A

Project Report

On

ELECTRONIC PASSPORT USING RFID

Submitted to

RAJIV GANDHI UNIVERSITY OF KNOWLEDGE TECHNOLOGIES, KADAPA

in partial fulfilment of the requirements for the award of the Degree of

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted by

B.MOUNIKA	**R171210**
N.SRUTHI	**R171136**
B.DHARANI	**R170751**
G.UMESH YADAV	**R170197**

Under the Guidance of

Mrs.V. LAKSHMI PRASANNA, M.Tech
Assistant Professor

Department Of Electronics and Communication Engineering

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

RGUKT, RK VALLEY

(RGUKT KADAPA is approved by UGC, AICTE, established in 2008, provide Education opportunities for rural people)
Vempalli, Kadapa-516330

2019-2023

CERTIFICATE

This is to certify that the project report entitled "ELECTRONIC PASSPORT USING RFID" a bonafide record of the project work done and submitted by

B.MOUNIKA	**R171210**
N.SRUTHI	**R171136**
B.DHARANI	**R170751**
G.UMESH YADAV	**R170197**

for the partial fulfilment of the requirements for the award of B.Tech Degree in **ELECTRONICS AND COMMUNICATION ENGINEERING,** RGUKT , Kadapa.

GUIDE

Mrs.V. Lakshmi Prasanna, M.Tech
Assistant Professor,
Department of ECE

Head of the Department

B. Madhan Mohan
Assistant Professor,
Head of Department of ECE

External Viva-Voice Exam Held on _____

INTERNAL EXAMINER

EXTERNAL EXAMINER

DECLARATION

We hereby declare that the project report entitled **"ELECTRONIC PASSPORT USING RFID"** submitted to the Department of ELECTRONICS AND COMMUNICATION ENGINEERING in partial fulfilment of requirements for the award of the degree of **BACHELOR OF TECHNOLOGY**. This project is the result of our own effort and that it has not been submitted to any other University or Institution for the award of any degree or diploma other than specified above.

B.MOUNIKA	**R171210**
N.SRUTHI	**R171136**
B.DHARANI	**R170751**
G.UMESH YADAV	**R170197**

ACKNOWLEDGEMENT

We are thankful to our guide **Mrs.V. Lakshmi Prasanna,** **M.Tech** for her valuable guidance and encouragement. Her helping attitude and suggestions have helped us in the successful completion of the project.

We would like to express our gratefulness and sincere thanks to Mr.**B. Madhan Mohan**, Head of the Department of ELECTRONICS AND COMMUNICATION ENGINEERING, for his kind help and encouragement during the course of our study and in the successful completion of the project work.

We have great pleasure in expressing our hearty thanks to our beloved Director **Prof.K. Sandhya Rani** for spending her valuable time with us to complete this project.

Successful completion of any project cannot be done without proper support and encouragement. We sincerely thanks to the **Management** for providing all the necessary facilities during the course of study.

We would like to thank our parents and friends, who have the greatest contributions in all our achievements, for the great care and blessings in making us successful in all our endeavors.

B.MOUNIKA **R171210**
N.SRUTHI **R171136**
B.DHARANI **R170751**
G.UMESH YADAV **R170197**

ABSTRACT

This dissertation analyses the use of RFID cards as e-passports instead of the conventional paper passport booklet with an embedded chip as the e-passport. Advancement in technology with so many possibilities that all information can be stored electronically.The purpose is to limit the use of fraudulently documents. This in turn will prevent illegal entry of the traveller into any specifc country at the same time maintaining the privacy and personal security of the e-passport bearers.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVATIONS

RFID	-	Radio frequency identification chip
LCD	-	Liquid Crystal Display
E-PASSPORT	-	Electronic Passport

APPENDIX B

List of Abbreviations

EEPROM	Erasable Electronically Programmed Read Only Memory
E-IDs	Electronic Identity Cards
E-Passport	Electronic Passport
HF	High Frequency
I/O	Input/output
ICAO	International Civil Aviation Organisation
ICT	Information Communications Technology
ID	Identity
LCD	Liquid Crystal Display

APPENDIX C

List of Components

Arduino Uno

RFID Reader

RFID Antenna

16*2 LCD

Resistors

LEDs

RFID cards

CHAPTER 1

1.INTRODUCTION

1.1 MOTIVATION OF WORK

Until recently, the travel documents such as a passport where just on paper possessing only the biographic information of the holder. However the has been a shift in technology such that biometric technologies may now be implemented in travel documents. When implemented in travel documents such reducing forgery. Secure and trusted travel documents are an essential part of international security, as they allow states and international institutions to identify. the movement of undesired or dangerous persons

This project is demonstrating the implementation of an e-passport using Radio Frequency Identity (RFID) cards to store the biographic information of the the limitations that come with RFID such as:

- RFID is susceptible to easy disruption this is because RFID systems make use of the electromagnetic spectrum thus they are easy to jam if energy is applied at the right frequency. If this is to happen at the border control checkpoints it can be very disastrous and it will inconvenience the travellers because this will mean longer waits at the checkpoints.
- RFID reader collision - If this system is to be implemented most probably at the border control check points there will be many readers, then certain techniques must be implemented to overcome this problem. Reader collision takes place when there are two or more signals from diferent readers that will be overlapping. One of the techniques that may be implemented to overcome this problem is making use of an anti-collision protocol.

Tag collision – If this system is implemented this is a more realistic problem as it is due to the presence of many tags in a small area. At the border controls of a truth there is no point where thereif this is achieved then at the same time the chances of having one's RFID card being read without their knowledge is reduced or even eliminated . Also if this is achieved this will mean that tags will only be one tag to be read,but the reader must be able to diferentiate signals from diferent tags only be read when tapped,swiped or scanned

Security problems with RFID – If RFID tags are used with a high gain antenna they may be read at a greater distance leading to privacy problems. However this may be overcome by using low gain antennas such that the distance between the tag and the reader is kept very small.

The project is interested in fnding out if the integration of RFID into passports will improve card in the project prototype and identifying the e-passport holder. The implementation of robustness against identity theft by storing the information of the passport bearer passports might eventually replace the conventional paper passport and accelerate clearance controls.

1.2 Problem Statement

This research is motivated by the problems that many countries are facing all over the comes to the issues of conventional paper passport booklets. The problems with paper do not provide privacy, identity can be revealed to anyone who can physically access the passport can be used by someone else what is known as identity theft, data can be Modifed on the passport as everything is accessible and readable and it can be duplicated. This will afect both the user and the border control checkpoints.Having noted the problems that come with paper passports it has also come to note that the use of forged passports by drug couriers and illegal immigrants is increasing and it comes with varying techniques such as photo substitution in combination with data alteration and look-alike fraud which neither requires photo substitution nor data alteration in our traditional paper passports.

Meanwhile, the added security that e-Passports can provide, with the provison That they are used correctly,will likely mean that fraudalent travellers will move away from falsifed passports and instead seek to subvert the border control system either by attempting look alike fraud using genuine documents, or by trying to subvert process in order to be fraudulently issued with genuine e-Passports. With the high crime rates that Zimbabwe is facing presently it is very easy for one to commit a crime and escape for countries over the borders before they are caught or brought to justice.

Thus the researcher hopes that by adopting e-passports the above problems will be a thing of the past as this system if implemented may also be linked to the Criminal Investigation Department (CID) of the country and an alert can be send to the border controls with the details of the people under investigation, thereby reducing the possibilities of criminals leaving the country.

States decide how long their passports will be valid. Most countries issue passports with a fve to ten year validity.In Zimbambwe adult passport booklets when issued are for ten years and for the children they are valid for fve years.

But with the passing of time personal appearances change such that by the time this passport expires there is need for new photographs because the images previously taken for the passport holder no longer resembles them as they will be presently,hence the rationale for wanting to fnd out the efectiveness of using e-passports as their images may constantly be updated in the systems database without having to worry about issuing another passport booklet to the holder.

The other problem with these conventional passport booklets is that for the business people who travel very often the pages are not sufcient and this requires them to apply for other passports when they have used up their pages before they exhaust the validity of their passports. This brings about the issue of stamping ,with the conventional paper passport booklets when the holder is granted access at the border controls their passport booklets are stamped indicating also the duration they have been granted to stay in the foreign land. This project is assuming that the border controls and immigration ofces will have a receipting system in place such that for the travellers with e-passports when granted access they are given this recepient which they are supposed to carry with them wherever they are in the foreign land. This receipt should should be stating that this traveller is an e-passport holder who has been granted Access in the foreign land for such duration.

Then if it so happens that the e-passport holder is required to produce their passport in the foreign land for instance by the police then they should produce that receipt together with their national Identity card.

Warsaw states that:

"The passport serves as an identifcation document and maybe checked by regular police or in criminal justice chain. Since establishing the identity of the holder is very important in these cases as well as verifying organisations may want to read and verify the chip."

Thus the researcher anticipates that the RFID card will be very useful to the business people as they do not have to worry about using up their pages. Moreover the card is portable,cheaper and requires shorter waiting periods when acquiring them. The card has so many advantages over the paper passport because with the paper passport sophisticated security features apply with them such as high Quality papers and adhesives, special or optical variable inks which are expensive, to mention but just a few.In Zimbabwe the paper that makes up the pages of the passport booklet is the same paper that is used for the money notes hence the chances of having one's passport being stolen with fraudsters is very high and take the pages and use them to print fake money notes.In addition the other pro blem is the time it takes to replace a lost or stolen passport in Zimbabwe, but system will speed up the processing. The process time will be greatly reduced while the tradition inspection requires information to be inputted manually.

1.3 Project Objective

To design a prototype that will resemble the operation of an e-passport booklet but using an RFID card eliminating the conventional paper passport booklet. The objective is to improve passport security by creating a stronger link between the passport and its holder.

1.3.1 Objective1

To develop an e-passport system using RFID cards.

1.3.2 Objective2

- To provide an afordable solution with the adoption of e-passports.
- To enhance imposter detection.
- To make it almost impossible to alter a document for use in gaining admission.
- To guard against multiple passport issuances to the same person.
- To provide protection against identity theft.

2.LITERATURE SURVEY

The e-passport possesses two aspects of technology which are RFID and bio metrics all incorporated so as to securely identify and verify the bearer possessing that travel document. In this section of chapter one the writer will site, acknowledge and quote similar works that have been done on the e-passport in brief and also state how this project is going to be diferent from all these works.

E-passports are already available and in use in several European countries and several researches have been conducted around the world following their deploy ment in these countries. Kumar discussed the efcient implementation of e-passports scheme using cryptographic security along with multiple biometrics. In this article he states that an e-passport is an identifcation document which possesses relevant bio graphic and biometric information of its bearer on paper and also has this information embedded on an RFID chip which is capable of cryptographic functionality.However this project seeks to eliminate the design of having a passport booklet with an RFID chip embedded on it but instead just make use of an RFID card with all the informa tion stored on that card.

In the e-passport design Kumar also talks of the certifcation whereby the authe tication procedure involves two processes which are Registration and Verifcation whereby during the former phase the applicant registers their biometric under human supervision and the data is stored on the passport tag. However the

In the e-passport design Kumar also talks of the certifcation whereby the authe tication procedure involves two processes which are Registration and Verifcation whereby during the former phase the applicant registers their biometric under human supervision and the data is stored on the passport tag. However the

In a thesis written by BC Vollmer in 2006 titled Biometrics, RFID technology and the e-passport he states that the American e-passport will have an RFID chip embedd ed inside the back cover of the passport booklet and it will store the same information that is printed on the bio-data page of the passport booklet. This project argues that if the passport booklet and the chip are both stored with the same information why then not resort to only one thing – the RFID card which will store all the information because RFID cards are easy to replace if lost or stolen and they are portable (easy to move around with or carry with you all the time) than a passport booklet.

Take note that the RFID card and the Chip use the same principle of operation and the same technology. No doubt that this RFID card then must incorporate strong security features to guard against skimming and information altering.

Vollmer also states that the RFID chip found in the e-passport is a passive, write once, read many version of an RFID chip technology. Whereas this project would like to consider the possibilities of writing on the RFID card several times so as to constantly update the photographs of the passport holders in the system after a certain period of time so as to keep them updated as possible. With the American e-passports chips can not be altered after production. The writer Vollmer mentions also of the read range of this American electronic passport which is about 121.92cm and it is the read range When the passport is opened. Now with the RFID tags it will depend with the type which one is using but the ones suitable for this project are the Low frequency RFID tags which have a lower read range than that of the chip. Since transmitting any further than a few centimetres.

With these entire facts one can conclude that with the use of an RFID based e-pass port it will be very difcult for sophisticated counterfeiters to steal these RFID based e-pass ports cards and alter the details to match them. It should prove to be impossible.
#comparison in between existing methods and proposed method

This project endorses these major objectives of this department by providing a fast and more efcient way to issue out passports to the general public. Although now the process of passport issuances has greatly improved than in the previous years, a more faster and efcient way will be provided in the sense that passports will be applied for and issu ed on the very same day and the waiting period will have been reduced to a few hours rather than the normal 4-6 weeks of the conventional passport booklet.

3.THEORETICAL ASPECTS

3.1 Introduction

We will discuss about existing methods and the proposed method here.Then We compare the both methods and discuss advantages and disadvantages.

3.2 Existing Methods

3.2.1 Paper based Passport System

A passport is an ofcial travel document issued by a government that contains a persons identity.A person with a passport can travel to and from countries more easily. A passport certifes the personal identity and natinality of its holder.It is typical for passports to contain the full name,photograph,place and date of birth,signature,and the expiration date of the passport.while passports are typically issued by national governments,certain subnational governments are authorised to issue passports to citizens residing within their borders.

This paper based passport is made with paper similar to a note book which is small in size. This passport will be verifed at airports by some authoritiThises.The following fgures are examples of passport.

Fig3.2.1 Passport

Fig3.2.2 Inside of a passport

Drawbacks :

Use of paper based passports have increased risk of security threats

3.3 Proposed Method

What is e-passport ?

The passport which contains electronic chip is called electronic passport (e-passport). This chip houses biometric information of the passport holder such as iris,fngerprints, facial information etc. It also stores other useful information of the passport holder which include name, birth date, present address, photograph etc.This e-passport stores digitally signed personal particulars of the individual on the chip. The frst e-passport was introduced in 1998 by Malaysia. US Government has introduced e-passports in 2006.

Fig 3.2.3 E- passport

The common features of e-passport are as follows.

- Chip contains memory with 64 Kilobytes of size.
- Can store information of about 30 visits.
- Embossed holographic image
- Biometric and demographic information of the holder.
- Stores iris and fngerprints of the bearer.
- Stores colour photograph and digital signature of the bearer.

This project can be used for security purpose where it gives information about the authorized persons and unauthorised persons.This can be applied in real time systems as time systems as such in recording the attendance,in the companies,airports for accessing the passports and in industries to know who are authorized.RFID is increasingly used with biometric technologies for security.Primarily,the two main components involved in a Radio

And the Interrogator(RFID reader).Communication between the RFID reader and tags Occurs wirelessly and generally doesn’t require a line of sight between the devices.

The aims of these mechanisms, among others, are:

1) Prevention of data skimming/eavesdropping on the communication between the chip and the reader

2)Data authentication (to ensure the data was not altered)

3)Chip authentication (to ensure that the chip is not manipulated or cloned)

4)Data security (to ensure the information used by issuers)

Data skimming/ eavesdropping prevention

e-Passports are protected by Basic Access Control (BAC). BAC establishes an encrypted Channel of communication between the reader and the chip thus preventing eavesdropping -by using a password called an access key.This access key is generated via a Combination Of the basic information of the document holder and is presented in the Machine Readable Zone(MRZ) to make it easily readable by a device.
The basic idea behind the access key is that you need access to the holder page of The passport to be allowed to read the chip like in a normal inspection environment where a

Traveler would hand over their passport to an agent.

Using BAC gives access to all information on the chip with one exception: fngerprints. Access to these is not possible without authorization from the issuing country.
Keep in mind fngerprints are unique to each other,eminently private and therefore very sensitive to handle.

Document data authentication

The data authentication mechanism involves both a private key and a public key.
The holder data is signed by the government with a private key and the immigration ofcer verifes that this data is actually from the issuing government by using that government's public key. The match of the two keys guarantees the data is as originallyissued by the government.

Clone detection

While the previous step aims at proving the unaltered nature of the data itself, it does not Guarantee the data,even when duly signed, was not copied and loaded from anothe passport. The most common security mechanism for clone detection in passport is called "active authentication." Simply put,it uses the chip's unique security number to guarantee that the chip interacting with the reader at the border is the same one that was used when the chip data were signed by the issuing country.

Public Key Infrastructure

The secure and reliable exchange of certifcates between the various countries

Issuing and verifying passports is based on:

1)The use of a specialized PKI applicable to travel document issuance and inspection, To guarantee the data signature and authenticity

2)Of certifcates from all countries that are active members of the scheme

3.4 Hardware Components

3.4.1 RFID System

Basically RFID (Radio Frequency Identifcation) is a wireless link to uniquely identify Objects are people. RFID enables identifcation from a distance without requiring line of sight.

The RFID system comprises the RFID tag/card, RFID reader, backend database and a control unit. RFID systems have two nroad categories passive and active.

The RFID reader communicates with the RFID tag

through tag interrogation.

3.4.2 RFID Tags/Cards

RFID tags/cards consist of an Integrated circuit attached on an antenna that is printed, etched or stamped onto a base which is often a paper substrate of Polyethylene Terephthalate (PET). The inlay which is the combination of the chip and antenna is then inserted amid the printed label and its adhesive backing or it is either placed in a more durable structure.

The tag consists of the following:

a) A radio frequency chip

b) Encoding and decoding circuitry

c) Antenna unit and

d) A memory unit.

Passive Tags	Semi-active Tags	Active Tags
These are tags with internal Internal power supply	These are also tags without internal power supply but the internal power supply internal memory circuitry.	These use their internal power unit to power both the antenna unit and its internal circuitry.

Tags can be classifed depending on their power capacity into passive, semi-active and active tags. The distinction of these classifcations is illustrated in the above table.

In addition tags can also be categorized basing on their frequency of communication. The energy,read range and in some cases the size of the tag is determined by the communication frequency between the tag and the reader.

Fig. 3.4.1 above shows an example of the type of RFID cards that are going to be used in this project

3.4.3 RFID Reader

The RFID reader is also known as an interrogator, it provides the connection between the tag data and the software that needs the information.

The image below is showing an RFID reader.

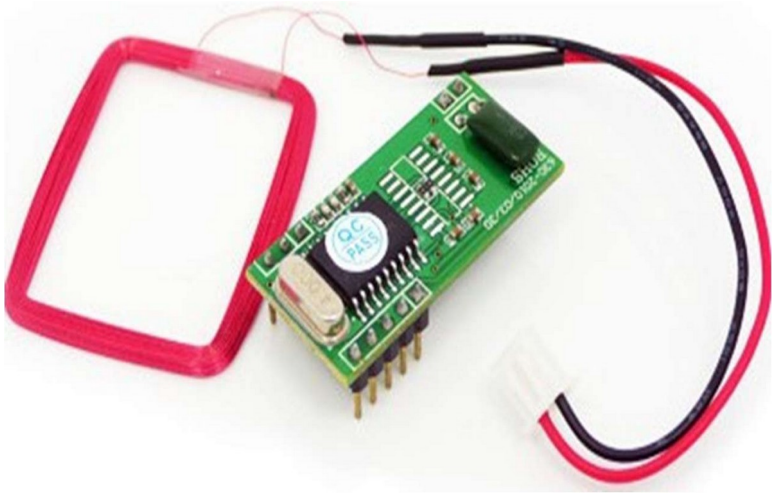

Fig 3.4.2 RFID Reader

By making use of an attached antenna, the reader extracts the data on the tags And then sends the data to a host computer for further processing.

Reader antennas

Their function is to change electrical current to electromagnetic signals that Are emitted into space where they are able to be received by the tag antenna and are Changed back to electrical current.Two most common reader antenna types are:

Linear antennas

1)These radiate electric felds that are linear.

2)Have long ranges.

3)These signals have the ability to enter various diverse materials so as to read tags Due to their high levels of power.

4)They are very sensitive to tag orientation.

5) They can experience a difcult time reading tags depending on the tag angle or placement.

Circular polarized antennas

1)These emit circular felds.

2)They are sensitive to orientation to a lesser extent.

3) Circular polarized antennas deliver less power than linear antennas.

3.4.4 Operating Frequency of RFID Systems

Basing on their operating frequency RFID tags can be classifed into three categories which are:

i.Low Frequency (LF)

ii.High Frequency (HF) and

iii.Ultra High Frequency (UHF)

Table 3-2 Categories of RFID tags and their diferences

	Low Frequency Tags	High Frequency Tags	Ultra High Frequency Tags
Operating Frequency	Operate at 125kHz there are some that operate at 134kHz.	operates at 13.56M Hz.	Frequencies range between 300MHz-30 Hz.
Operating Range	Operate within the Range of >=30kHz and<=300kHz	Operates within the range of >=3MHz <=30MHz.	In Gen-2 protocols operate in ranges of >=866MHz and <=960MHz.
Read Range	Has a short read 10cm.	Read ranges are between 10cm and 1m.	
Read Speed	Has a slower read speed than High Frequencies.		
Sensitivity to Radio Waves Interference	Not very sensitive.	Experience moderate sensitivity to interference.	
Use		It is the most used tag.It is used for ticketing,payment and data transfer applications.	Applicability varies in diferent countries.

It is these operating frequencies that determine the data rate and the read range of an RFID system. For passive RFID tags they operate at>30cm for LF and >7m for UHF tags. Yet for an active tag the range can span to 100m because the tag does not require the reader to power its internal circuitry.

3.4.5 Working Principle of an RFID system

Basically the RFID structure comprises of three elements which are:

1)An antenna or coil

2)Transponder (RF Tag) electronically programmed with unique information.

3) Transceiver (with decoder)

These elements communicate by means of radio signals,which carry data either Unidirectinal or bidirectional. When a transponder gets into a read zone, its contents are captured by the reader and can then be transferred thriugh standard interfaces to host devices such as a computer, printer or programmable logic controller(PLC)for storage or action.

3.4.6 Merits of RFID systems

1)Tag detection which does not require human intervention eliminates human errors from data collection.

2)No line of sight is required hence tag placement is not as much constrained. Distinctive item identifcation is easy to implement with RFID.

3) RFID has the ability to identify items individually instead of generically.

4)Tags are less afected by adverse conditions such as dust, chemicals, Physical damage, etc. meaning they are able to with-stand harsh environmental conditions.

5)RFID tags can be combined with sensors.

6)Tracking people, items and equipment in real time.

3.4.7 Demerits

1) Faulty manufacture of tags manufacturing is not until now 100% failure free currently.

2) Standardization – The sparse standards leave much freedom in the choice of
a)communication protocols and the format and amount of information stored in the tag.
b)Collision – If several tags are read at a time it may result in signal collision and result In data loss.

3..4.8 Arduino Uno board

The Arduino UNO R3 is frequently used microcontroller board in the family of an Arduino. This is the latest third version of an Arduino board and released in the year 2011.The main advantage of this board is if we make a mistake we can change the microcontroller on the board. The main features of this board mainly include, it is available in DIP,detachable and ATmega328 microcontroller. The programming of this board can easily be loaded by using an Arduino computer program. This board has huge support from the Arduino community,which will make a very simple way to start working in embedded electronics ,and many more applications.

What is Arduino Uno R3?

Arduino Uno R3 is one kind of ATmega328P based microcontroller board. It includes the Whole thing required to hold up the microcontroller; just attach it to a PC with the help of a USB Cable,and give the supply using AC-DC adapter or a battery to get started. The term Uno Means “one” in the language“Italian” and was selected for marking the release of Arduino’s IDE . 1.0software.The R3 Arduino is the 3rd as well as most recent modifcation of the Arduino Uno, Arduino board and ID reference versions of Arduino and currently progressed to new releases. The Uno-board is the primary in a sequence of USB- Arduino board & the reference model designed for the Arduino platform.

Fig 3.4.3 Arduino Uno Board

Arduino Uno R3 Specifcations

The Arduino Uno R3 board includes the following specifcations.

- The Operating Voltage of the Arduino is 5V
- The recommended input voltage ranges from 7V to 12V
- The i/p voltage (limit) is 6V to 20V
- Digital input and output pins-14
- Digital input & output pins (PWM)-6
- Analog i/p pins are 6
- DC Current for each I/O Pin is 20 mA
- DC Current used for 3.3V Pin is 50 mA
- Flash Memory -32 KB, and 0.5 KB memory is used by the boot loader
- SRAM is 2 KB
- EEPROM is 1 KB
- The speed of the CLK is 16 MHz
- In Built LED
- Length and width of the Arduino are 68.6 mm X 53.4 mm
- The weight of the Arduino board is 25 g

Arduino Uno R3 Pin Diagram

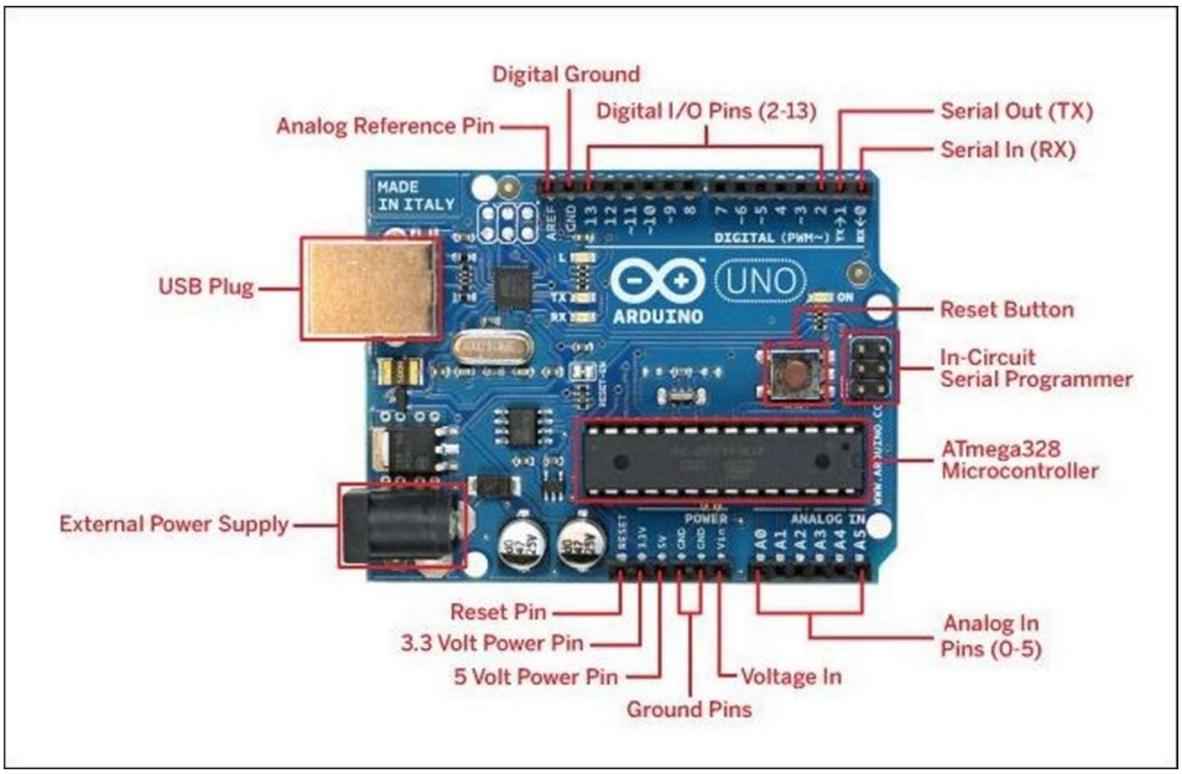

Fig 3.4.4 Pin Diagram of Arduino Uno Board

The Arduino Uno R3 pin diagram is shown below. It comprises 14-digit I/O pins. From these pins, 6-pins can be utilized like PWM outputs.This board includes 14 digital input/ output pins,Analog inputs-6, a USB connection,quartz crystal-16 Mhz,a powerjack, a USB connection resonator-16MHz, a power jack, an ICSP Header an RST button.

Power Supply:-

The power supply of the Arduino can be done with the help of an exterior power supply otherwise USB connection.The exterior power supply(6 to 20 volts)mainly includes a battery or an AC to DC adapter. The connection of an adapter can be done by plugging a center--positive plug (2.1mm) into the power jack on the board.The battery terminals can be placed in the pins of Vin as well as GND. The power pins of an Arduino board include the following board include the following.

Vin:-

The input voltage or Vin to the Arduino while it is using an exterior power supply opposite to volts from the connection of USB of else RPS(Regulated Power Supply)By using this pin, one can supply the voltage.

5Volts:-

The RPS can be used to give the power supply to the microcontroller as well as components which are used on the Arduino board.This can approach from the input voltage through a regulator.

3V3:-

A 3.3 supply voltage can be generated with the onboard regulator, and the highest draw Will be 50mA.

GND:

GND (ground) pins

Memory:-

The memory of an ATmega328 microcontroller includes 32 KB and 0.5 KB memory is utilize for the Boot loader),and also it includes SRAM-2 KB as well as EEPROM-1KB

Input and Output:-

We know that an arguing Uno R3 includes 14-digital pins which can be used as an input otherwise output by using the functions like pin Mode(),digital Read(),and digital Write(). These pins can operate with 5V, and every digital pin can give or receive 20mA,&includes a 20k to 50k ohm pull up resistor.The maximum current on any pins is 40mA which cannot surpass for avoiding the microcontroller from the damage.Aditionally,some of the pins of an Arduino include specifc functions.

Serial Pins:-

The serial pins of an Arduino board are TX (1) and RX (0) pins and these pins can be used to transfer the TTL serial data.The connection of these pins can be done with the equivalent pins of the ATmega8 U2 USB to TTL chip.

External Interrupt Pins:-

The external interrupt pins of the board are 2 & 3, and these pins can be arranged to activate an interrupt on a rising otherwise falling edge,a low-value otherwise a modify in value.

PWM Pins:-

The PWM pins of an Arduino are 3, 5, 6, 9, 10, & 11, and gives an output of an 8-bit PWM with the function analog Write().

SPI (Serial Peripheral Interface) Pins:-

The SPI pins are 10, 11, 12, 13 namely SS, MOSI, MISO, SCK, and these will maintain the SPI Communication with the help of the SPI library.

LED Pin:-

An arguing board is inbuilt with a LED(Light Emitting Diode) using digital pin-13. Whenever the digital pin is high,the LED will glow otherwise it will not glow.

TWI (2-Wire Interface) Pins:-

The TWI pins are SDA or A4, & SCL or A5, which can support the communication of TWI with the help of Wire library.

AREF (Analog Reference) Pin:-

An analog reference pin is the reference voltage to the inputs of an analog i/ps using The function like analog Reference().

Reset (RST) Pin:-

This pin brings a low line for resetting the microcontroller, and it is very useful for using an RST button towards shields which can block the one over the R3 board.

Communication:-

The communication protocols of an Arduino Uno include SPI, I2C, and UART Serial Communication.

UART:-

An Arduino Uno uses the two functions like the transmitter digital pin1 and the receiver Digital pin0.These pins are mainly used in UART TTL serial communication.
UART stands for universal-asynchronous receiver and transmitter.

SPI Pins:-

The SPI communication includes MOSI, MISO, and SCK.

MOSI (Pin11):-

This is the master out slave in the pin, used to transmit the data to the devices

MISO (Pin12):-

This pin is a serial CLK, and the CLK pulse will synchronize the transmission of which Is produced by the master.

SCK (Pin13):-

The CLK pulse synchronizes data transmission that is generated by the master. Equivalent pins with the SPI library is employed for the communication of SPI.ICSP(in-circuit serial programming) headers can be utilized for programming Atmega controller directly with the boot loader.

Arduino Uno R3 Programming:-

1)The programming of an Arduino Uno R3 can be done using IDE software.
2)The microcontroller on the board will come with pre-burned by a boot loader that Permits to upload fresh code without using an exterior hardware programmer.
3)The communication of this can be done using a protocol like STK500.
We can also upload the program in the microcontroller by avoiding the boot loader Using the header like the In-Circuit Serial Programming.

3.4.9 LCD Display

One of the most common devices attached to an 8051 is an LCD display. Some of the most common LCDs connected to the 8051 are 16*2 and 20*2 displays.This means 16 characters per line by 2 lines and 20 characters per line by 2 lines,resoectively.
In recent years the LCD is fnding widespread use replacing

LED’s.

This is due to the following reasons:

1. Declining prices
2. Ability to display numbers, characters and graphics.
3. Incorporation of a refreshing controller into the LCD.
4. Ease of programming

Fortunately, a very popular standard exists which allows us to communicate with the vast majority of LCDs regardless of their manufacturer.The standard is referres to as HD44780U, which refers to the controller chip which receives data from an external source LCD, requires 3 control lines as well as either 4 or 8 I/O lines for the data bus. The user may select whether the LCD is to operate with a 4-bit data bus or an 8-bit data bus.If a 4-bit data bus is used the LCD will require a total of 7 data lines(3 control lines plus the 4 lines for the data bus). If an 8-bit data bus is used the LCD will require a total of 11 data lines (3 control lines plus the 8 lines for the data bus).

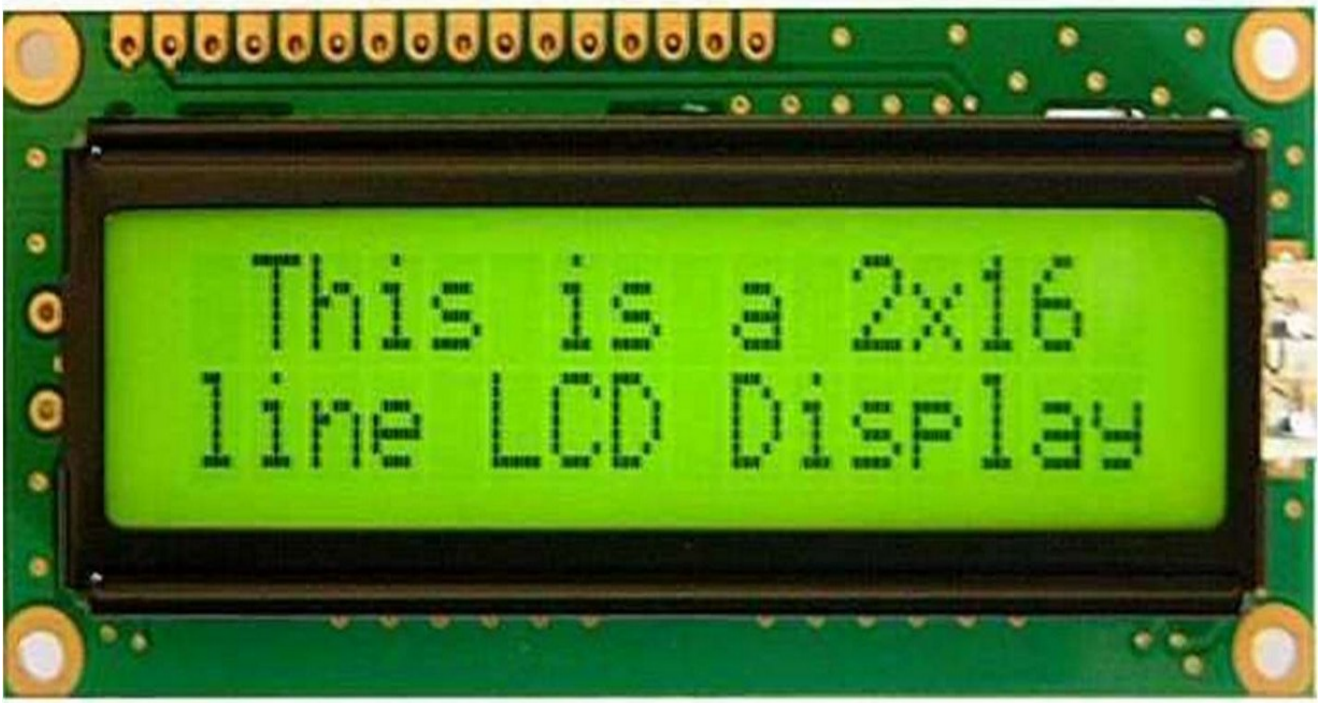

Fig 3.4.5 Liquid Crystal Display

Table LCD pin symbol I/O description

PIN NO	Symbol	Fuction
1	VSS	GND
2	VDD	+5V
3	V0	Contrast adjustment
4	RS	H/L Register select signal
5	R/W	H/L Read/Write signal
6	E	H/L Enable signal
7	DB0	H/L Data bus line
8	DB1	H/L Data bus line
9	DB2	H/L Data bus line
10	DB3	H/L Data bus line
11	DB4	H/L Data bus line
12	DB5	H/L Data bus line
13	DB6	H/L Data bus line
14	DB7	H/L Data bus line
15	A	+4.2V for LED
16	K	Power supply for BKL(0V)

Important Signals:-

The following pins are important to LCD’s while programming

Enable (EN):-

The EN line is called "Enable." This control line is used to tell the LCD that you are sending it data. To send data to the LCD,your program shoukd make sure this line is low (0) and then set the other two control lines and/or put data on the data bus. When the other lines are completely ready, bring EN high (1) and wait for the minimum amount of time required by the LCD datasheet (this varies from LCD to LCD), and end by bringing it low (0) again.

Register Select (RS):-

The RS line is the "Register Select" line. When RS is low (0), the data is to be treated as a command or soecial instruction(such as clear screen,position cursor,etc.) When RS is high (1), the data being sent is text data which should be displayed on the screen.For example, to display the letter "T" on the screen you would set RS high.

Read/Write (R/W):-

The RW line is the "Read/Write" control line. When RW is low (0), the information on the data bus is being written to the LCD .When RW is high(1),the program is efectively querying (or reading) the LCD. Only one instruction (“Get LCD status”)is a read command. All others are write commands so RW will almost always be low.Finally, the data bus consists of 4 or 8 lines (depending on the mode of operation selected by the user). In the case of an 8-bit data bus, the lines are referred to as DB0, DB1, DB2, DB3,DB4, DB5, DB6, and DB7.

Above is the quite simple schematic. The LCD panel's Enable and Register Select is connected to the Control port.The control port is an open collector/open drain output. While most Parallel Ports have internal pull-up resistors,there is a few which don't. Therefore by incorporating the two 10K external pull up resistors ,the circuit is more 18 portable for a wider range of computers, some of which may have no internal pull up resistors.

We make no efort to place the Data bus into reverse direction. Therefore we hard wire the R/W line of the LCD panel,into write mode.This will cause no bus confcts on the data lines. As a result we cannot read back the LCD's internal Busy Flag which tells us if the LCD has accepted and fnished processing the last instruction .
This problem is Overcome by inserting known delays into our program.

The 10k Potentiometer controls the contrast of the LCD panel. Nothing fancy here. As with all the examples ,I've left the power supply out.You can use a bench power supplyset to 5v or use a onboard +5 regulator.Remember a few de-coupling capacitors, especially if you have trouble with the circuit working properly.

Table : LCD command set

Code (Hex)	Command to LCD Instruction Register
1	Clear Display screen
2	Return home
4	Decrement cursor (Shift cursor to left)
6	Increment cursor (Shift cursor to Right)
5	Shift display right
7	Shift display left
8	Display off, cursor off
A	Display on, cursor off
C	Display on, cursor off
E	Display on, cursor blinking
F	Display on, cursor blinking
10	Shift cursor position to left
14	Shift cursor position to right
18	Shift the entire display to the left
1C	Shift the entire display to the right
80	Force cursor to beginning of 1st line
0C0	Force cursor to beginning of 2nd line
38	2 lines and 5x7 Matrix

3.4.10 Jumper Wires

A jump wire is an electrical wire or group of them in a cable, with a connector or pin at each end (or sometimes wothout them-simply “tinned”),which is normally used to interconnect the components of a breadboard or other prototype or test circuit, internally or with other equipment or components, without soldering.

Individual jump wires are ftted by inserting their "end connectors" into the slots provided in a breadboard, the head connector of a circuit borad,or apiece of test equipment.

There are diferent types of jumper wires. Some have the same type of electrical connector at both ends, while others have diferent connectors.

Some common connectors are:

1)Solid tips – are used to connect on/with a breadboard or female header connector. The arrangement of the elements and ease of insertion on a breadboard allows increasing the mounting density of both components and jump wires without fear of short-circuits. The jump wires vary in size and colour to distinguish the diferent working signals.

2)Crocodile clips are used, among other applications, to temporarily bridge sensors, buttons and other elements of prototypes with components or equipment that have arbitrary connectors, wires,screw terminals etc.,

3)Registered jacks(RJnn) – are commonly used in telephone (RJ11) and compute.
4)RCA connectors– are often used for audio, low-resolution composite video signals, frequency applications requiring a shieleded cable.

5)RF connectors are used to carry radio frequency signals between circuit, which is used to connect antennas and other components to network cabling. Jumpers are also used in base stations to connect antennas to radio units. Usually the most bendable jumper cable diameter is 1/2.

Fig 3.4.6 Jumper Wires

3.4.11 Bread Board

A breadboard, solderless breadboard, or protoboard is a construction base used to build semi-permanent prototypes of electronic circuits.Unlike a perfboard or stripboard, breadboards do not require soldering or destruction of tracks and hence reusable.

For this reason, breadboards are also popular with students and in technological education. A variety of electronic systems may be prototyped by using breadboards, from small analog and digital circuits to complete central processing units(CPUs).

Compared to more permanent circuit connection methods, modern breadboards have high parasitic capacitance,relatively high resistance,and less reliable connections,which which are subject to jostle and physical degradation.Signaling is limited to about 10 Mhz, and not everything works properly even well below that frequency.

Fig 3.4.7 BreadBoard

Uses of Breadboard

A breadboard is used to make up temporary circuits for testing or to try out an idea. No soldering is required so it is easy to change connections and replace components. Parts are not damaged and can be re- used afterwards.

Almost all the Electronics Club website projects started life on a breadboard to check that the circuit worked as intended.

Connections on Breadboard

Breadboards have many tiny sockets (called 'holes') arranged on a 0.1" grid. The leads of most components can be pushed straight into the holes.Ics are inserted across the central gap with their notch or dot to the left.

Wire links can be made with single-core plastic-coated wire of 0.6mm diameter (the standard size), this is known as 1/0.6mm wire.I suggest buying a pack with several colours to help identify connections, red for +Vs wires,black for 0V,and so on.

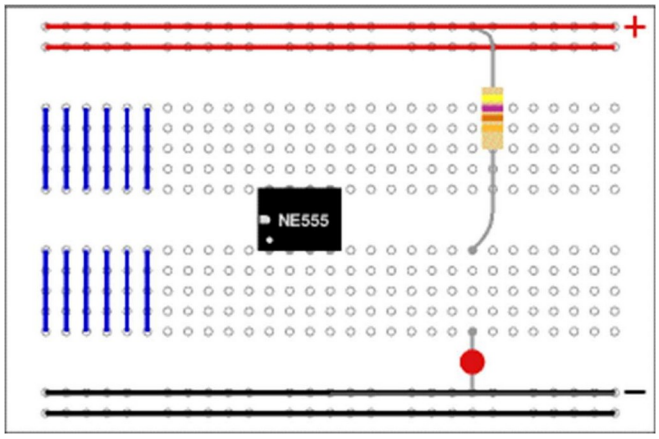

Fig:-3.10 The diagram shows how the breadboard holes are connected

The top and bottom rows are linked horizontally all the way across as shown by the red and black lines on the diagram.The power supply is connected to these rows,+ at the top and 0V (zero volts) at the bottom.The other holes are linked vertically in blocks of 5 with no link across the centre as shown by the blue lines on the diagram.Notice hoe there are separate blocks of connections to each pin of Ics.

3.5 Software Requirements:

1.Embedded C in Arduino

Embedded C is a set of language extensions for the C Programming language by The standards committe to address community issues that exist between c extension Embedded for diferent embedded systems. Historically,embedded C programming requires nonstandard extensions to the C language in order to support exotic features such as fxed-point arithmetic, multiple distinct memory banks, and basic I/O operations.

CHAPTER 4

DESIGNING PROCESS

4.1 Block Diagram of RFID System

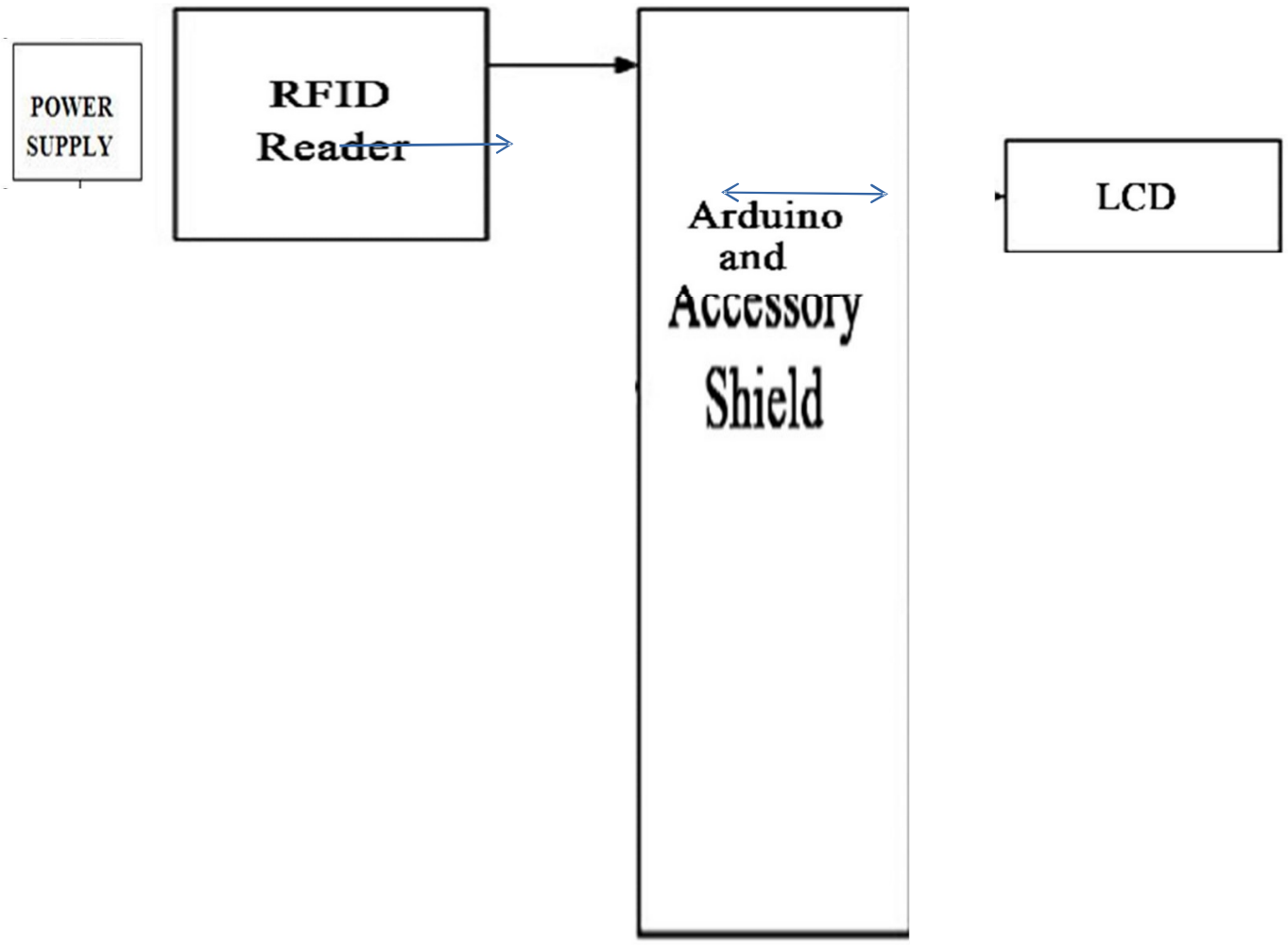

Fig 4-1 Block Diagram E passport using RFID System

The block diagram in the above fgure shows the overall electronic passport architecture.When an individual arrives at the border control checkpoint they produce their RFID card on the RFID reader.The RFID reader in-turn defects the passport RFID card and it decodes the information embedded on the card.If there is no match the LCD's invalid,and alarm is signifed by a red led and the user is denied access.

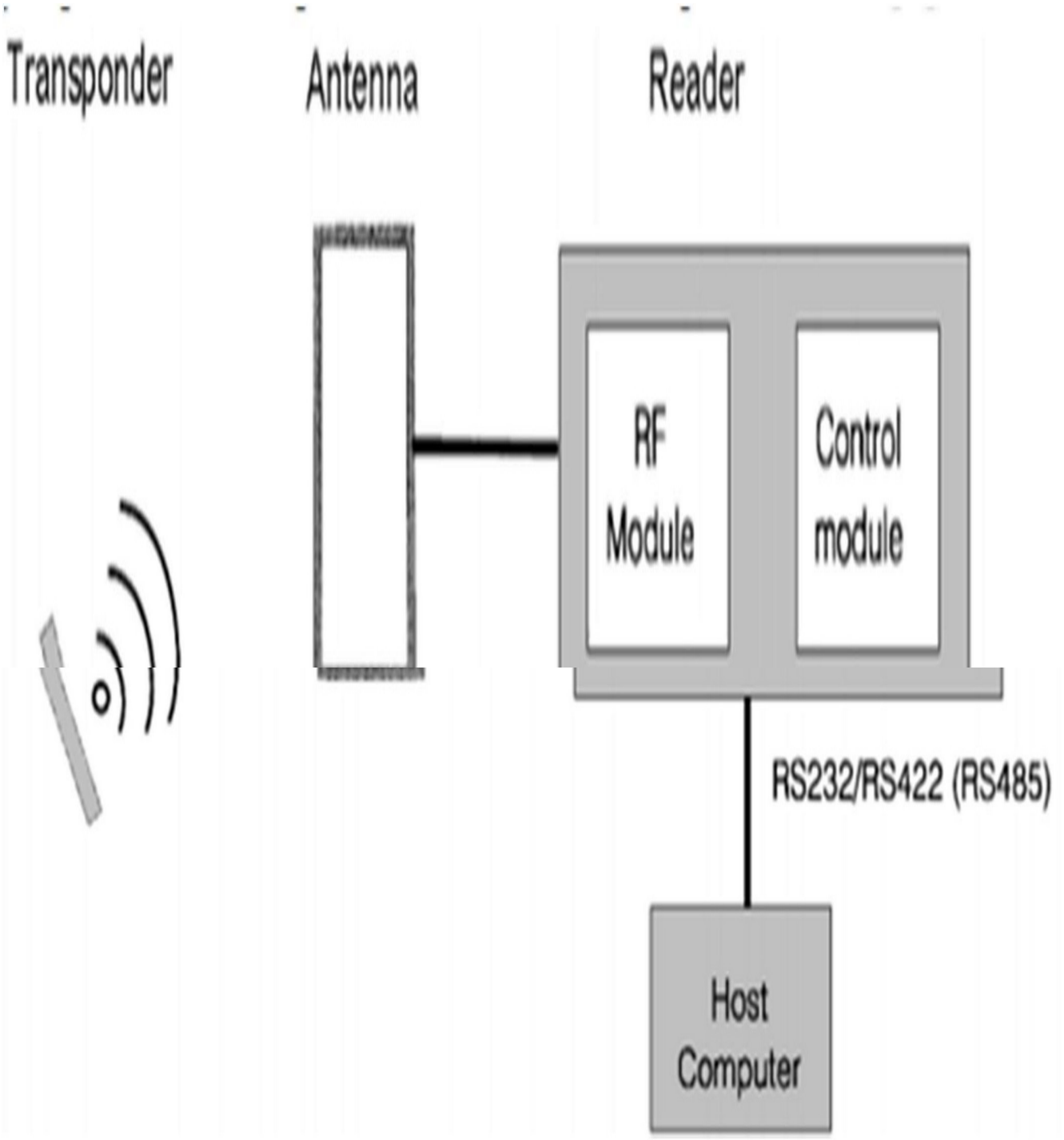

Fig 4-2 process fowchart of RFID module

CHAPTER 5
EXPERIMENT ANALYSIS

5.1 CODE IMPLEMENTATION:

5.2.1 CODE FOR TESTING INFORMATION

```
#include <SPI.h>
#include <MFRC522.h>
#include <LiquidCrystal.h>
#include <LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x27,16,2);// includes the LiquidCrystal Library
 // Creates an LCD object. Parameters: (rs, enable, d4, d5, d6, d7)
#defne SDA_PIN 10
#defne RST_PIN 9
MFRC522 mfrc522(SDA_PIN, RST_PIN);   // Create MFRC522 instance.
void setup()
{
  lcd.begin(16,2);
  lcd.print("Show your Card");
  // Look for new cards
  Serial.begin(9600);   // Initiate a serial communication
  SPI.begin();      // Initiate  SPI bus
  mfrc522.PCD_Init();   // Initiate MFRC522
  Serial.println("Approximate your card to the reader...");
  Serial.println();
}
void loop()
{
```

```
 if ( ! mfrc522.PICC_IsNewCardPresent())
 {
  return;
 }
 // Select one of the cards
 if ( ! mfrc522.PICC_ReadCardSerial())
 {
  return;
 }
 //Show UID on serial monitor
 Serial.print("UID tag :");
 String content= "";
 byte letter;
 for (byte i = 0; i < mfrc522.uid.size; i++)
 {
    Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
    Serial.print(mfrc522.uid.uidByte[i], HEX);
    content.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
    content.concat(String(mfrc522.uid.uidByte[i], HEX));
 }
 Serial.println();
 Serial.print("Message : ");
 content.toUpperCase();
  if (content.substring(1) == "D9 56 A4 24") //change here the UID of the card/cards
that you want to give access
 {
     Serial.println("Authorized access");
     Serial.println()
      lcd.clear();
       lcd.setCursor(0,0);
```

```
      lcd.print("   Authorized");
      lcd.display();
      lcd.setCursor(0,1);
      lcd.print("information matched");
      delay(3000);
  }
  else
    if (content.substring(1) == "D1 F8 52 73") //change here the UID of the card/cards
that you want to give access
    {
      Serial.println("Authorized access");
      Serial.println();
      lcd.clear();
     lcd.setCursor(0,0);
      lcd.print("   Authorized");
      lcd.display();
      lcd.setCursor(0,1);
      lcd.print("information matched");
      delay(3000);
      }
 else   {


      Serial.println(" Access denied");
      lcd.clear();
      lcd.setCursor(0,0);
      lcd.print("  Access denied");
      lcd.setCursor(0,1);
      lcd.print("  Wrong Card! ");
     delay(3000);
```

RESULT ANALYSIS

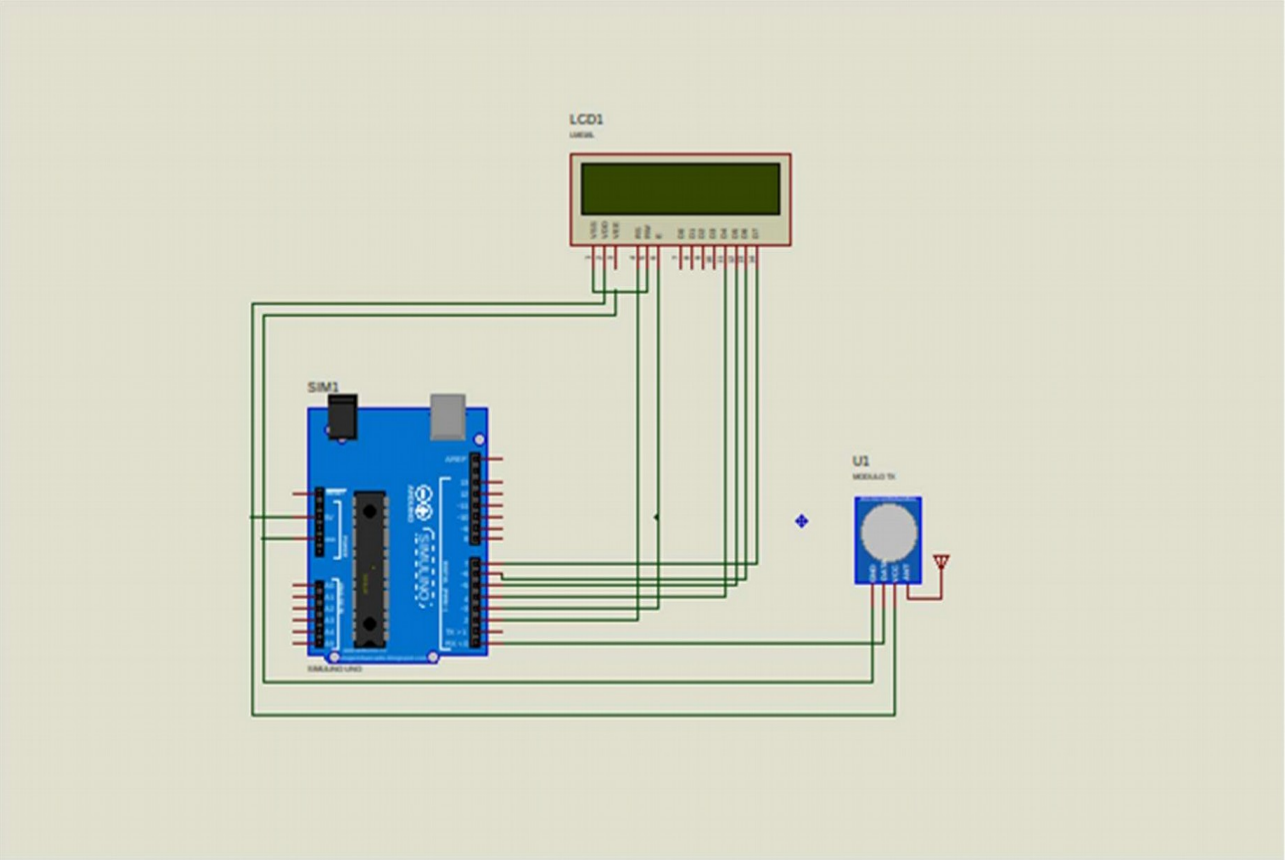

Fig 5-1 Schematic Diagram of Electronic Passport using RFID

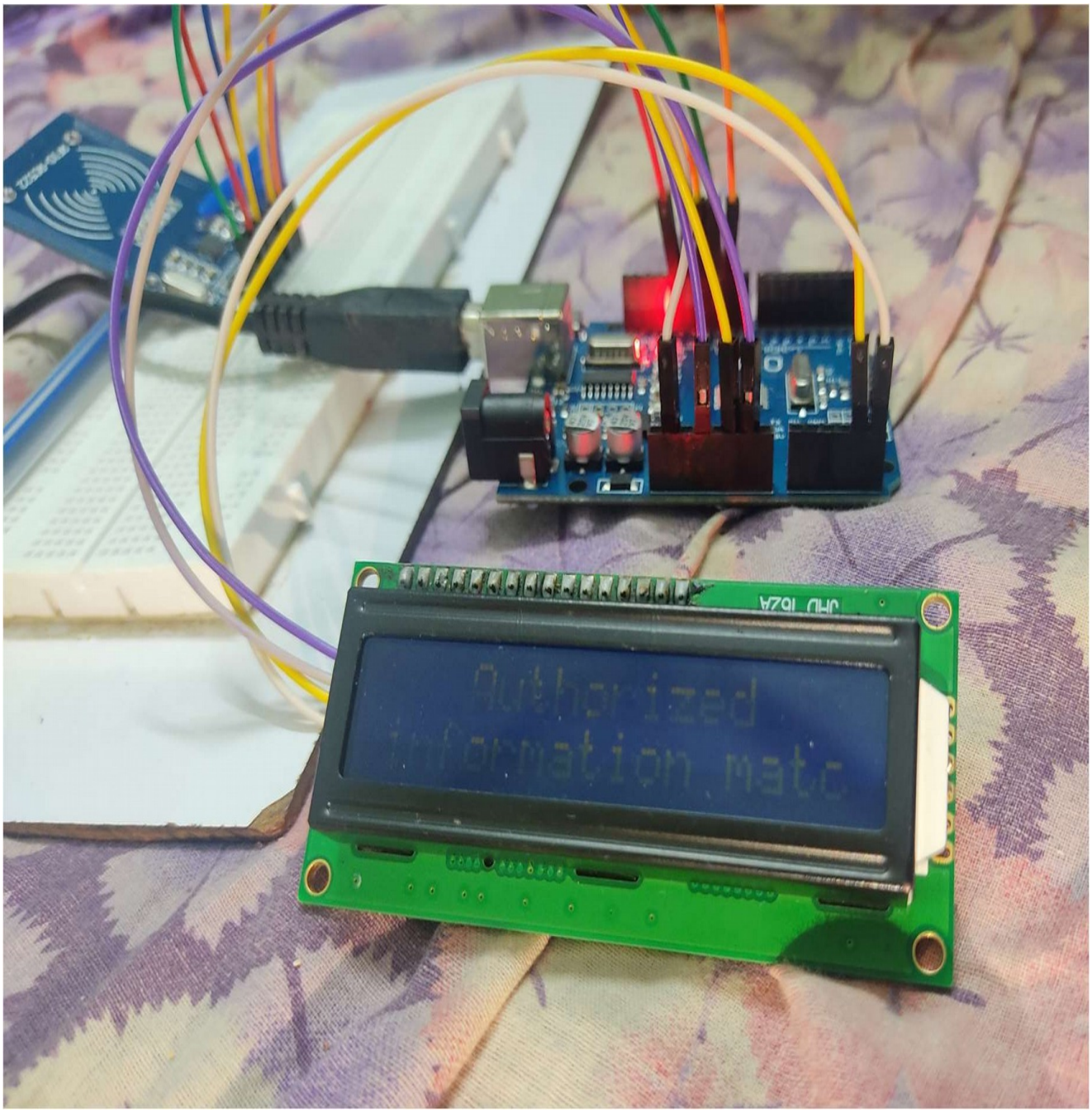

Fig. 4-3 Display showing the data

The RFID reader is interfaced with the reader antenna on the pins labelled ANTO and ANT1 where the e- passport RFID card is tapped.

Having tapped the card, if it is a valid card, the details shown on Fig. 4-2 are Displayed on the Arduino serial monitor and the LCD. These results were shown On a LCD display circuit of the prototype available.

Fig 5-4 Results for Tag1

From the results shown on Fig. 4-4 above it can be observed that tag is also valid, meaning that it is recognized by the system and has its details stored in the system which are then displayed after the card has been swiped.

The below fgure shows the results of a swiped electronic passport using RFID.Based on having we can able to diferentiate the authorised users and unauthorised users.

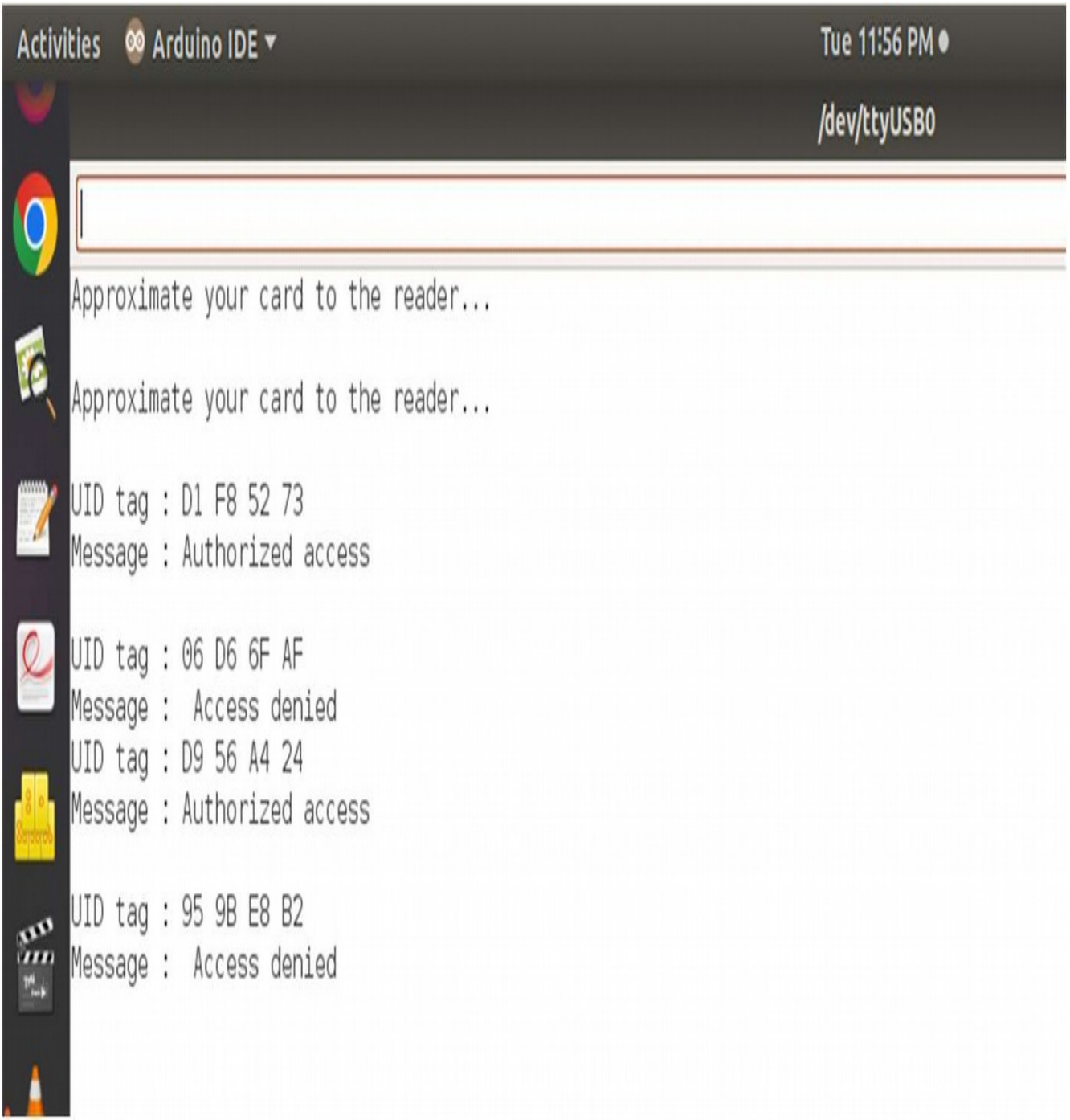

Fig:5.5 Results for diferent Tags

Fig. 5-5 is showing the results for tag three. The results are for an invalid card which is not recognized by the system and this is signifed by a red led on the circuit of the available prototype. This is the result that should be obtained for any card that would not have had its details previously stored in the system.

A total of three RFID cards were administered and out of these three, all the three were successfully read by the RFID reader giving a 100% RFID reader response. Of these three cards two were valid and one was not valid.

CHAPTER 6
CONCLUSION

This RFID based e-passport prototype was successful. The biographic information of the e-passport holder was able to be electronically stored and retrieved without any difculties.This project ensures that privacy is ensured as the holder's identity will not be revealed to anyone as these details are stored electronically but will only be revealed to the authorized personnel who can access the serial monitor. Problems such as photo substitution and forgery are inevitable and problems like look-alike fraud and data duplication are eliminated. These results show that security is highly ensured. The fast response of the RFID cards means that movement at the border checkpoints will be fast.

6.1 Analysis:

of forgery, duplication of identity or identity theft, major problems which come with the conventional paper passport booklet. The system also proves that it is possible to constantly update the details of the card holder in the system without any problems.

The RFID cards as soon as they enter the electromagnetic feld zone of the reader they are read without any hassles and in a split of a second the details of the card are displayed on the system monitor. Thus the system saves time and provides enriched border control.

For any RFID cards which will not have been stored in the system's database these were not recognized by the system. In the event that there are some who will present any RFID cards to the system there is guarantee that they will not be recognized by the system. The e-passport as observed from the prototype demonstration (available) is a user-friendly system which one can easily adapt to.The project showed positive results as the passport details could be viewed on the system monitor without any problems.

Advantages :

1) It reduces threat of identity fraud by increasing security features in it.

2) It embeds biometric informations such as fngerprint, iris and face. These informa tion helps to identify individual carrying e-passport.

3) It helps in detection of counterfeit documents.

4) It makes it very difcult to alter the e-passports. Hence it restricts admission of Unauthorized individuals to any country on fake documents.

5) It protects privacy of the citizens.

6) Tempering of the chip is notifed to the system which results into passport authent ication failure.

7) It can be scanned in few seconds which avoids long wait for passengers.

Disadvantages :

Following are the disadvantages of e-passport:

- Contactless RFID embedded chips can be read using radio frequency from few centimeters away. Unprotected chips are subject to clandestine scanning or eavesdropping.
- E-passports use standard ISO 14443 which generates unique chip ID during protocol initiation. Using this unique chip ID, e-passport holder can be tracked by unauthorized parties.
- Digital signatures used in e-passports do not bind data to any particular chip used on passport. Hence it does not ofer any defense for passport cloning.
- E-passport supports automation which can lead to biometric data-leakage and consecutively weakens human oversight.
- Passport to reader communication should be authenticated and encrypted which is optional mechanism as per ICAO guidelines. If it is not implemented then it may lead to cryptographic weaknesses between passport and reader.

6.1 Conclusion :

This project endorses these major objectives of this department by providing a fast and more efcient way to issue out passports to the general public. Although now the process of passport issuances has greatly improved than in the previous years, a more faster and efcient way will be provided in the sense that passports will be applied for and issued on the very same day and the waiting period will have been reduced to a few hours rather than the normal 4-6 weeks of the conventional passport booklet.

6.2 Future Scope:

As anticipated in the ICAO guidelines, e-passports will likely see use not just in airports but in new areas like e-commerce and they may also provide valuable experience in how to build more secure and moreprivate identifcation platforms in the years to come. Thus another area of study might be to look into the future use of the e-passports.The issue of e-passports serving as e-IDs must also be taken into consideration. In an article in the Newsday on July 23, 2014 the Registrar General Tobaiwa Mudede Wanted the alreadyexisting plastic IDs as passports thus if this system can be implemented such that these RFID cards will also be serving as the e-ID then theycan serve multiple purposes. The issuance of Visas on the e-passport must Also be considered. How visas can be implemented in-conjunction with these e-passports is also another area which can be studied in the future.

CHAPTER 7
REFERENCES

https://nevonprojects.com/rfd-based-passport-project

https://www.researchgate.net/publication/347841967_RFID_Based_E-Passport_System

www.circuits.com/interfacing-lcd-to-arduino

https://en.wikipedia.org/wiki/Biometric_passport