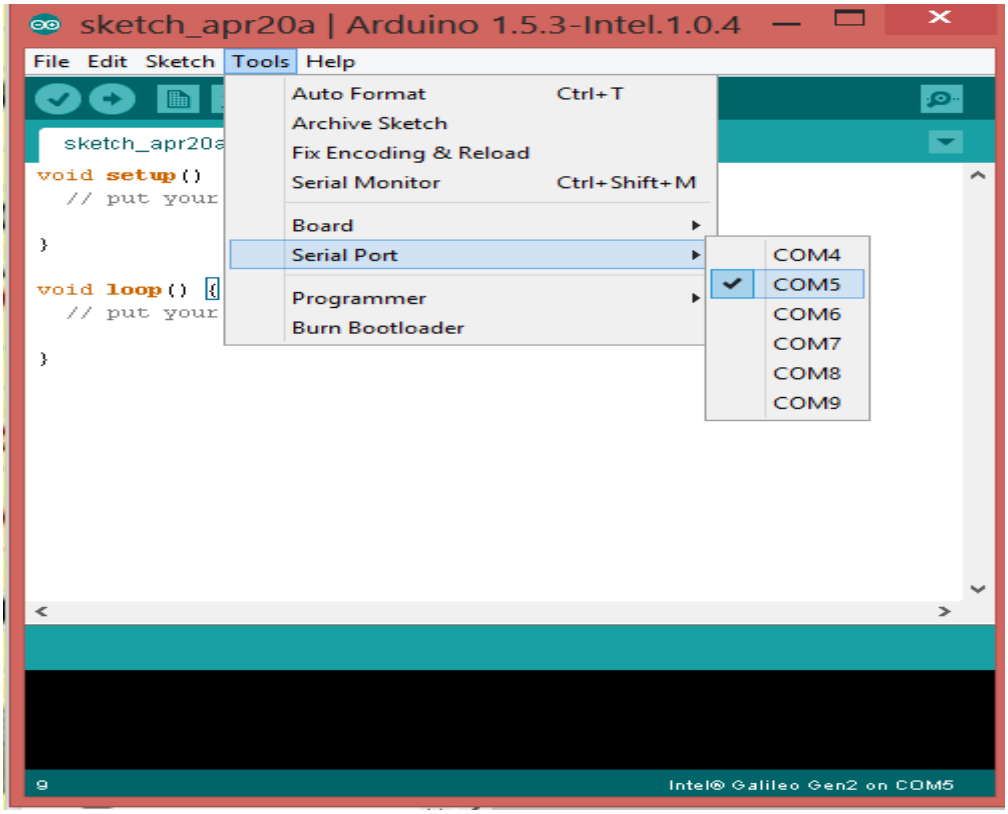


Fig1.5 screenshot of selecting serial port

Thirdly Go to File then to Examples then Basic and select Blink

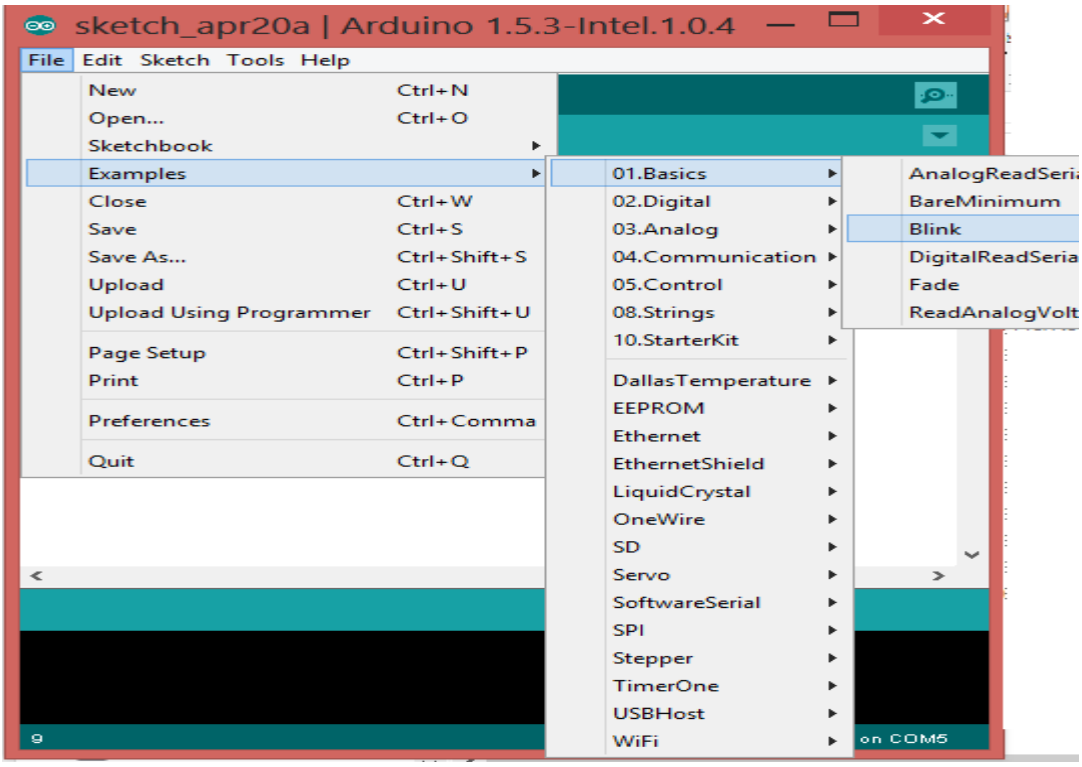


Fig1.6 screenshot of selecting example

Then a program will open that blinks the little Light Emitting Diode next to “ON” on your board. Now wait for Transfer to complete.

Advantages

It is Cheap – With respect to other microcontroller platform that is Arduino boards are comparatively inexpensive.

It is Open source software- Software of Arduino is an open source tool, which is available for the extension by experienced programmers.

It has Cross-platform - Windows, Linux operating systems and few others run on the software of the Arduino.

It is Simple and also has the clear programming environment - The programming environment of Arduino is easy-to-use for the beginners, and is also flexible enough so that advanced users can also take the advantage.

Summary

Voltage for operating	5 Volts
ATmega Microcontroller	168
Recommended Input Voltage	7-12 Volts
Limits of Input Voltage	6-20 Volts
Memory (Flash Memory)	16 KB of ATmega168 and 32 KB of ATmega328
Digital Input/Output Pins	14 (6 are provided for PWM output)
Input Pins (Analog)	6
Speed of Clock	16 MHz
DC Current per Input/Output Pin	40 milli Ampere
For 3.3V Pin DC Current	50 milli Ampere
Static RAM	1 KB (ATmega168) or 2 KB (ATmega328)
Electrically Erasable Programmable ROM	512 bytes (ATmega168) or 1 KB (ATmega328)

Data Encryption:

If the data is send from point X to point Y in private manner, then you need the tools to accomplish the data that is unreadable in carrying.

There is large number of applications where this communication type can be proved profitable. For instance, generals may wish to send the commands to the troop members over a long distance so that the enemy will not be able to interrupt and read the disclosures, revolutionaries may wish to practice in secret to avoid danger from being detected, or a supporter of the online merchant may be willing to send the credit card number of his/her account on the internet for a purchasing. All of these stages require that individual is able to conduct discussion with other individuals without the fear of an auditor who can listen to the conversations.

This can be done with the help of various ways, and throughout the succession of the history, humans had involved themselves in the process of developing new and significant ways to send the secure messages as well as new ways for eavesdroppers too, to get access to those secure messages.

In the creation of automated systems that are used to send the data from point X to point Y, we have a number of tools that can be operated on arbitrary input data to apply ordinary unencrypted text into a meaningless written text that can be only understood by our intended recipient.

Encryption is a term that is used to refer to be operated on the input string to produce the clipper-text (gibberish), and decrypted outlines the reverse procedure of taking the clipper-text and doing operations on it to convert it again into plaintext. As we already know that what is meant by algorithms, so it should be understood when one says that the specific process which he/she will be using to encrypt are known as encryption algorithms, and naturally the reverse termed as decryption algorithms, and also the term clipper is used to deduce these processes. Such algorithms take the input string as input and do various operations on it in association with the key to encrypt or to decrypt the data. As per our requirements, we can choose one of the algorithms from, first where the encryption and the decryption key are same known as symmetric cryptography, and second where the encryption and the decryption key are different known as asymmetric cryptography.

Encrypted and Decrypted Keys:

These keys are provided as the input into the algorithm to deliver the random unencrypted data into an encrypted data, or vice verse. As we know, the miracle of mathematics which is working under the hat to use the keys in powerful ways. What we need to be known about is that a key is basically a buffer or can be said as byte string. Before moving on, let's qualify what is exactly meant by that, in order to prevent any kind of confusion. The most literal sense of Byte string here is a continuous string of bytes. Added to this is to make sure to keep the key as effortful to guess as possible. The key is digital means that there is a need to make sure we must limit the degree with which transient copies of this can be made and that unauthorized individuals must be unable to get the access to that value. All This basically means that we wanted to be sure that one protected the keys; one used the keys with care.

IoT:

The **Internet of things** (also known as **IoT**) is basically the internetworking of connected devices (can be referred to as physical devices and also the smart devices), vehicles, building and various other items that are embedded with the software, electronics, actuators, sensors, and network connectivity between them that enable these devices/objects for collecting and exchanging the data from one another. The IoT is described as "infrastructure of information society" by the IoT-GSI (Global Standards Initiative on Internet of Things) in 2013.

The Internet of Things grants objects to be controlled and/or sensed remotely across the existing network infrastructure, and create opportunities for numerous direct integration of physical world into the computer-based systems, as well as results in efficiency improvement, improved accuracy and various economic benefits.

When Internet of Things is build up with the sensor and the actuator, this technology becomes an example of the more generic class of the cyber-physical systems, that also encircles technologies like smart grids, intelligent transportation , smart homes and smart cities. Each and every thing can be uniquely identified, through its installed computing systems and is able to operate in itself within the Internet infrastructure which already exists. Experts estimate that Internet of Things will consist of approximately 50 billion objects till 2020.

Things, in Internet of Things, can refer to a huge variety of devices for example heart monitoring implants, electric clams in the coastal water, the automobiles with some built-in sensors, biochip transponders on the animals that are in farms, DNA analysis devices for food/ environmental /pathogen monitoring or for the field operating devices which can assist fire fighters basically in search as well as in rescue operations. The Legal Scholars suggested by having a look on the word Things as the "inextricable mix of software, hardware, data and the services". The above devices can collect effective data with help of different existing technologies, after that autonomously flow data between various other devices. Now Current market examples cover smart home devices (also known as home automation) for instance the automation and control of lighting, ACs(air conditioning systems), air purifiers, heating (like smart thermostat), ventilation, and appliances like washer/dryers, ovens or refrigerators/freezers, robotic vacuums that use Wi-Fi for the remote monitoring.

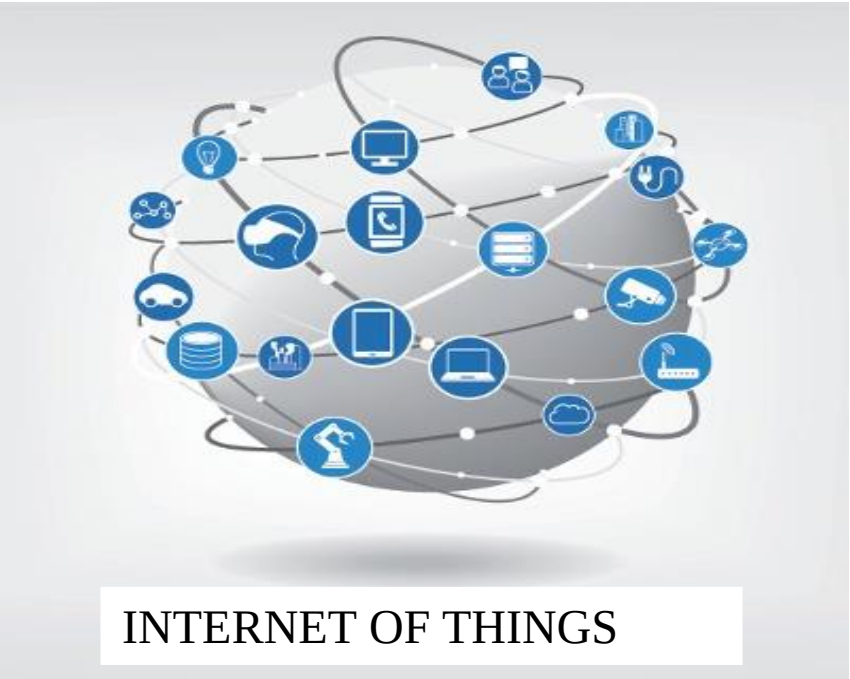


Fig 1.7 Internet of Things

1.2 Problem Statement

As everyone knows that the lock and the keys always go together, also a combination lock that does not had a physical key, but still had some kind of key(example a sequence instead of a physical artefact). When we start to considering about it, all of us have a plenty number of locks: of their cars, their houses, their file cabinet at the workplace, etc. From all those locks, each lock is designed to do same thing: allow a group of people (or a particular person) to have an access to a specific place. Digital keys also have the similar functions. Digital keys restrict the access to the resources, the data, and application functionality, and also prevent from gaining the access of unauthorized users.

Before moving ahead to the digital ones let's review various properties of physical keys. Clearly, we all know the following about keys that we encounter in our day to day life:

- There is a need to protect the key, while it is being used.
- There is sometimes need to replace the key.
- There is a need to safely store the key, while it is not being used.
- Keys are different in size as well as in shape correspondingly to function (example house key and car key looks different)

In the real world, there is always a need to have the secure access to the keys. Precisely, one should make sure that the user he/she wants to have the access to him do, and the user he/she doesn't want to have the access to him don't. If the keys govern the access to a specific resource, one should make sure to give the key only to that user whom he/she trust; as an analogy to this, everyone also knows that there is a need to restrict the opportunities from untrustworthy user to borrow, steal, or make various copies of a key.

There were all sorts of indirect variations to whom, on when and how the distribution of the key takes place. For instance, one might has an apartment in a building, then want superintendent to have an access to every apartment in a specific building, or may be employed as manager in an office and then have to maintain the master key of all the offices in the place of work in case of any emergency. For the limited access to the key one should have a place to store the key safely until that is distributed to the authorized user. Sometimes, if the key is lost somewhere, and don't know where it was lost, and now it is unsafe as somebody who may not be trusted upon pick up the key and can have access to it.

For instance, if one is not at her home, she might give the keys to trustworthy user that is to the good neighbours so that the maid can come and is able to clean our house. Also there can be a fear that is some confusion, if she had left the door unlocked and is on a vacation might haunts her often. Or want to keep door locked in order to protect the kids while they are alone at home. In short to increase/enhance the security and the convenience is basically the main concern that is the protection from unwanted person to enter the houses and the offices as well as there is demand of a low cost design of an electronic security system for the home as it can provide much more security as compared to the ordinary mechanical lock.

1.3 Objectives

The IoT (Internet of Things) can be described as the global framework which is used to combine the intelligent services along with the awareness from the situations, as well as allows the mutual information transfer between two things and also between the intelligent things and people over a particular network. IoT is different from M2M (i.e. Machine to Machine) communication because a person is not able to directly control the intelligent instruments or equipment; as they are only responsible for the communication on the behalf of people.

Recently, the variation in communication technology has been merged to provide and receive information about the things. Exclusively, IoT technology has been able to exchange information by amalgam of devices like mobile and home appliances.

In our study, we had designed and implemented an EMF-based electronic door lock to enhance various monitoring functions and the security using Internet of Things technology.

1 Security of all the objects or the places plays an important role, in everyday life. Our project had given consideration about that as well as constructed a secure access for the door for which a password is needed to open a specific door.
2 If Battery Goes Out: There is a possibility of an alternate key which can be physical or digital which he/she might not always carry with them, in our project battery can be charged through the EMF induced.
3 The biggest threat is that if malicious user hack and may get the access of the home from any remote location. Our project had taken care of this also.

1.4 Methodology

Wireless communication: Communication basically means the transfer of information from one source to its recipient/ destination. In conventional telephony, when the source and the destination were situated over long distances, then the transfer was usually happened by connecting the source and the destination physically by conducting the wires, which carry the information in form of electrical signals.

Now, Wireless Communication that is the main concept for this project. It can be defined as the communication between two or more points or nodes when there is no physical electrical conductor present.

It generally works with the help of electromagnetic signals that are being broadcast within air, physical atmosphere or environment by an enabled device. The sending devices can be the senders or the intermediate devices which has the ability to propagate the wireless signals. Communication between any two machines occurs when the receiving intermediate device or the destination captures the signals, and creates a communication bridge wirelessly between sender and the receiver machine. It has various technology and forms that includes:

- Satellite communication
- Wireless network communication
- Mobile communication
- Bluetooth communication
- Infrared communication

The most common technology that is wireless which is used is a radio. The range of space-radio communications and radio communication are alike that is as short as a minor meter to as far as even millions of kilometre. This radio communication can also be of various types that include fixed, portable, and mobile applications like two way radios, cellular telephones, wireless networks and GPS units. Various other applications of the radio communication are television remotes, PDA (i.e. Personal Digital Assistants), computer accessories that are wireless such as mice, garage door openers, keyboard and headsets, RFID tags, cordless telephones etc.

One of wireless communication technology is **Bluetooth Technology.** The main function of Bluetooth technology is that it allows everyone to connect to a variety of distinct wireless electronic devices to a particular system for exchanging the data. Wireless keyboard are there, mobile phones connected to earpieces that re hands-free, mike and mouse to the laptops

with the help of the Bluetooth technology because it can transmits the information from one device to another.

Electromagnetic induction

Electromagnetic induction (also called as just induction) is basically a process where the conductor is placed in the magnetic field which is changing, that causes production of the voltage across conductor. The Electromagnetic induction, in return, produces an electrical current which is called as induce current.

The electromagnetic induction, also states that magnetic field that is time-dependent produces electric field which is circulating. Magnetic field that is time dependent is produced either by the movement of magnet analogous to the circuit, through the motion of one circuit with respect to another circuit (one of these or both must carry current), or by keep on changing current in circuit that is fixed. By changing the current, if the effect is on circuit itself, is called as self-induction; whereas the effect on other circuit is called as mutual induction.

This law also describes the working principle of generators, electrical motors, inductors and electrical transformers. This shows the link between magnetic field and electric circuit is. Faraday executes the experiment with a coil and a magnet. For a circuit, the EMF that is induced electromagnetically is decided by the rate of the magnetic flux changed by the circuit as per the induction law of Faraday.

The first factor of Faraday's law of electromagnetic induction was number of wire turns in the coil, because of this the amount of the wire exposed to magnetic field increased. The Faraday's experiments results showed that the induced voltage is directly proportional to the number of turns in the coil.

The second factor of Faraday's law of electromagnetic induction was how rapidly the magnetic field was changing. There are different ways through which we can make change the magnetic field. One of the ways is to vary the strength of magnetic field produced by magnet. By doing change in the current so that there is a change in the field or on/off of the magnet. The other way is to move the magnetic field relative to a conductor.

Faraday's Law results in: It states that magnitude of the voltage that is induced is directly proportional to both the rate at which field changes and to the number of wire turns.

Whenever there is some change in a flux linkage, an EMF is induced in the conductor or the coil. Depending up on the way, the changes were brought, there are two types that are when there is a stationary/fixed magnetic field and the conductor is moving in it to solicit change in

flux linkage, the EMF is induced statically. Motional EMF is the electromotive force which is generated by motion. The EMF is induced dynamically, when there is change in the flux linkage, because of change in magnetic field around stationary conductor. Transformer EMF is the electromotive force that is generated by a transformer EMF magnetic field which is varying with time.

1.5 Organization

The major role is played by the security now a day's. This project has a study about that as created a safe access for the door that needs a password to open the lock of door. Using mobile keypad user can enter a password and if it is correctly entered door will open by motor (servo) which can be used to rotate handle of lock. This will give a certain number of attempts (three in this case) to enter the password, if it incorrect password is entered at the first time. Features such as adding a new user or change of old password are being configured.

In today's world, most of the systems are being automated in order to achieve good results and to face new challenges. As automated system has less manual operations, so that the reliabilities, flexibilities are accurate and high. That is why; every field adopts control system that is automated, exclusively in the electronics field. The main goal of this project is to build a high security for offices, houses etc.

This project also has a low cost for the security systems which are widely used in the daily life. The system under this project is basically designed to prevent houses or offices locks from opening by unauthorized persons. The application is used to the control the password entry system for opening/closing the doors. The correct password enters by the user, results in the opening of the door locks. If incorrect password is entered, the system allows the user to enter password for two more time before being disabled temporarily.

EMF is used to send the password from one coil to another, which was entered by the user with the help of mobile application. The password which was sent is encrypted then decrypted and then matched at server side if correct, results in opening/closing of the door as chosen by the user in the mobile application.

Chapter 2

LITERATURE SURVEY

Today with the advancement in technology, Objects of everyday use are being getting digitalized and connected to internet for better experience of the user. Smart-Phones, smart bands, LiFi, WiFi, Bluetooth etc type of gadgets/new technologies making this possible as well as more adaptable then it was before. Related to this, Smart Locks are also gaining momentum all over the world with many companies or start-ups as now they are working in this area.

Physical Door Locks Evolution

Fig 2.1 Door lock Evolution

There are various devices that are largely used for security purpose. Some of the security devices that are used are bluetooth locking system, smart card, pass code.

2.1 Bluetooth locking system: Smart homes for a better living using Bluetooth communication based on atmega microcontroller, Monika Rana1, Ramandeep Singh[2]. Bluetooth is easy to access as it can open the door without entering the password if it gets paired. Most of the times one has to carry devices for unlocking the door but limitation is that lack of security as easily connection can be done.

Fig 2.2 Bluetooth locking system

Smart card: Design analysis of a security lock system using pass-code and smartcard, Omijeh Boand, G.O. Ajabuego[3]. This smart-card locking system now a day's used in many hotels which works by scanning and then unlocking the door It is also easy to use But the limitation is that loss of this card leads to difficult situations.

Fig 2.3 Smart card locking system

Pass code: Design and Implementation of a Digital Code Lock, Annie P. Oommen, Rahul A P, Pranav V, Ponni S, Renjith Nadeshan[1]. The Pass code door locking system (shown in the figure) has a keypad on the lock. It is also easy to use, there is a need to enter the correct password and it opens the door. But the limitation is that cracking the password through multiple combinations is not so hard.

Fig 2.4 Pass code locking system

The drawbacks that were discussed above implies that there is need of more secure locking system and advanced latest technology one of that can be based on IoT, so known as "IOT based EMF data transfer for Electronic Locking System" that is the proposed system. It is more secure, advanced, and also user friendly than the technologies discussed above.

2.2 For Disabled People : N.H. Ismail, Zarina Tukiran, N.N. Shamsuddin [11]Android-based Home Door Locks Application via Bluetooth for Disabled People (2014). This paper had discussed about the project that has served the needs of the people who are physically disabled at home. In this paper the Bluetooth technology is being used for communication establishment between controller board and the user's Android Smartphone. The prototype supports microcontroller controlling as well as manual controlling for locking and unlocking the door locks at home. Here a relay board is connected with the circuit and then connected to the Arduino controller board which is controlled by a Bluetooth in order to provide remote

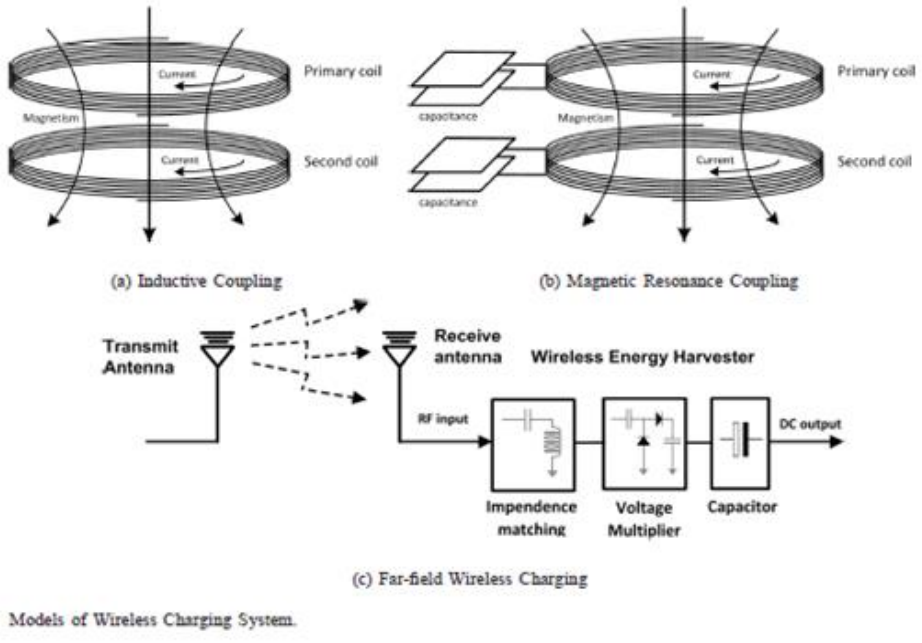
access from smart phone or tablet. This paper addresses the functionality and the development of the Android app (i.e. Android-based application) to help disabled person to gain control of the living area, rooms etc.

The disabled person can use the GUI (Graphic User Interface) application very easily that had been created for locking or unlocking the door lock with the help of Bluetooth Protocol in the Android Smartphone using android programming. And also created an mobile application for using Bluetooth pairing.

2.3 Wireless Charger Networking for Mobile Devices:

Fundamentals, Standards, and Applications: Xiao Lu, Ping Wang, Dusit Niyato, Dong In Kim, and Zhu Han [10] .Wireless charging technology is able to transfer power wirelessly from one power source to a load for example from a charger to a mobile device across an air gap. This technology also provides better user experience and convenience. In recent time, charging wirelessly has rapidly been evolved from the theories towards the standards, and adoption in the commercial products, especially portable devices and mobile phones.

Wireless Charging Techniques



Models of Wireless Charging System.

Fig 2.5 Types of wireless charging

There are three major techniques for charging wirelessly that is magnetic resonance coupling, magnetic inductive coupling, and the microwave radiation. The magnetic resonance coupling and magnetic inductive coupling work on the field, where the region close to the transmitter or scattering object is being dominated by the generated electromagnetic field.

COMPARISON OF DIFFERENT WIRELESS CHARGING TECHNIQUES.

Wireless charging technique	Advantage	Disadvantage	Effective charging distance	Applications
Inductive coupling	Safe for human, simple implementation	Short charging distance, heating effect, Not suitable for mobile applications, needs tight alignment between chargers and charging devices	From a few millimeters to a few centimeters	Mobile electronics (e.g, smart phones and tablets), toothbrush, RFID tags, contactless smart cards
Magnetic resonance coupling	Loose alignment between chargers and charging devices, charging multiple devices simultaneously on different power, High charging efficiency, Non-line-of-sight charging	Not suitable for mobile applications, Limited charging distance, Complex implementation	From a few centimeters to a few meters	Mobile electronics, home appliances (e.g., TV and desktop), electric vehicle charging
Microwave radiation	Long effective charging distance, Suitable for mobile applications	Not safe when the RF density exposure is high, Low charging efficiency, Line-of-sight charging	Typically within several tens of meters, up to several kilometers	RFID cards, wireless sensors, implanted body devices, LEDs

Table 2.1 Different Wireless Charging Techniques

CHAPTER 3

SYSTEM DEVELOPMENT

3.1 SOFTWARE REQUIREMENTS:

- Android Studio
- Arduino IDE
- JDK (Java Development Kit)

3.2 HARDWARE REQUIREMENTS:

- **For making setup:**
  - ✓ Coil with 30 loops
  - ✓ Hardware-based electro-mechanical lock
  - ✓ Bluetooth module
  - ✓ Arduino Galileo
  - ✓ Android Mobile

- **System Requirements:**
  - ✓ RAM: 1GB or above
  - ✓ CPU: 2GHz Processor and above
  - ✓ OS: Windows 7 and above

3.3 MODEL DEVELOPMENT:

Block Diagram:

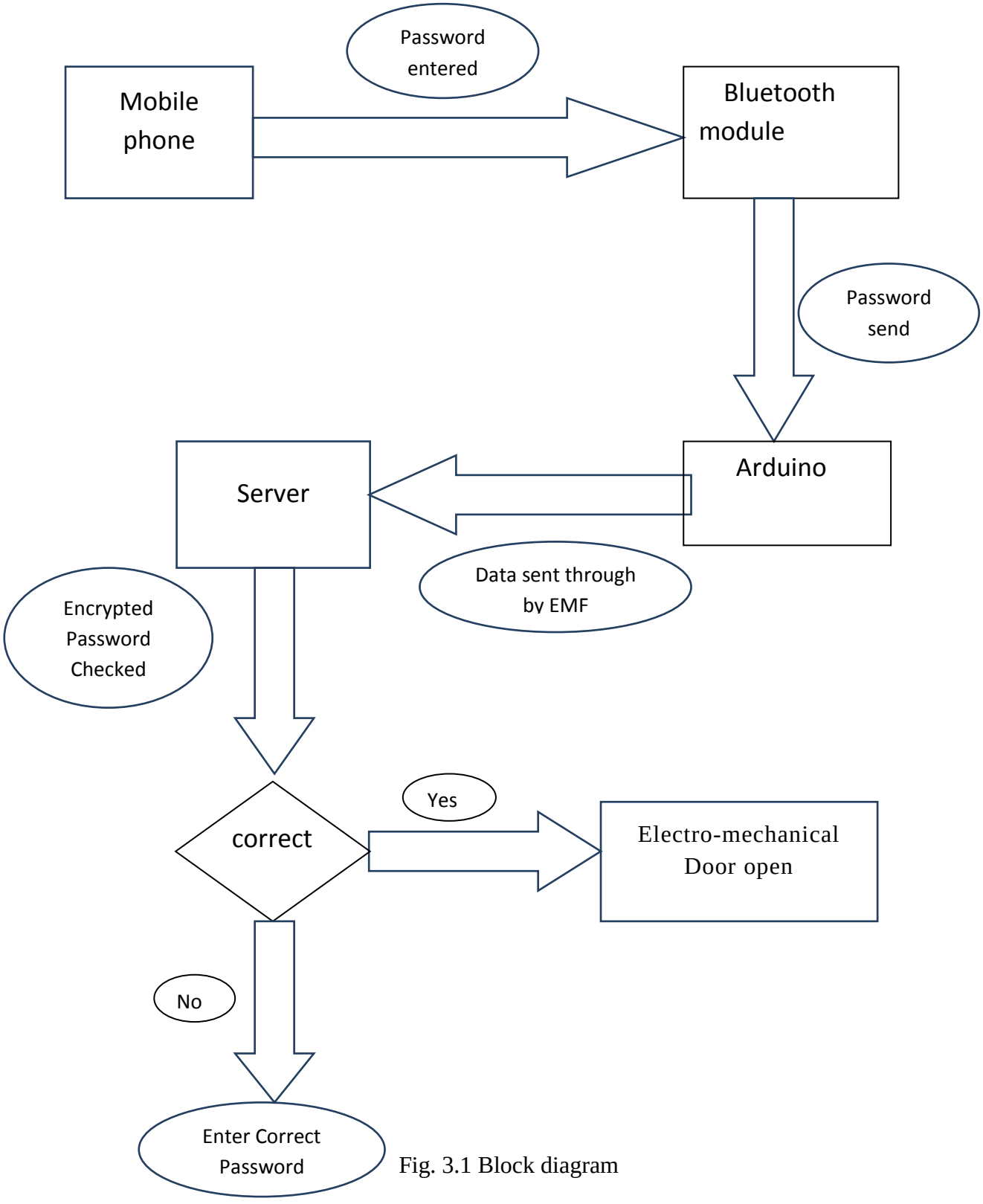


Fig. 3.1 Block diagram

Use Case DIAGRAM

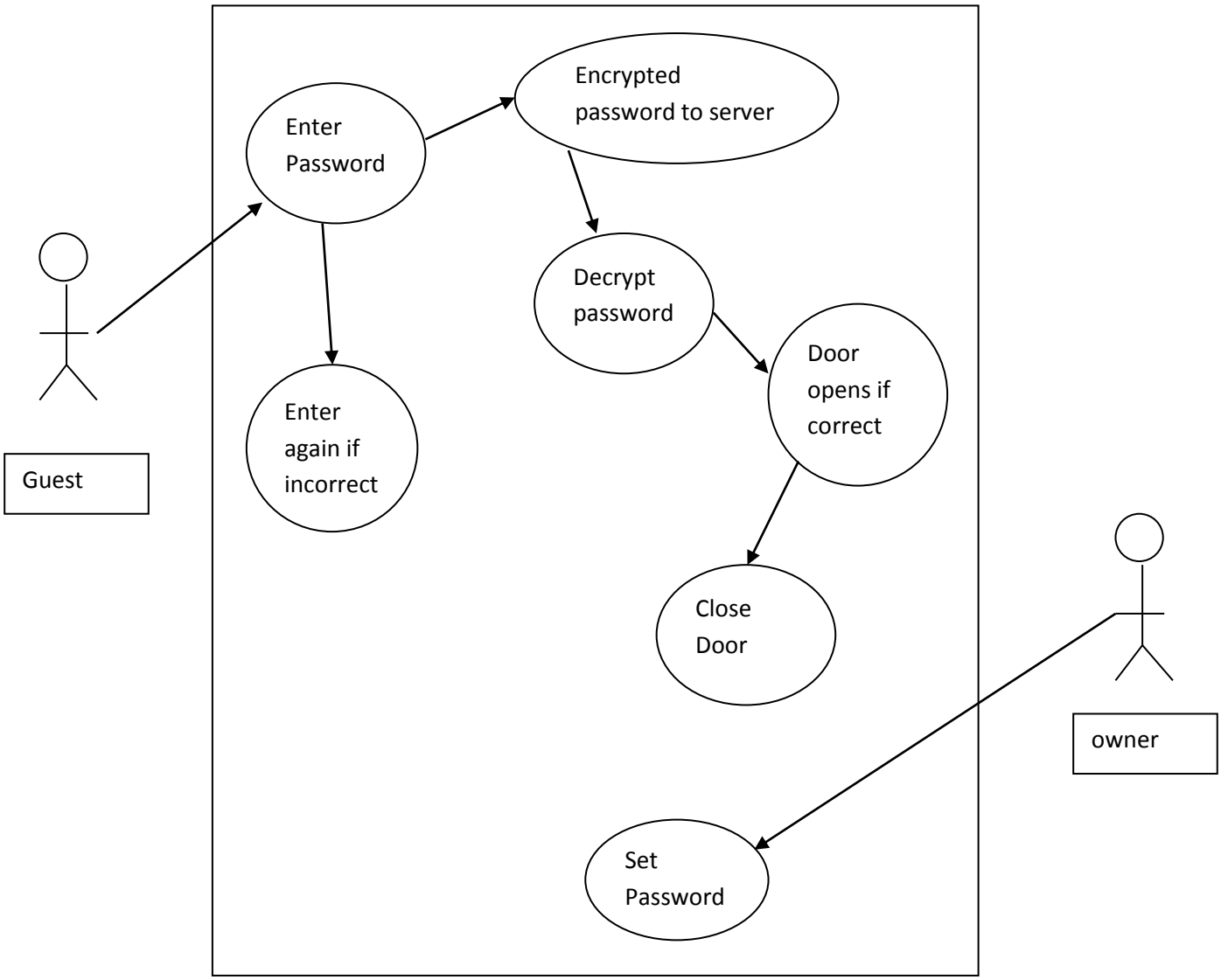
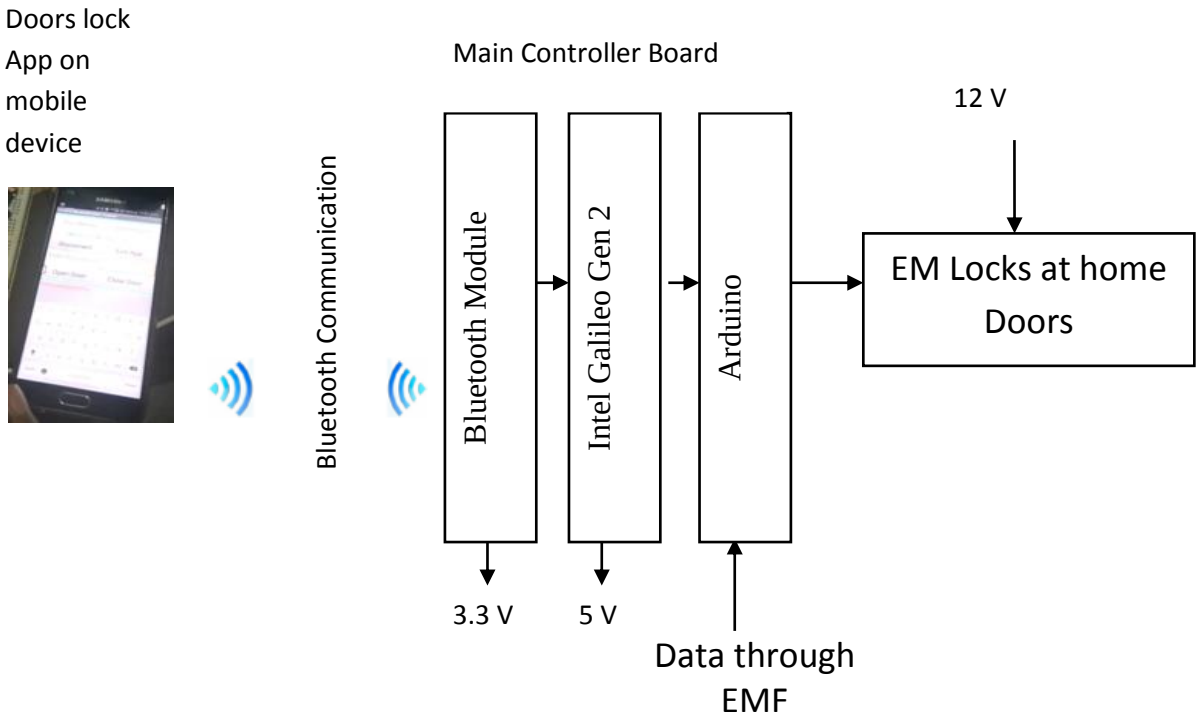


Fig 3.2 Use Case diagram of the door locking System

3.4 Experimental Implementation

The Block diagram depicts the architecture of proposed locking system using Bluetooth technology



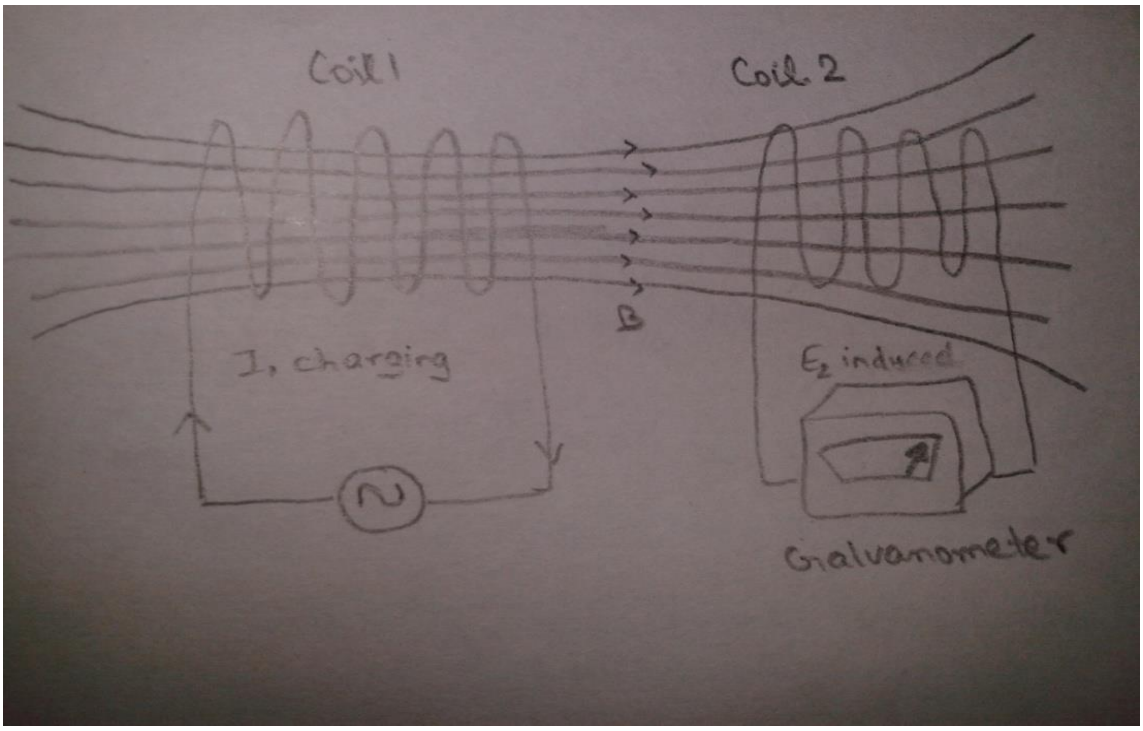


Fig 3.3 System architecture

An Android App has been designed to let the user choose their selection either lock or unlock the door lock. The App was designed using Android studio software and programmed with the help of Java programming language.

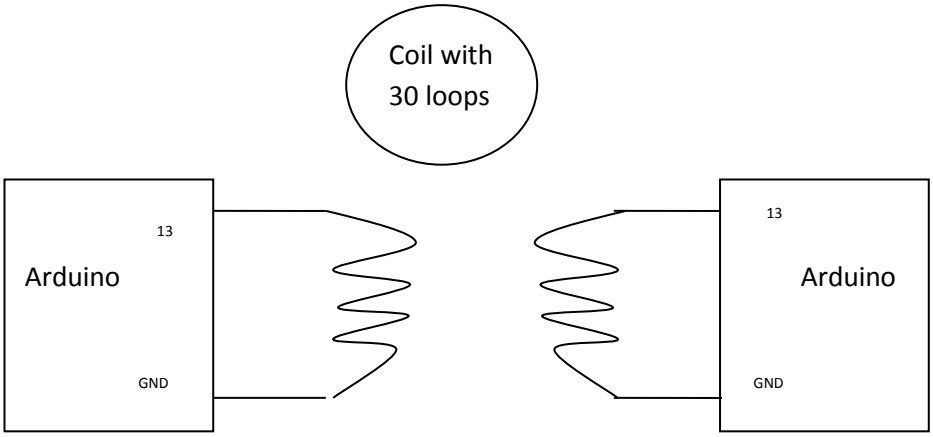


Fig 3.4 Data sending through EMF

Data/Password sent through EMF using Arduino

Android phone Bluetooth app and Bluetooth hardware module connects through wireless communication which is termed as pairing.

Then user enters the password in the locking app. Through Bluetooth, it reaches to Arduino Galileo controller. The password is send from one copper winding to the another copper winding Arduino Galileo controller send encrypted key to the server where the decryption of that key takes place. If the password is correct then the door lock open else if the password is not correct then two more times user can enter the password if all the times password entered is not correct the system temporarily disabled.

The Arduino is programmed using C language. It can sense the Radio Frequency signals at the controller's input port. The relay circuit that is inside the Arduino released the Electromechanical lock to open the door if the relay circuit is triggered at 12V. For Arduino the voltage should be up to 5 V otherwise more than that it will not be tolerated by Arduino.

PSEUDO CODE for overall system

1. **foreach** *user*

2. **input** *action*

3. **if** *password is correct* **then** *open the door lock*

4. **else if** *number of mismatch >=3* **then** *delay(200)*

5. **else** *go to step 2*

6. **End**

Bluetooth

By adding a module of Bluetooth to this project makes the work easy. Just connect RX (i.e. Receiver) of the Bluetooth module to TX (i.e. Transmitter) of the Intel Galileo board, and TX fn the Bluetooth module is connected to RX of the Arduino, respectively. GND (i.e. Ground) is connected to ground, and lastly VCC is connected to 3.3 volts or 5 volts depending on your Bluetooth module.

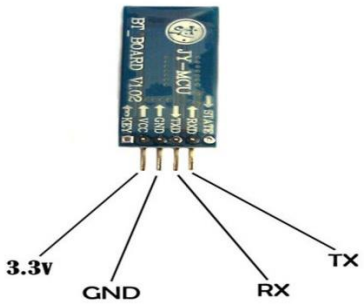


Fig 3.5 Bluetooth

Pseudocode with Bluetoth Module

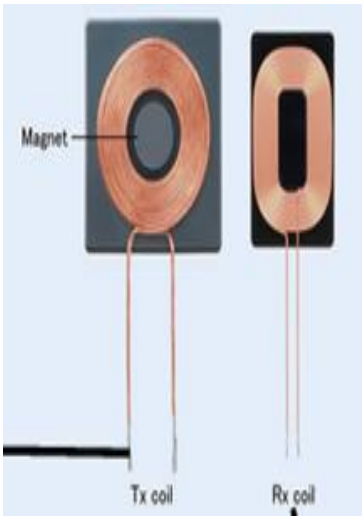
Start

1. Scan the Bluetooth module
2. Create link between Bluetooth devices i.e Bluetooth module aand mobile phone
3. Password is sent to arduino
4. By EMF, it reaches to second coil and then arduino
5. Encrypted password is sent to the server
6. Decryption takes place
7. If password matches on the server then
    a. it will return ‘1’ and lock open
    b. it will return ‘0’ and lock remain close

End

Parts Needed

Component	**Function**	**Specification**
Microcontroller	Controller	Arduino Galileo(Gen 2)
Bread Board	Circuit runs	Mini Bread Board
Web Server	Mobile App. Service	Android Studio
Connecting Wire		5-15
Language	Mobile Application	C
EMF Coil		30 loops
Bluetooth	Communication Controller & Mobile Device	Wireless Pin Bluetooth
An Android phone	send serial data to the bluetooth modem	Iphones, computers, Samsung
Hardware-based electro-mechanical lock		



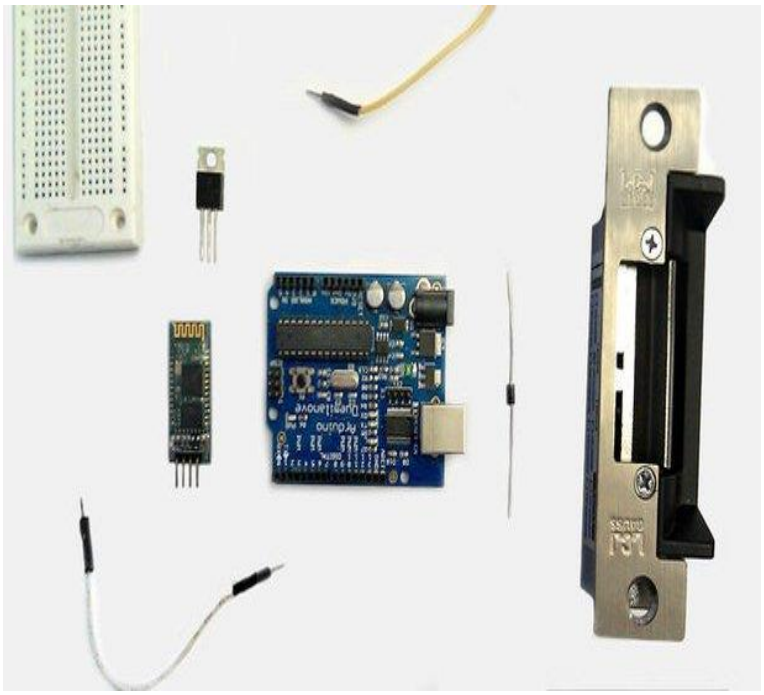


Fig 3.6 Requirements

Data Transfer through coil by EMF

Data has been transmitted to the copper winding through the Intel Galileo before passing to the coil digital data is converted to analog data and 3.3 Volt to 12 Volt using relay and then passed to second copper winding though magnetic induction in the coil. Then, AC (Alternating Current) is generated as shown in following figure . After converting from AC to DC (Direct Current), the analog data is converted to digital data again.

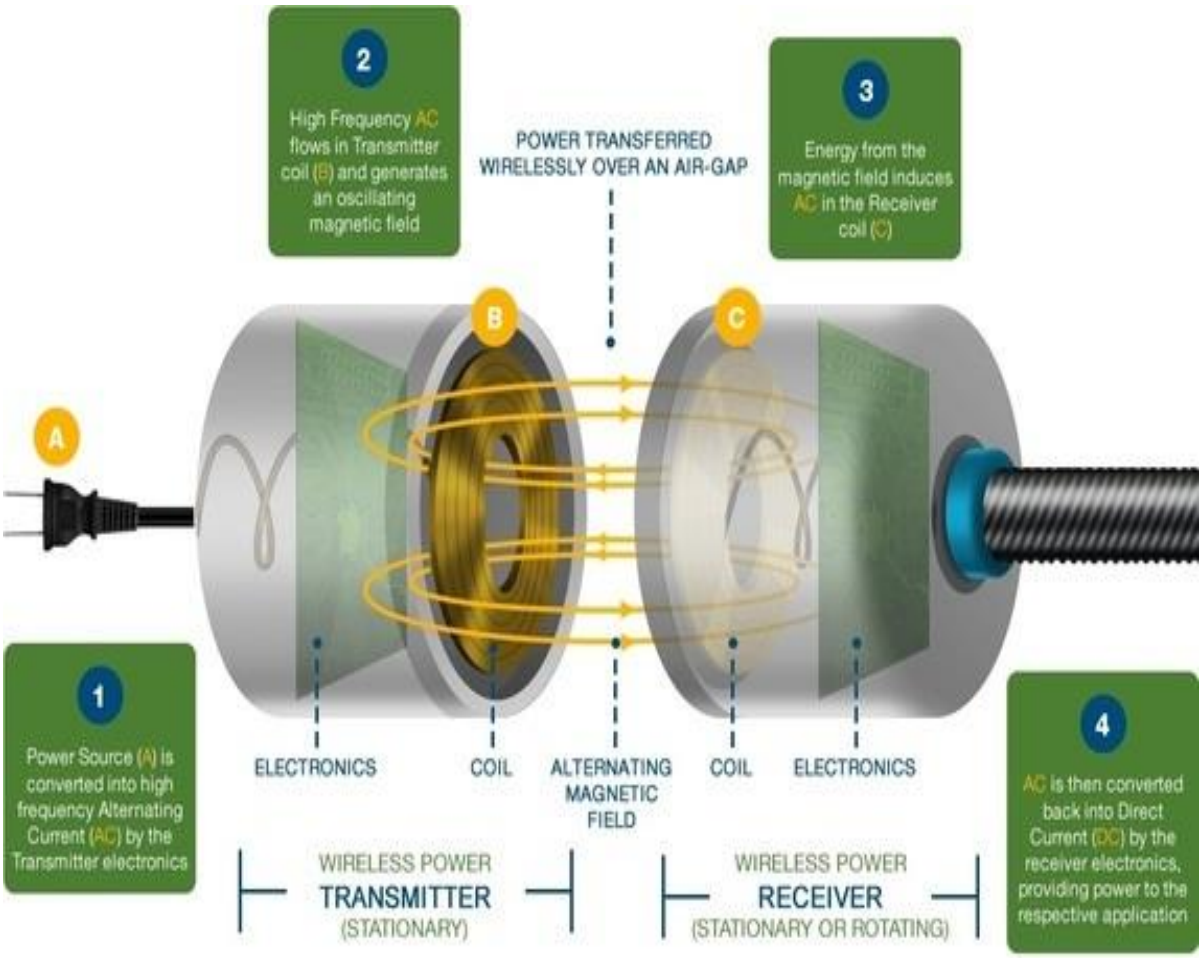


Fig 3.7 Transfer of Data

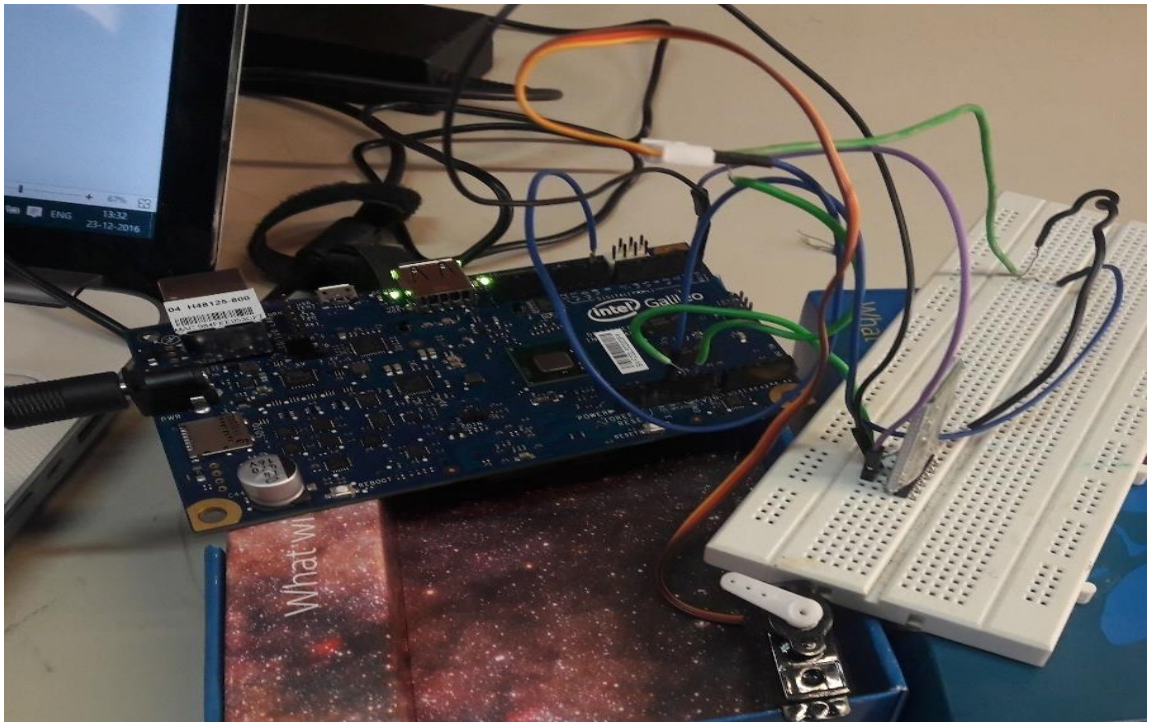


Fig 3.8 Final Look with Bluetooth and servo

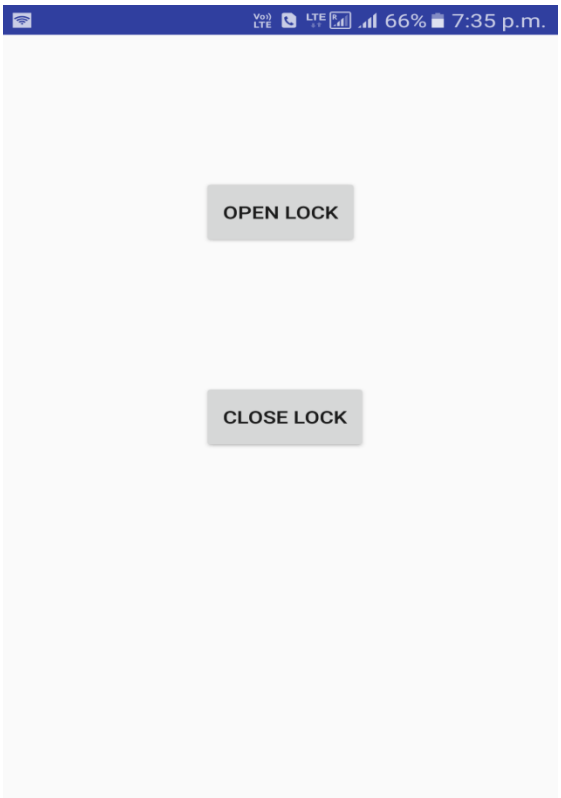
On the Arduino, it will check if anything is being received through serial. If it is being received, then it will read those chars into an array and from that point verify that what was received either it matches with the password that is defined by the user. In our example assume that the password defined is ABCD.

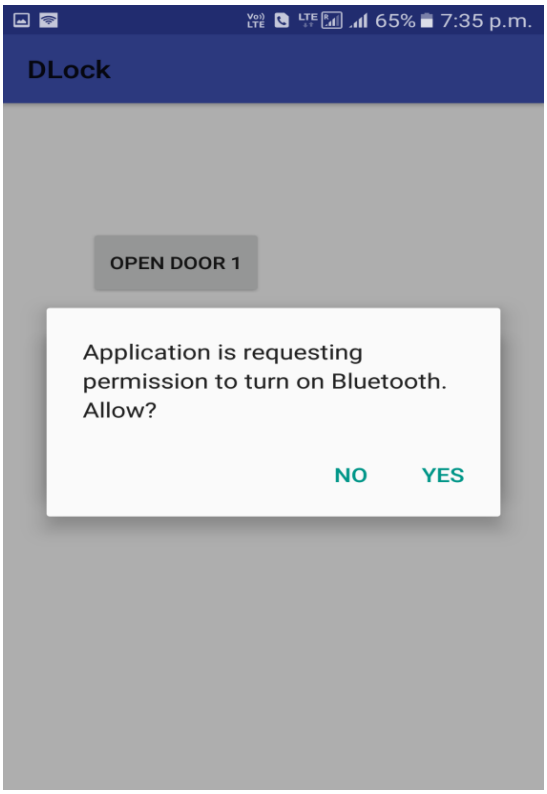
CHAPTER 4

PERFORMANCE ANALYSIS

4.1 Output at various stages

When the app will run, it will check either the Bluetooth radio is enabled or not, if not so a Bluetooth enabling dialog will appear. To turn on the Bluetooth radio, click yes. Using pair device button, pair the devices. Then click on connect button, if it is connected successfully to any device the application shows the MAC address and name of the connected device. Enter password to the text box then click on the open lock button, if the password entered is correct door lock will open and a message that your door is now open will be shown at the display of the application. But if password entered is incorrect app will show incorrect password message. If want to close the door then enter the password again.





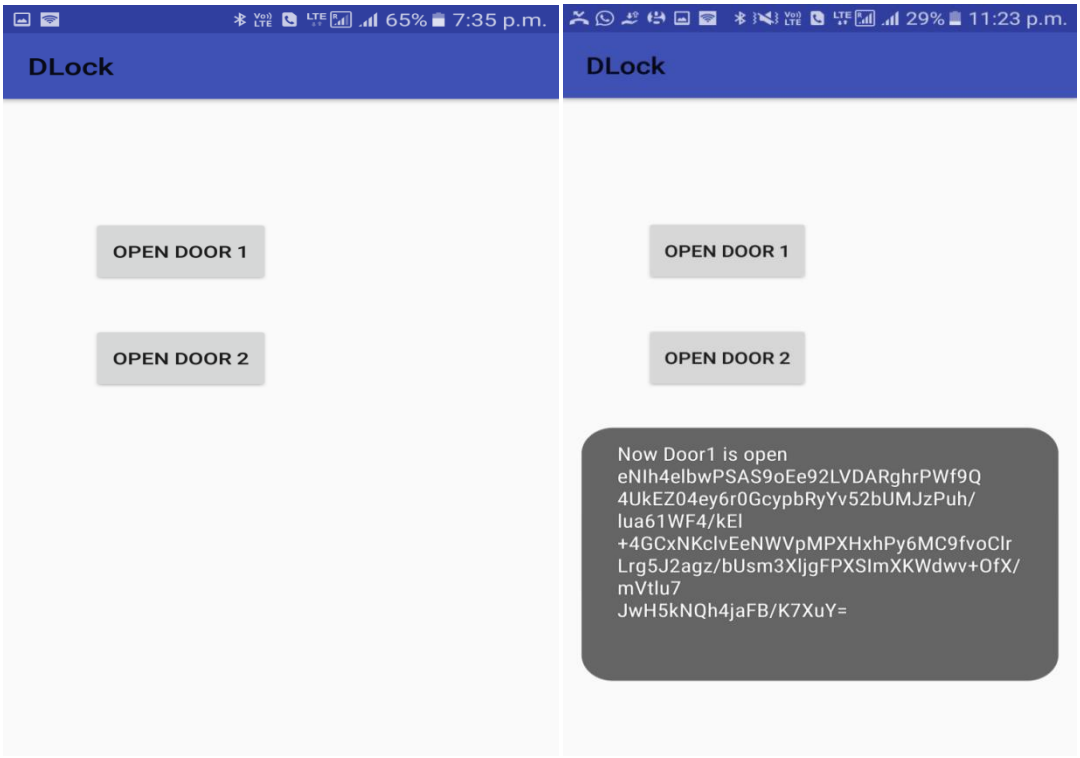


Fig 4.1 Arduino Bluetooth Door Control

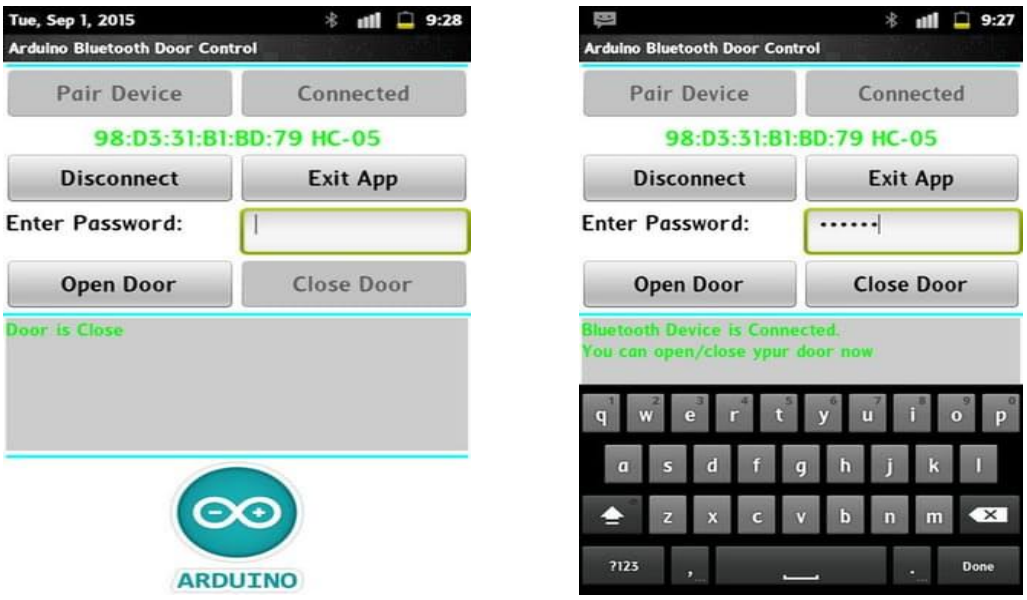
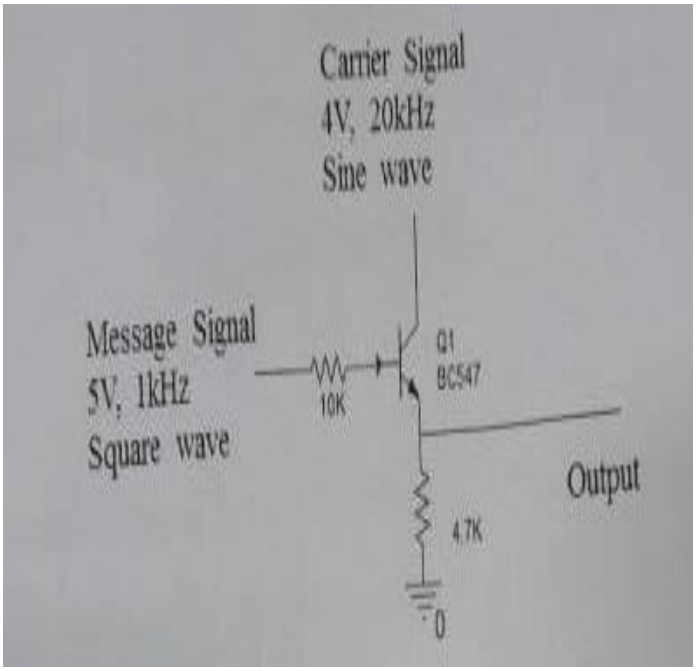


Fig 4.2 Screenshots of previous mobile application (downloaded)



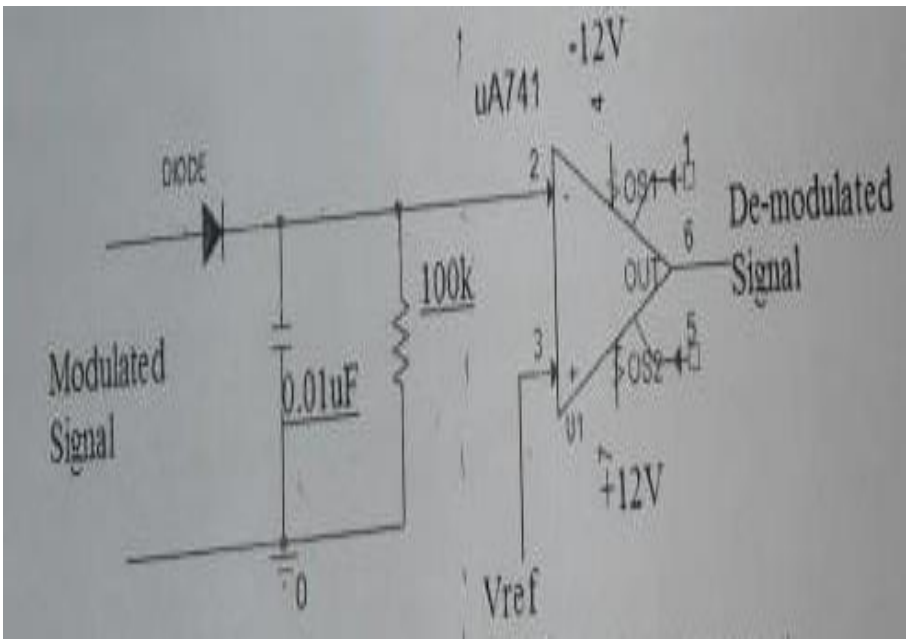


Fig 4.3 Circuit for EMF Data transfer

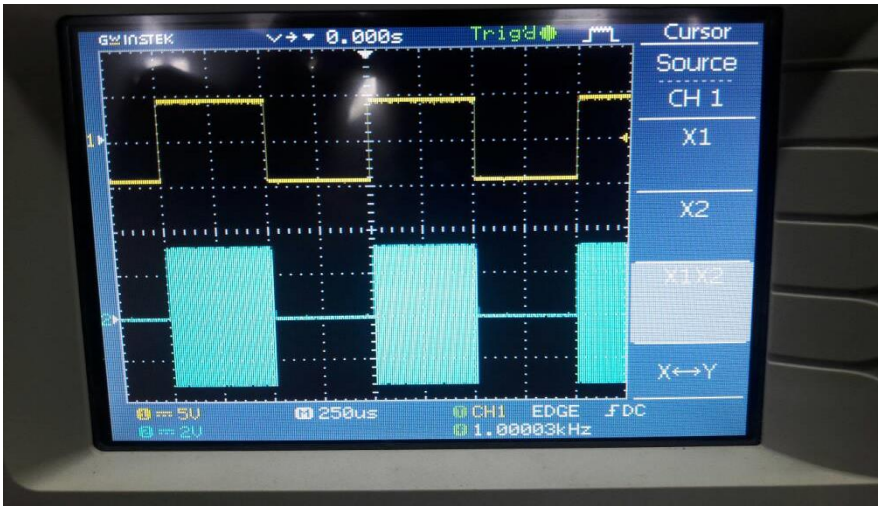


Fig 4.4 message signal and signal at primary coil while EMF data transfer

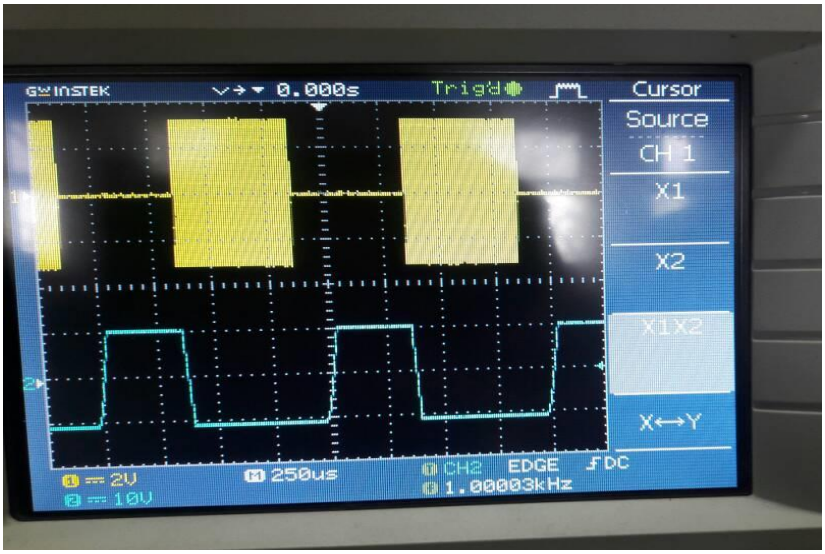


Fig 4.5 signal at primary coil and at secondary coil while EMF data transfer

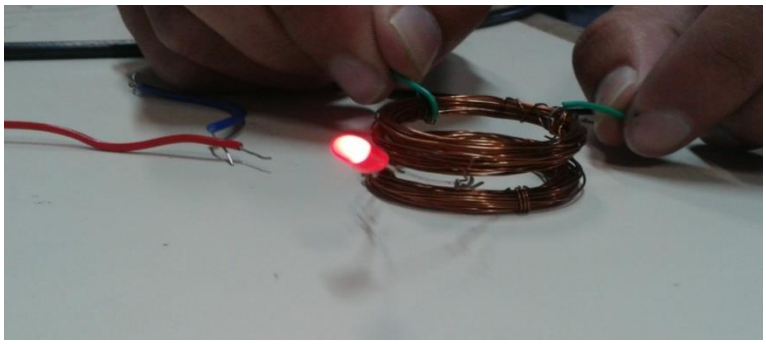


Fig 4.6 LED glows when EMF induced in secondary coil due to primary coil

Global Web portal

With the help of web portal user can access the server and database from any remote location in the world. User can change the password of a particular door lock and can even see the status of all door locks either close or open or if any invalid visitor tries to open the door lock.

```
# Mutex default:logs

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 192.168.43.151:80
Listen 80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding `LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by `httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
#
LoadModule access_compat_module modules/mod_access_compat.so
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule allowmethods_module modules/mod_allowmethods.so
LoadModule asis_module modules/mod_asis.so
LoadModule auth_basic_module modules/mod_auth_basic.so
#LoadModule auth_digest_module modules/mod_auth_digest.so
#LoadModule auth_form_module modules/mod_auth_form.so
#LoadModule authn_anon_module modules/mod_authn_anon.so
LoadModule authn_core_module modules/mod_authn_core.so
#LoadModule authn_dbd_module modules/mod_authn_dbd.so
#LoadModule authn_dbm_module modules/mod_authn_dbm.so
```


Fig 4.7 Screenshot of global web portal

All user have to write the server computer's IP address in httpd.conf file in Xampp folder. So that xampp server can be accessed from other computer after writing server computer's IP address on browser as show below.

Fig 4.8 Screenshot of Xampp server (after opening xampp)

The IP address of the client machine can be known from cmd type ipconfig there and it will give the configuration of the computer including the IP address which is useful.

After opening the wamp server, the user have to enter the username and password on the login page as different users have different passwords and might be for different door locks.

After both the fields filled, then click on log-in button if correct password then Connected successfully message will display otherwise login unsuccessful message will be there on the screen.

Fig 4.9 Screenshot of login page

After the connection is made that is with the connected sucessfully message there will be a lock table which describes the status, password and id of different locks as shown in fig 4.10.

Also there will a option of change password to protect from others (or if any invaliduser now knows the password) by clicking on that button password canbe changed after filling the fieldslike old password, new password, for which door (door1 or door2) etc as shown in fig 4.11.

Fig 4.10 Screenshot of status of door locks

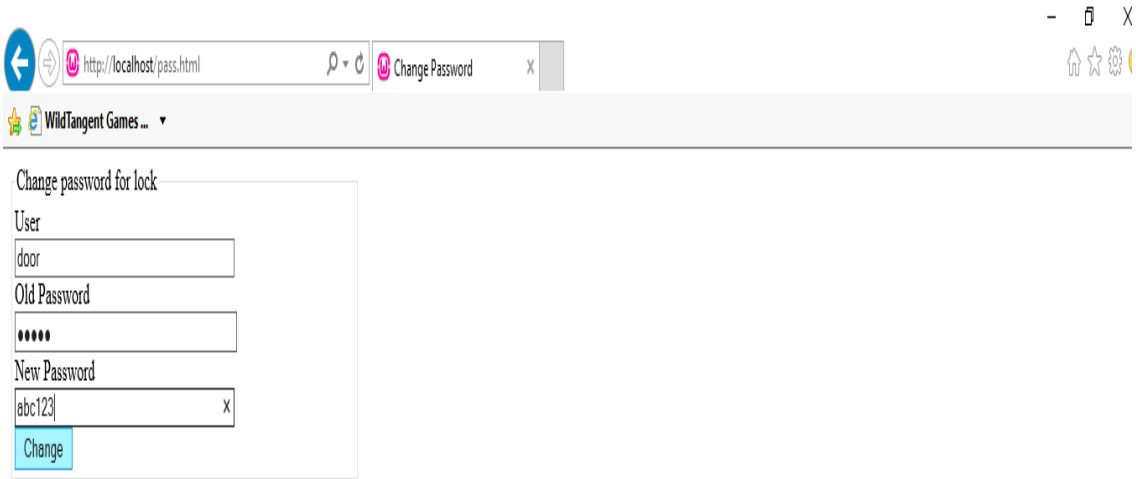


Fig 4.11 Screenshot of display for changing the password

After changing password, the lock table which contains the id, password and status of door lock had the updated password in the updated table is shown in fig 4.11 .

Fig 4.12 Screenshot of updated status of door locks

4.2 Analysis

1. Measurement set-up for different location

Three different types of measurements that are being used in this project:

(i) indoor
(ii) outdoor with non-obstacle area
(iii) indoor with obstacle area

As shown in Table 4.1, it has been found that, in case of indoor (in both obstacle and non-obstacle area), Radio Frequency signal from Smartphone that can be detected by the receiver is the maximum distance of around 15 meters in the house while in case of outdoor area, around 20 meters is the maximum distance .

Reading	**Area**	**Distance(m)**	**Conected/ Intermittent/ Disconnected**
First	Indoor(non-obstacle)	5	Connected
		10	Connected
		15	Intermitted
		20	Disconnected
		25	Disconnected
		30	Disconnected
Second	Outdoor(non-obstacle)	5	Connected
		10	Connected
		15	Connected
		20	Intermitted
		25	Intermitted
		30	Disconnected
Third	Indoor(obstacle)	5	Connected
		10	Connected
		15	Intermitted
		20	Intermitted
		25	Disconnected
		30	Disconnected

Table 4.1 Set up for different locations

2. Power strength measurement of Bluetooth

The measurement of power strength of Bluetooth had been done in UTHM, EMC (i.e. Electromagnetic Compatibility Canter). Depending up on the data, 3 distinct kinds of analysis can be considered in terms of range of frequency, FHSS and strength of power for any two particular distances.

i) Frequency range: Basically on theoretical biases, Bluetooth is a used for short distance and is for exchanging data through wireless technology standard from fixed or mobile (portable) devices, and building PANs (i.e. personal area networks). It uses UHF radio waves that are short-wavelength in the ISM band ranges from 2.4 to 2.485 Giga Hertz. Thus, it has been proved that the frequency range is still in the range of Bluetooth frequencies even at different distances and conditions.

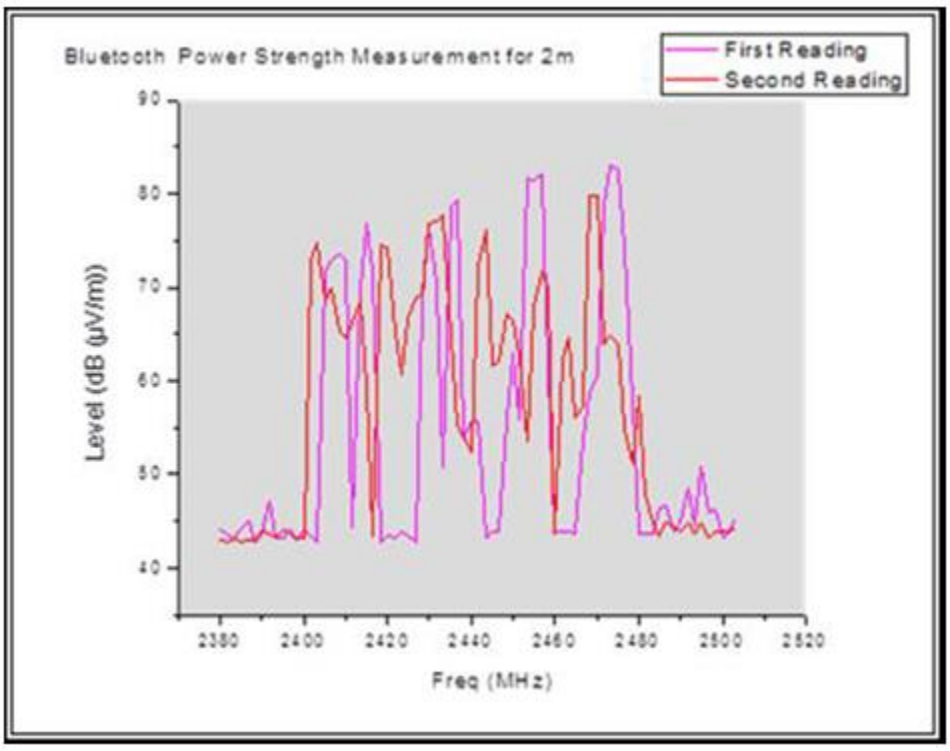


Fig. 4.13 Bluetooth power strength for 2m

ii) Frequency Hoping Spread Spectrum: It is modulation technique which is the most secure technique that is available. Its prime responsibility is to receive and modulate the data signal input that are to be transmitted with a carrier signal so that at the different time slots the signal that are modulated hops from one frequency to other frequency and is spread over a large band of frequencies. A signal's power spreads by Spread spectrums over a large band of frequencies, for instance: in order to gain SNR (signal-to-noise) performance there is a trade-off of band width.

All these theories conclude that why the graph at fig. 4.9 had too many peaks from 2.4GHz to 2.48 GHz range, from the point when the Bluetooth begins to communicate/exchange information between the Android Smartphone and Bluetooth module.

Electromechanical door locks consists of a steel plate, various mounting accessories and a bar magnet. Until the current is cut off, they are bonded together very strongly from When current starts flowing.

The relationship between the magnetic field and source current element is known as the Biot-Savart law which is written below in Equation 1.

$$dB = \frac{\mu I}{4\pi} \frac{dl \times r}{r^3} \qquad (1)$$

where:

dB is perpendicular both to the direction of the current (which is ds) and to the unit vector that is r which is directed from the element to a point A

μ is magnetic constant in free space,

dl is a length vector whose magnitude is equal to the length of the wire's differential element

I is the steady current

r is the distance from the point A to the element

Due to the positively and negatively charge atoms, a weak magnetic field has been generated, when the electrical current starts flowing through the conductor. The direction of contribution of magnetic field follows right-hand rule for a wire which should be straight-line.

When the signal of Unlocking the door lock transmitted from the Android Smartphone, it had triggered the relay and relay was in a simply open condition, so the Door Lock will release so that no more current flow.

B. power measurement of EMF

It has been found that when there was large distance between the coils, and the data transfer was not happening. As increasing distance between the coils, also more chance of error. But in a specific distance range, without any problem through the coils, data was transferring.

CHAPTER 5

CONCLUSION

5.1 Conclusions

In today's hacking world, security emphasising is a crucial part, up gradations are being done for door locking devices. By making use of advanced and recent technologies gives a new dimension to stated purposes. Apart from those ones always being used, Smartphone technology i.e. the most trending technology has been brought in the use for one more day to day purpose. Besides information and entertainment utilities Smartphone devices aspect can also serve the purpose of the door unlocking.

EMF and IoT technology, added an additional quality to the project's proposed module. The continuous drop in the prices of chipsets makes it an economical/cost effective option which is also included in other devices. The Connection to the wireless Communication device can be done with Computer systems and various other devices which includes PDAs and smart phone. What makes it more reliable is having more superior level of attribute that are safe and least limitations. Overall satisfaction to the user is provided by this.

In this project, a door lock with security functions that are enhanced was designed to do the work with the IoT (Internet of Things).

The designed door locking system detects if invalid visitor uses this system. As if an incorrect password is repeated more than a certain number of times (3 in this case), then it will display a message of incorrect password entered.

It is expected that the proposed system can be used commercially as a useful product, like a security system with enhanced security and convenience, especially when compared to existing digital door lock systems.

The main aim of the task undertaken in this project was to check the correctness of a password/secret code using the Arduino (Intel Galileo) technology. When the correct password is entered through Mobile application, a small solenoid is powered, and will strongly attract the metal slug in its center, pulling it into place, when the power is removed,

it is free to move. Then the password that is decrypted at server side now checked with the pre-defined password if matched the door lock opens and if not so message of incorrect password will appear.

5.2 Future Scope

First, it can have alarm functions and impact detection. This means to detect an invalid visitor/intruder who is trying to invade by breaking or applying force to the lock.
Second, it can have a function that is an image transfer. An attacker, to whom password is not known, might make various numbers of attempts to enter. Therefore, the system takes the image of the intruder, if an attacker types the incorrect password more than certain number of times, and then transfers the image to the mobile of the owner.
Third, the records of passwords entered and all closing and opening records can be stored in the database which can be later viewed by the user.
Fourth, the system is able to recognise visitor's image in real-time and then can open the door lock. In case if a visitor don't remember the password, he/she can click forget button in the application, then the door locking system send his/her image to the owner's mobile device. After viewing his/her image, the owner can access the door lock while sitting in a remote location.

Fifth, the controller can close or open the door lock at remote location, after detecting a valid visitor who is approaching the door lock only if he/she has the mobile phone.

The physical impacts that are applied by any visitor can be detected by the controller, and discloses the mobile phone of the user. There is a camera that is used to capture the images of the visitor, when the password error is there more than a specified number of times and this can be detected by the controller also. Then the image is transferred to the user's mobile phone. The user is able to view all the records of accessing the lock later from its database where the records were being stored, using the mobile phone.
By pressing a particular key the image of visitor can be captured and sent to the user mobile phone in case if his key has lost, the user then is able to control the locking of door remotely when it is verified that the visitor is valid.

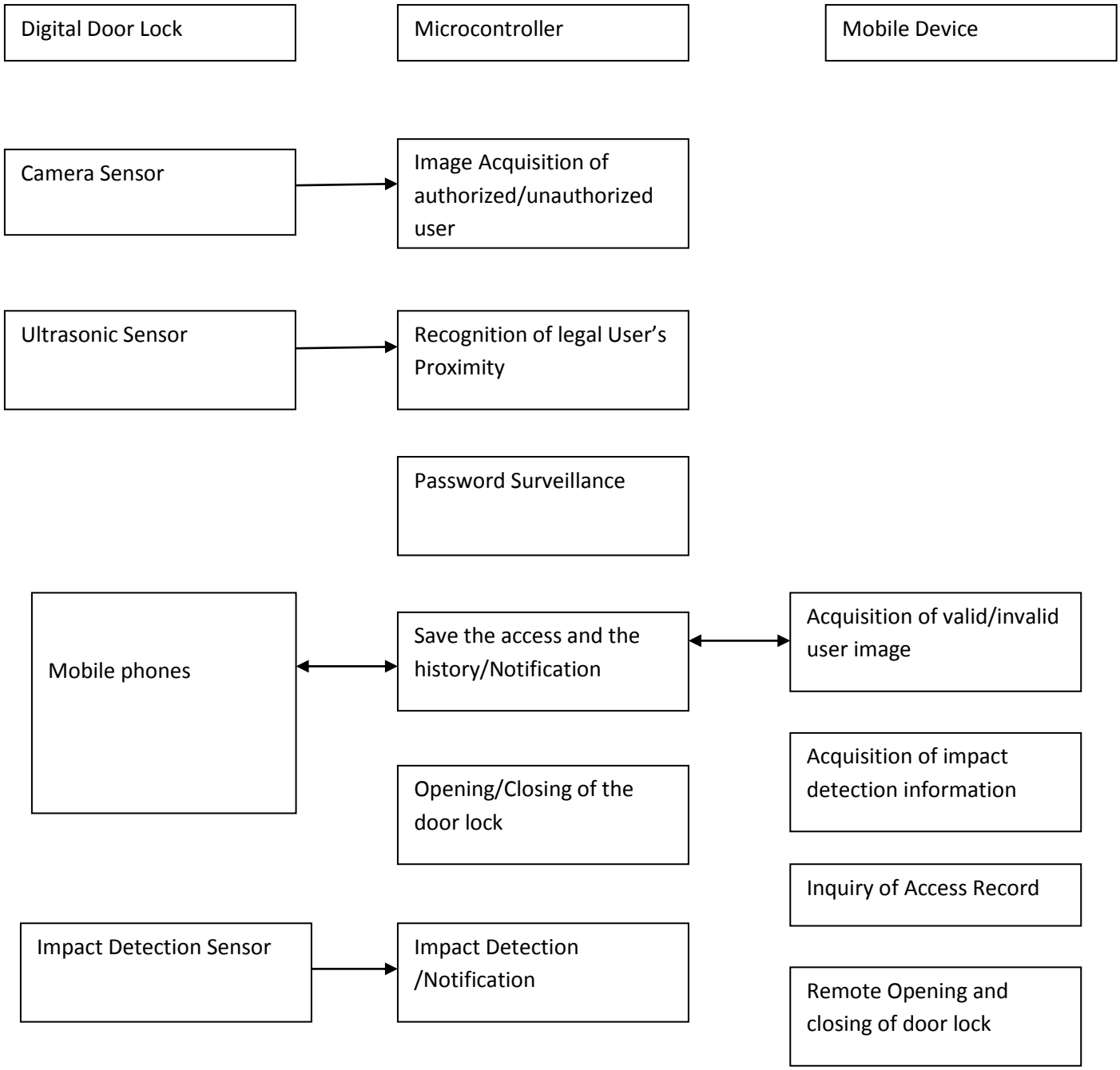


Fig. 5.1 Structure of the described door locking system

There can be automatically opening or closing of the door, only when an authorized user comes near the door lock. When for an authorized user it is difficult to operate the door lock, the controller's another important function is to communicate with the owner's mobile phone via Bluetooth and automatically opens the lock of the door.

The user can take useful actions when mobile phone detects harmful physical impact on lock or when controller sends the image of the unauthorized visitor. Further, it is also possible to open or close the door from any location, if the user reviewed the image of a valid visitor.

In case if someone tried to hack the lock‘s secret code/ provide any physical harm then there can be use of GSM and GPS system to track. These systems are able to track the unauthorized user's location & also owner’s location, so by sending a message to alert the owner that there is an attack which is going on the smart-lock. Implementation through cloud computing can be used so that the user is able to control the door lock from any location. For surveillance there can be use of cameras, for more security than this following can be used finger scanner (biometric locks), face recognisor etc. With the person on the next side of the door, voice conversation may also used, to avoid closing or opening of the door each and every time. An fire alarm can also be installed in this system. This system can work as both lock and fire alarm as usually there aren't any fire alarms at home. This door locking system can also be used in banks, hotels, motels, or any different place for additional security as an alternative door lock.

An Electromagnetic Door Locking system with Arduino technology can be made. Implementation of a failsafe maglock (fail Safe = power off, it’s unlocked), fail secure maglock(Fail Secure = power off, it’s locked) also can be implemented.

Separate passwords can be used for controlling Lights, TV, Computer System etc kind of Electrical devices. For further control, personal computer can be easily connected to the system.

If password entered is incorrect for certain times, all the lights remain turn on and also a camera which may be hidden can be used for recording the faces of visitors who trespassed.

This system can be used as an register for the student’s attendance, through which they enter a their respective class room with help of passwords.

A system to open/close a wireless magnetic door using Android smart phone can help disabled people. In the mobile device embedded Bluetooth can consider range and security aspects.

5.3 Applications Contributions

- Secure lock surveillance which is controlled electronically
- Domestic locking systems, which includes safes and cabinets for fruits, wine and food, doors
- Locks in hotels for doors and windows
- Locks in the Industries, Office, Malls, Shops
- Commercial building locking, including sophisticated flexibility in employee access to sections of a building
- Protective door locks
- bank locker purpose(with added security)
- Locks on almanac containing cash or precious things etc

This electronic door locking system is marketable as it is easy to use, inexpensive because of less power consumption as compared to others, and is highly reliable. This door locking system is therefore useful in applications as described above like door locks in hotel room, in residential housing, and even office, banks buildings etc.

5.4 Advantages

- **Unauthorized entry indication is given:** This locking system will only allow the person who enters correct password and will not allow who enter incorrect password and will display log in unsuccessful in case of incorrect password entered by any malicious user.

- **Cost effective:** This locking system has easily available components like resistors, electro-mechanical locks, diode, solenoid and connecting wires and are less costly comparatively from other to security systems.

- **EMF can charge the Battery**: The transformer's primary winding is housed in unit that is connected to AC supply from the mains, while the transformer's secondary winding is being housed in that same sealed unit that has the battery. This also allows the battery to get charged without any mains physical connection and also without any electric shock to the user.

- **No crack for EMF based locking system** : Unlike Wi-Fi or Bluetooth there is no hacking of password until user himself tell other person about this.The data transferred can easily be known or detected, If the system is hacked so.

- **Advantages of Arduino:** Open source**,** Cross-platform and extensible software, clear programming environment, Simple etc

REFERENCES

[1] Lia Kamelia, Alfin Noorhassan S.R, Edi Mulyana, Mada Sanjaya And W.S.,"Door-Automation System Using Bluetooth-Based Android For Mobile Phone", Vol. 9, No. 10, October 2014 Issn 1819-6608 Arpn Journal Of Engineering and Applied Sciences

[2] 2013. Business Insider Homepage [online], available:http://www.businessinsider.com/15-billion-sm rtphonesin- the-world-22013-2?IR=T&.

[3] Pei Zheng, Lionel Ni. 2006. Smart Phone and Next Generation Mobile Computing, Morgan Kaufmann publisher, san Fransisco.

[4] Prof. Pratima Patel and Prof. Samir Ajani, "The Digital Locking and Unlocking System Based on Android" Volume 6, Nagpur, Maharashtra, February 2016

[5] Xiao Lu, Dusit Niyato, Ping Wang, Dong In Kim, and Zhu , "Wireless Charger Networking for Mobile Devices: Fundamentals, Standards, and Applications), 2014

[6] Jojo,"Digital Door Lock – Password based Electronic Code Lock using 8051" ,2016 [online]. Available: http://www.circuitstoday.com/digital-door-lock-password-based-security-8051 [Accessed : 10- Sep- 2016]

[7] Sravanthi Sinha,"Magnetic door lock using arduino" ,2016 [online]. Available: http://www.slideshare.net/SravanthiSinha/magnetic-door-lock-using-arduino-16578354 [Accessed : 20- Aug- 2016]

[8] Zeydin Pala and Nihat Inan, "Smart parking applicationusing RFID technology", RFID Eurasia, 1st Annual in RFID Eurasia, 2007.

[9] R. John Robles and Tai-hoon Kim, 2010. Application, System and Method in Smart Home Technology: A Review, International Journal of Advanced Science and Technology. 15: 37-48.

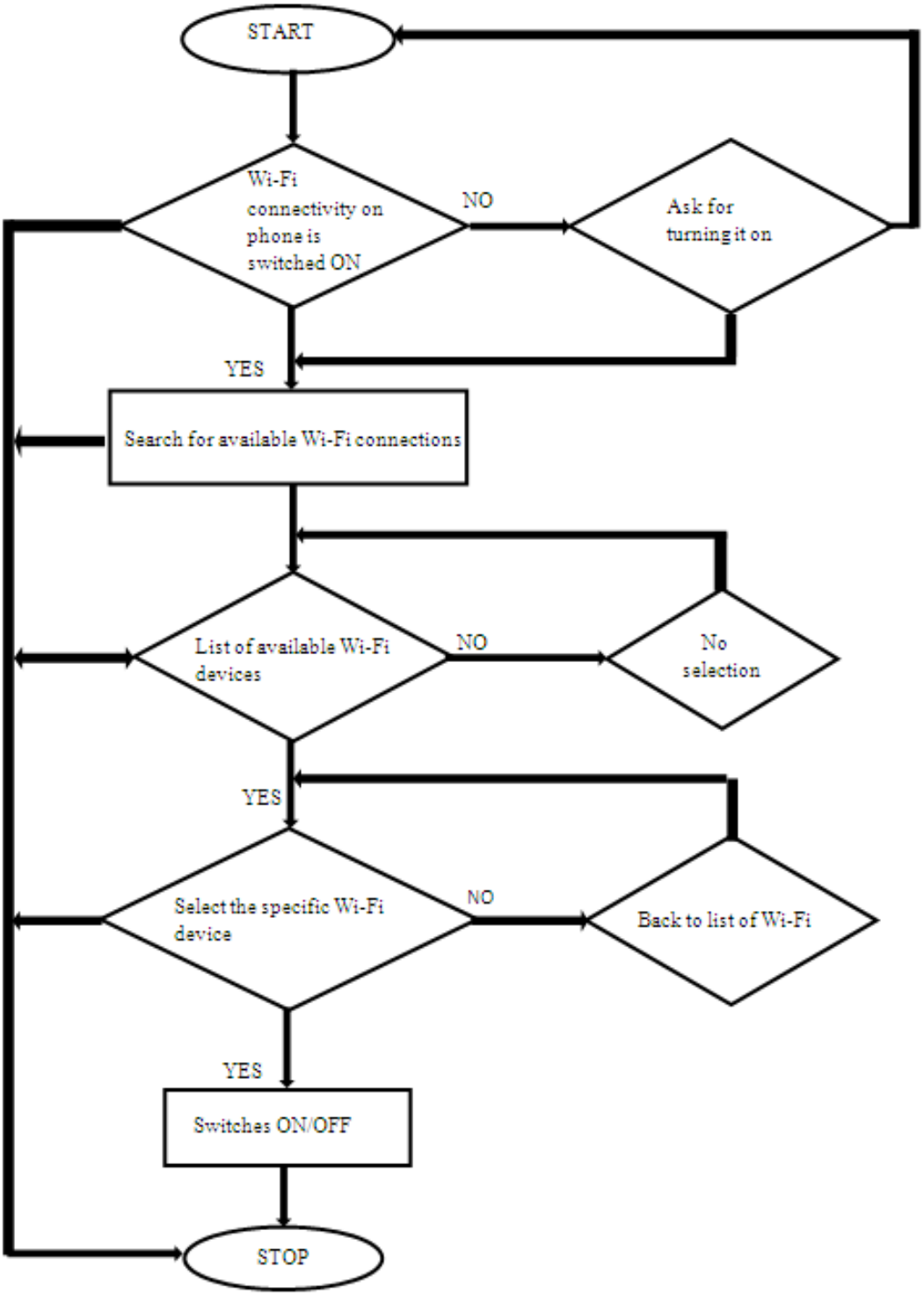
[10] Gyanendra K Verma , Pawan Tripathi "A Digital Security System with Door Lock System UsingRFID Technology", International Journal of Computer Applications (0975 – 8887)Volume 5– No.11, August 2010

[11] N.H. Ismail, Zarina Tukiran,N.N. Shamsuddin, Faculty of Electrical and Electronic Engineering Universitiy Tun Hussein Onn "Malaysia Android-based Home Door Locks Application via Bluetooth for Disabled People" , November , 2014

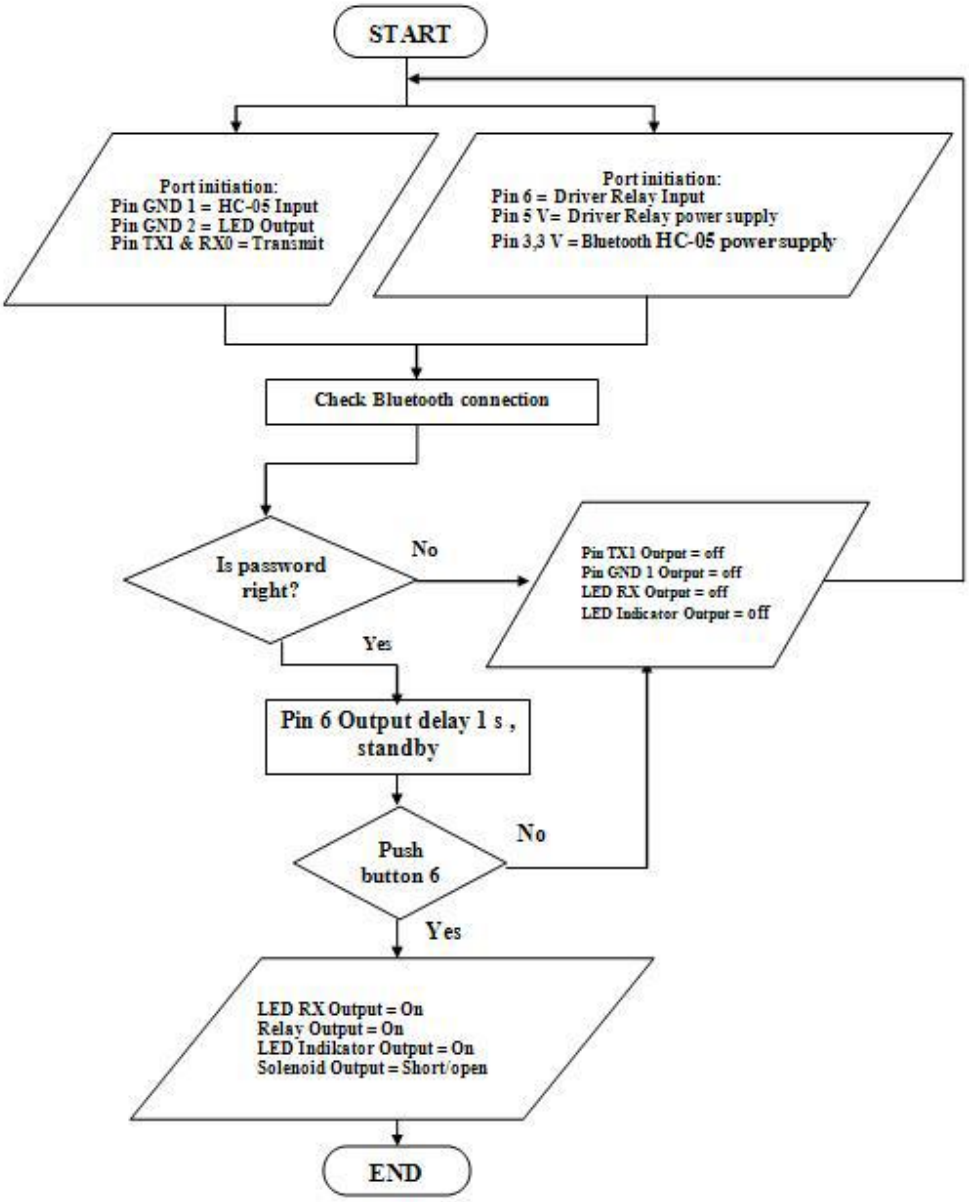
[12] Bassam Ruwaida, Toni Minkkinen, "Home Automation System A cheap and open source alternative to control household appliances"

APPENDICES

A.



B


START
Port initiation:
Pin GND 1 = HC-05 Input
Pin GND 2 = LED Output
Pin TX1 & RX0 = Transmit
Port initiation:
Pin 6 = Driver Relay Input
Pin 5 V= Driver Relay power supply
Pin 3,3 V = Bluetooth HC-05 power supply
Check Bluetooth connection
Is password right?
No
Pin TX1 Output = off
Pin GND 1 Output = off
LED RX Output = off
LED Indicator Output = off
Yes
Pin 6 Output delay 1 s , standby
Push button 6
No
Yes
LED RX Output = On
Relay Output = On
LED Indikator Output = On
Solenoid Output = Short/open
END

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT
LEARNING RESOURCE CENTER

PLAGIARISM VERIFICATION REPORT

Date: 25/04/2017

Type of Document (Tick): Thesis | M.Tech Dissertation/ Report | B.Tech Project Report ✓ | Paper

Name: Diksha , Divyanshu Department: IT

Enrolment No. 131410 , 131411 Registration No. _____

Phone No. 9816927326 , 7017366524 Email ID. khatridiksha7@gmail.com
divyanshu0078@gmail.com

Name of the Supervisor: Dr Punit Gupta

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): IOT BASED EMF DATA TRANSFER FOR ELECTRONIC LOCKING SYSTEM

Kindly allow me to avail Turnitin software report for the document mentioned above.

Diksha
(Signature)
Divyanshu

FOR ACCOUNTS DEPARTMENT:

Amount deposited: Rs. 600/- Dated: 26/4/17 CRV17026/171 Receipt No. .....
(Enclosed payment slip)

(Account Officer)

FOR LRC USE:

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	Report delivered on	Similarity Index in %	Submission Details	
26-04-2017	27-04-2017	13%	Word Counts	10417
			Character Counts	52095
			Page counts	60
			File Size	2.31 M

27/04/2017

Checked by
Name & Signature

Librarian

LIBRARIAN
LEARNING RESOURCE CENTER
Jaypee University of Information Technology
Waknaghat, Distt. Solan (Himachal Pradesh)
Pin Code: 173234

Submission Info

SUBMISSION ID	805697242
SUBMISSION DATE	27-Apr-2017 11:15
SUBMISSION COUNT	1
FILE NAME	project_Report_Diksha_...
FILE SIZE	2.31M
CHARACTER COUNT	52095
WORD COUNT	10417
PAGE COUNT	60
ORIGINALITY	
OVERALL	13%
INTERNET	10%
PUBLICATIONS	5%
STUDENT PAPERS	6%
GRADEMARK	
LAST GRADED	N/A
COMMENTS	0
QUICKMARKS	

LIBRARIAN
LEARNING RESOURCE CENTER
Jaypee University of Information Technology
Waknaghat, Distt, Solan (Himachal Pradesh)
Pin Code: 173234