REMOTE ACCESS TO IMPROVE ATM SECURITY

BY USING IOT

A PROJECT REPORT

Submitted by

ABIRAMI.K(810015104004)

KIRUTHIGA.S(810015104039)

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

UNIVERSITY COLLEGE OF ENGINEERING – BIT CAMPUS,

TIRUCHIRAPPALLI

ANNA UNIVERSITY::CHENNAI 600 025

APRIL 2019

UNIVERSITY COLLEGE OF ENGINEERING,

BIT CAMPUS,

TIRUCHIRAPPALLI-620 024

BONAFIDE CERTIFICATE

Certified that this project report"**Remote Access To Improve ATM Security By Using IOT**" is the bonafide work of **" Ms. K.ABIRAMI (810015104004)** and **Ms.S.KIRUTHIGA (810015104039) "** who carried out the project work under my supervision.

SIGNATURE

Mr. D. Venkatesan

HEAD OF THE DEPARTMENT

Assistant Professor
Computer Science & Engineering
University College of Engineering,
Anna University-BIT Campus,
Tiruchirappalli-620 024

SIGNATURE

Ms.N.Vivekapriya

SUPERVISOR

Assistant Professor
Computer Science & Engineering
University College of Engineering,
Anna University-BIT Campus,
Tiruchirappalli-620 024

Submitted for the project Viva voce examination held on ……

Internal Examiner **External Examiner**

DECLARATION

We hereby declare the work entitled "**REMOTE ACCESS TO IMPROVE ATM SECURITY BY USING IOT"** is submitted in partial fulfillment of the requirement for the award of the degree in B.E., Computer Science and Engineering, University College of Engineering(BIT Campus), Tiruchirappalli, is a record of our own work carried out by us during the academic year 2018-2019 under the supervision and guidance of Ms.N.Vivekapriya, Teaching Fellow, Department of Computer Science and Engineering, University College of Engineering(BIT Campus), Tiruchirappalli. The extent and source of information are derived from the existing literature and have been indicated through the dissertation at the appropriate places. The matter embodied in this work is original and has not been submitted for the award of any degree, either in this or any other University.

SIGNATURE OF THE CANDIDATES

K.ABIRAMI (810015104004)

S.KIRUTHIGA (810015104039)

I certify that the declaration made above by the candidate is true.

SIGNATURE OF THE GUIDE

Ms.N.VIVEKAPRIYA

Teaching Fellow,

Department of CSE,

University College of Engineering,

BIT Campus, Anna University,

Tiruchirappalli-620 024.

ACKNOWLEDGEMENT

I would like to convey my heartfelt thanks to our honorable Dean **Dr. T. SENTHILKUMAR,** Associate Professor for having provided me with all required facilities to complete my project without hurdles.

I would like to express my sincere thanks and deep sense of gratitude to guide **Mr. D. VENKATESAN,** Assistant Professor and Head, Department of Computer Science and Engineering, for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of this project work.

I would like to thank my project guide **Ms.N.VIVEKAPRIYA,** Teaching Fellow, Department of Computer Science and Engineering, for his valuable guidance throughout the phase of the project. It is our responsibility to thank our project coordinator **Mr. C. SANKAR RAM,** Assistant Professor, Department of Computer science and Engineering for his constant inspiration that he has all through the project period.

I would like to thank **Mr. C. SURESH KUMAR,** Teaching Fellow, Department of Computer Science and Engineering, for his encouragement for this work.

I extend my thanks to all other teaching and non-teaching staffs for their encouragement and support.

I thank my beloved parents and friends, for their full support in my career development of this project.

TABLE OF CONTENTS

ABSTRACT

Our project proposes a secured ATM (Automated Teller Machine) system using a card scanning system along with LINK system for improved security. Usual ATM systems do not contain the LINK feature for money withdrawal. If an attacker manages to get hold of ATM card and the pin number, he may easily use it to withdraw money fraudulent. So our proposed system supports the ATM card scanning system along with an LINK system. This user may scan his card and login to the system. But after user is through with this authentication he may view details but is asked to enter LINK as soon as he clicks money withdrawal option. At this stage the system generates and sends an LINK to the registered mobile number to that particular user. The password is generated ad sent to the user mobile phone. He now needs to enter the LINK in the system in order to withdraw money. Thus our system provides a totally secure way to perform ATM transactions with two level security structure.

LIST OF FIGURES

LIST OF ABBREVIATIONS

IOT	Internet Of Things
GSM	Global System for Mobile
LCD	Liquid Crystal Display
GPRS	General Packet Radio Service
TDMA	Time Division Multiple Access
CDMA	Code Division Multiple Access
TTL	Transistor-Transistor Logic
RFID	Radio Frequency Identification
SIM	Subscriber Identity Module
HLR	Home Location Register
MS	Mobile Station
VLR	Visitor Location Register
BTS	Base Transceiver Station
EIR	Equipment Identity Register
BSC	Base Station Controller
AC	Authentication Center
MSC	Mobile services Switching Center
PSTN	Public Switched Telecomm Network
VLR	Visitor Location Register
ISDN	Integrated Services Digital Network

CHAPTER 1

INTRODUCTION

An embedded system is some combination of computer hardware and software, either fixed in capability or programmable, that is designed for a specific function or for specific functions within a larger system. Industrial machines, agricultural and process industry devices, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines and toys as well as mobile devices are all possible locations for an embedded system. Embedded systems are computing systems, but can range from having no user interface (UI) -- for example, on devices in which the embedded system is designed to perform a single task -- to complex graphical user interfaces (GUI), such as in mobile devices. User interfaces can include buttons, LEDs, touchscreen sensing and more. Some systems use remote user interfaces as well. Embedded systems can be microprocessor or microcontroller based. In either case, there is an integrated circuit (IC) at the heart of the product that is generally designed to carry out computation for real-time operations. Microprocessors are visually indistinguishable from microcontrollers, but whereas the microprocessor only implements a central processing unit (CPU) and thus requires the addition of other components such as memory chips, microcontrollers are designed as self-contained systems. Embedded systems can be microprocessor or microcontroller based. In either case, there is an integrated circuit (IC) at the

heart of the product that is generally designed to carry out computation for real-time operations. Microprocessors are visually indistinguishable from microcontrollers, but whereas the microprocessor only implements a central processing unit (CPU) and thus requires the addition of other components such as memory chips, microcontrollers are designed as self-contained systems.

With the development of computer network technology and e-commerce, the self-service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. Nowadays, using the ATM (Automatic Teller Machine) which provides customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years; a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects[4]. Using credit card and password cannot verify the client's identity exactly. Anyone who knows the PIN and have the ATM card can easily access the user account.

Figure1. ATM. This paper describes a new method combining with the traditional method. Here RFID and GSM is used to improve the security of the transaction[2][3]. To overcome the disadvantages of inserting the ATM card

into the ATM machine, RFID card is used. It reads the user information by sensing and it also manages different banks accounts in a single RFID card. The GSM is used to improve the security by providing OTP and also informs the user by an SMS in case the entered password is wrong.

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. The IoT is a giant network of connected things and people – all of which collect and share data about the way they are used and about the environment around them. That includes an extraordinary number of objects of all shapes and sizes – from smart microwaves, which automatically cook your food for the right length of time, to self-driving cars, whose complex sensors detect objects in their path, to wearable fitness devices that measure your heart rate and the number of steps you've taken that day, then use that information to suggest exercise plans tailored to you. There are even connected footballs that can track how far and fast they are thrown and record those statistics via an app for future training purposes.

CHAPTER 2

LITERATURE SURVEY

1. Enhancing security and privacy in biometrics-based authentication systems: N. K. Ratha, J. H. Connell, R. M. Bolle

Reliable user authentication is becoming an increasingly important task in the Web-enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer or network access. Many other applications in everyday life also require user authentication, such as banking, ecommerce, and physical access control to computer resources, and could benefit from enhanced security. It is important that such biometrics-based authentication systems be designed to withstand attacks when employed in security-critical applications, especially in unattended remote applications such as ecommerce. In this paper we outline the inherent strengths of biometrics-based authentication, identify the weak links in systems employing biometrics-based authentication, and present new solutions for eliminating some of these weak links. Although, for illustration purposes, fingerprint authentication is used throughout, our analysis extends to other biometrics-based methods.

2. Graphical Password Authentication: Implementation and Evaluation of Personalized Persuasive Cued Click Points: Asher D'Mello, Rohan Bagwe, Victor Fernandes, Ankita Karia

Persuasive Cued Click-Points (PCCP) is an integrated evaluation of the graphical password scheme, including usability and security evaluations, and implementation considerations. The systematic examination provides a comprehensive and integrated evaluation of PCCP covering both usability and security issues. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of higher security, in the sense of being from an expanded effective security space. This research work explores the possibility of designing and constructing a module that is easily pluggable into the existing authentication systems being used as of now. The working prototype is an open source simulation consisting of all the necessary modules to build the authentication system. This system is built using Java and Oracle 10g Express Edition as the database although most database systems can be used.

3. A Smart User Interface to Prevent Shoulder Surfing Attack Using Color Code: Yathiraj GR, Santosh VG, Sushma KR, Muthappa KU

Classical PIN entry mechanism is broadly used for authenticating a user. It is a popular scheme because it properly balances the usability and safety aspects of a organism. However ,if this scheme is to be used in a public system then the design might endure since accept surfing attack. In this attack, an

unauthorized user can completely or partially watch the login session .Even the activities of the login gathering can be recorded which the attacker can use it soon after to get the actual PIN. In this paper ,the suggest an intelligent user interface, known as Color Pass to oppose the accept surfing attack so that any authentic user can enter the session PIN without disclosing the authentic PIN. The Color Pass is based on a partially noticeable attacker model. The experimental analysis shows that the Color Pass interface is secure and simple to use even for novice users.

4. Biometric Online Signature Verification: Fincy Francis1, Aparna M.S, Anitta Vincent

Person identification can be done precisely by Biometrical method, where physiological or behavioral characteristics are used for this purpose. Handwritten signature is a behavioral trait it can be used for person identification accurately. There are two types of identification modes either online or offline mode. Which depends upon the signature acquisition method. In offline acquisition method the shape of the signature is used for authenticating signer. While in online signature verification uses dynamic characters that is dynamic time dependent of the signature to authenticate the signer. This paper describes the implementation on field programmable gate arrays (FPGAs) of an embedded system for online signature verification. The online signature recognition algorithm mainly consists of three stages. Initial pre-processing is the first stage which is applied on the captured signature for

removing noise and normalizing information related to horizontal and vertical positions. Dynamic time warping algorithm is used to align this processed signature with its template previously stored in a database. Finally, a set of features is extracted and passed through a Gaussian Mixture Model. Degree of similarity between both signatures can be find out from this. For fast computation of floating point calculations vector floating point unit is used (VFPU). Additionally system consists of a microprocessor which interacts with the VFPU. All the procedures of verification can be done in software. Furthermore this paper studies about online signature verification on touch interface-based mobile devices. A simple and effective method for signature verification is developed. An online signature is represented with a discriminative feature vector derived from attributes of several histograms that can be computed in linear time. The resulting signature template is compact and requires constant space.

5. Touchscreen Mobile Authentication Using Multi-Touch Sequential Gestures: Balaji Chaugule*, Prof. Asha Pawar

Recently all handheld devices are touch screen and the popularity of touchscreen devices increases more and more due to the easy fast Internet access and large storage capacity. People may store their all personal information such as banking detail, password, confidential documents, trade secrets etc. on the handheld devices. In any case such handheld device is lost or stolen then security of such handheld device are more important because it

contains users personals, banking information, secrets of user and that can be misuse by unauthorized person in any terrorist activity or other purposes that harm to user financially and socially. Securing the personal data stored and accessed from android touchscreen mobile makes user authentication a problem of paramount importance. The rigidity between security and usability renders however the task of user authentication on mobile devices a challenging task. This paper introduces Multi-Touch Authentication and unauthorized user tracking technique to protect mobile banking data stored on touch screen mobile devices (Finger gestures with priority Authentication System using Touch screen Devices), a behavioural touch screen based authentication approach on mobile devices. Besides extracting touch data from touch screen equipped smart phones. This system complements and validates this data using a touch screen mobile device. A addressable feature in the system is its continuity, users transparent post login authentication and tracing of location of mobile devices.

6. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens: Marian Harbach1, Alexander De Luca2, Serge Egelman

To prevent unauthorized parties from accessing data stored on their smartphones, users have the option of enabling a “lock screen” that requires a secret code (e.g., PIN, drawing a pattern, or biometric) to gain access to their devices. We present a detailed analysis of the smartphone locking mechanisms currently available to billions of smartphone users worldwide. Through a month-long field study, we logged events from a panel of users with

instrumented smartphones. There are able to show how existing lock screen mechanisms provide users with distinct tradeoffs between usability (unlocking speed vs. unlocking frequency) and security. The find that PIN users take longer to enter their codes, but commit fewer errors than pattern users, who unlock more frequently and are very prone to errors. Overall, PIN and pattern users spent the same amount of time unlocking their devices on average. Additionally, unlock performance seemed unaffected for users enabling the stealth mode for patterns.

7. Color PIN- Securing PIN entry through indirect input: Alexander de luca

Automated teller machine (ATM) frauds are increasing drastically these days. When analyzing the most common attacks and the reasons for successful frauds, it becomes apparent that the main problem lies in the PIN based authentication which in itself does not provide any security features (besides the use of asterisks). That is, security is solely based on a user's behavior. Indirect input is one way to solve this problem. This mostly comes at the costs of adding overhead to the input process. We present ColorPIN, an authentication mechanism that uses indirect input to provide security enhanced PIN entry. At the same time, ColorPIN remains a one-to-one relationship between the length of the PIN and the required number of clicks. A user study showed that ColorPIN is significantly more secure than standard PIN entry while enabling good authentication speed in comparison with related systems.

8. DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices

Toan Van Nguyen, Napa Sae-Bae , Nasir Memon

This paper presents DRAW-A-PIN, a user authentication system on a device with a touch interface that supports the use of PINs. In the proposed system, the user is asked to draw her PIN on the touch screen instead of typing it on a keypad. Consequently, DRAW-A-PIN could offer better security by utilizing drawing traits or behavioral biometrics as an additional authentication factor beyond just the secrecy of the PIN. In addition, DRAW-A-PIN inherently provides acceptability and usability by leveraging user familiarity with PINs. To evaluate the security and usability of the approach, DRAW-A-PIN was implemented on Android phones and 3203 legitimate finger-drawn PINs and 4655 forgery samples were collected through an extensive and unsupervised field experiment over 10 consecutive days. Experimental results show that DRAW-A-PIN achieves an equal error rate of 4.84% in a scenario where the attacker already knows the PIN by shoulder surfing. Finally, results from a user study based on the System Usability Scale questionnaire confirm that DRAW-A-PIN is highly usable.

9. Reducing Shoulder-surfing by Using Gaze-based Password Entry: Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd

Shoulder-surfing – using direct observation techniques, such as looking over someone's shoulder, to get passwords, PINs and other sensitive personal information – is a problem that has been difficult to overcome. When a user

enters information using a keyboard, mouse, touch screen or any traditional input device, a malicious observer may be able to acquire the user's password credentials. The present Eye Password, a system that mitigates the issues of shoulder surfing via a novel approach to user input. With Eye Password, a user enters sensitive input (password, PIN, etc.) by selecting from an on-screen keyboard using only the orientation of their pupils (i.e. the position of their gaze on screen), making eavesdropping by a malicious observer largely impractical. The present a number of design choices and discuss their effect on usability and security. The conducted user studies to evaluate the speed, accuracy and user acceptance of our approach. The results demonstrate that gaze-based password entry requires marginal additional time over using a keyboard, error rates are similar to those of using a keyboard and subjects preferred the gaze-based password entry approach over traditional methods.

10. SkullConduct: Biometric User Identification on Eyewear Computers Using Bone Conduction Through the Skull: Stefan Schneegass, Youssef Oualil

Secure user identification is important for the increasing number of eyewear computers but limited input capabilities pose significant usability challenges for established knowledge based schemes, such as passwords or PINs. The present Skull- Conduct, a biometric system that uses bone conduction of sound through the user's skull as well as a microphone readily integrated into many of these devices, such as Google Glass. At the core of Skull Conduct is a

method to analyze the characteristic frequency response created by the user's skull using a combination of Mel Frequency Cepstral Coefficient (MFCC) features as well as a computationally light-weight 1NN classifier. The report on a controlled experiment with 10 participants that shows that this frequency response is person specific and stable – even when taking off and putting on the device multiple times – and thus serves as a robust biometric.

The show that our method can identify users with 97.0% accuracy and authenticate them with an equal error rate of 6.9%, thereby bringing biometric user identification to eyewear computers equipped with bone conduction technology.

CHAPTER 3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

The existing ATM Simulation System was built for the original concept of regional private banks. Small banks in villages and towns will service the needs of the local community and will only require ledgers to record account details. This system is prone to human error and causes undue frustration to users. This system was augmented with the introduction of excel sheets and emails. Banks could now record all information in an excel sheet and then set an update schedule when they will mail all records to a central hub where these records will again be processed and consolidated to form a unified record of all account transactions. These systems did not enable easy access to money and were greatly prone to grievous errors.

3.2 LIMITATIONS

- The customer must use ATM to made transactions.
- Possible to share pin.
- Insecure transaction.
- Misbehaviour activities to the customer’s account.

3.3 PROPOSED SYSTEM

The proposed system aims to solve all this by constant updating of bank records. The Java based construction of the system will enable transactions at any bank or ATM to be registered within a matter of seconds. Security of these details is also a top priority in this system. This central hub will be accessed by an ATM for secure customer transactions. In our project we are going to place an extra button in ATM machines. When that button got pressed the control window will be telecasted to accountant cellular phone. Then the accountant can enter the pin and amount manually in his mobiles telecasted pop-up window. By this control system accountant can keep his pin number with him and he can vend the amount by his own control by the desired person.

CHAPTER 4

SYSTEM SPECIFICATION

4.1 HARDWARE REQUIREMENTS

CPU type : Intel Pentium 4

Clock speed : 3.0 GHz

Ram size : 512 MB

Hard disk capacity : 40 GB

Monitor type : 15 Inch color monitor

Keyboard type : internet keyboard

4.2 SOFTWARE REQUIREMENTS

Operating System : Windows OS

Language : PHP

4.3 ABOUT THE SOFTWARE

Embedded C

Introduction to Embedded C

Looking around, find ourselves to be surrounded by various types of embedded systems. Be it a digital camera or a mobile phone or a washing

machine, all of them has some kind of processor functioning inside it. Associated with each processor is the embedded software. If hardware forms the body of an embedded system, embedded processor acts as the brain, and embedded software forms its soul. It is the embedded software which primarily governs the functioning of embedded systems.

During infancy years of microprocessor based systems, programs were developed using assemblers and fused into the EPROMs. There used to be no mechanism to find what the program was doing. LEDs, switches, etc. were used to check correct execution of the program. Some ‘very fortunate’ developers had In-circuit Simulators (ICEs), but they were too costly and were not quite reliable as well.

As time progressed, use of microprocessor-specific assembly-only as the programming language reduced and embedded systems moved onto C as the **embedded programming language** of choice. C is the most widely used programming language for embedded processors/controllers. Assembly is also used but mainly to implement those portions of the code where very high timing accuracy, code size efficiency, etc. are prime requirements.

Initially C was developed by Kernighan and Ritchie to fit into the space of 8K and to write (portable) operating systems. Originally it was implemented on UNIX operating systems. As it was intended for operating systems development, it can manipulate memory addresses. Also, it allowed

programmers to write very compact codes. This has given it the reputation as the language of choice for hackers too.

As assembly language programs are specific to a processor, assembly language didn't offer portability across systems. To overcome this disadvantage, several high level languages, including C, came up. Some other languages like PLM, Modula-2, Pascal, etc. also came but couldn't find wide acceptance. Amongst those, C got wide acceptance for not only embedded systems, but also for desktop applications. Even though C might have lost its sheen as mainstream language for general purpose applications, it still is having a strong-hold in embedded programming. Due to the wide acceptance of **C in the embedded systems**, various kinds of support tools like compilers & cross-compilers, ICE, etc. came up and all this facilitated development of **embedded systems using C**.

Subsequent sections will discuss **what is Embedded C**, **features of C language**, similarities and **difference between C and embedded C**, and **features of embedded C programming**.

EMBEDDED SYSTEMS PROGRAMMING

Embedded systems programming is different from developing applications on a desktop computers. Key characteristics of an embedded system, when compared to PCs, are as follows:

Embedded devices have resource constraints(limited ROM, limited RAM, limited stack space, less processing power)

Components used in embedded system and PCs are different; embedded systems typically uses smaller, less power consuming components.

Embedded systems are more tied to the hardware.

Two salient **features of Embedded Programming** are code speed and code size. Code speed is governed by the processing power, timing constraints, whereas code size is governed by available program memory and use of programming language. Goal of embedded system programming is to get maximum features in minimum space and minimum time.

Embedded systems are programmed using different type of languages:

- Machine Code
- Low level language, i.e., assembly
- High level language like C, C++, Java, Ada, etc.
- Application level language like Visual Basic, scripts, Access, etc.

Assembly language maps mnemonic words with the binary machine codes that the processor uses to code the instructions. Assembly language seems to be an obvious choice for programming embedded devices. However, use of assembly language is restricted to developing efficient codes in terms of size and speed. Also, assembly codes lead to higher software development costs and code portability is not there. Developing small codes are not much of a problem, but large programs/projects become increasingly difficult to manage in assembly language. Finding good assembly programmers has also become difficult

nowadays. Hence high level languages are preferred for embedded systems programming.

Use of **C in embedded systems** is driven by following advantages

- It is small and reasonably simpler to learn, understand, program and debug.
- C Compilers are available for almost all embedded devices in use today, and there is a large pool of experienced C programmers.
- Unlike assembly, C has advantage of processor-independence and is not specific to any particular microprocessor/ microcontroller or any system. This makes it convenient for a user to develop programs that can run on most of the systems.
- As C combines functionality of assembly language and features of high level languages, C is treated as a ‘middle-level computer language’ or ‘high level assembly language’
- It is fairly efficient
- It supports access to I/O and provides ease of management of large embedded projects.
- Many of these advantages are offered by other languages also, but what sets C apart from others like Pascal, FORTRAN, etc. is the fact that it is a middle level language; it provides direct hardware control without sacrificing benefits of high level languages.

Compared to other high level languages, C offers more flexibility because C is relatively small, structured language; it supports low-level bit-wise data manipulation.

Compared to assembly language, C Code written is more reliable and scalable, more portable between different platforms (with some changes). Moreover, programs developed in C are much easier to understand, maintain and debug. Also, as they can be developed more quickly, codes written in C offers better productivity. C is based on the philosophy 'programmers know what they are doing'; only the intentions are to be stated explicitly. It is easier to write good code in C & convert it to an efficient assembly code (using high quality compilers) rather than writing an efficient code in assembly itself. Benefits of assembly language programming over C are negligible when we compare the ease with which C programs are developed by programmers.

Objected oriented language, C++ is not apt for developing efficient programs in resource constrained environments like embedded devices. Virtual functions & exception handling of C++ are some specific features that are not efficient in terms of space and speed in embedded systems. Sometimes C++ is used only with very few features, very much as C.

Ada, also an object-oriented language, is different than C++. Originally designed by the U.S. DOD, it didn't gain popularity despite being accepted as an international standard twice (Ada83 and Ada95). However, Ada language has many features that would simplify embedded software development.

Java is another language used for embedded systems programming. It primarily finds usage in high-end mobile phones as it offers portability across systems and is also useful for browsing applications. Java programs require Java Virtual Machine (JVM), which consume lot of resources. Hence it is not used for smaller embedded devices.

Dynamic C and B# are some proprietary languages which are also being used in embedded applications.

Efficient embedded C programs must be kept small and efficient; they must be optimized for code speed and code size. Good understanding of processor architecture embedded C programming and debugging tools facilitate this.

Difference between C and embedded C:

Though **C and embedded C** appear different and are used in different contexts, they have more similarities than the differences. Most of the constructs are same; the difference lies in their applications.

C is used for desktop computers, while **embedded C** is for microcontroller based applications. Accordingly, C has the luxury to use resources of a desktop PC like memory, OS, etc. While programming on desktop systems, we need not bother about memory. However, embedded C has to use with the limited resources (RAM, ROM, IOs) on an embedded processor. Thus, program code must fit into the available program memory. If code exceeds the limit, the system is likely to crash.

Compilers for C (ANSI C) typically generate OS dependant executables. **Embedded C** requires compilers to create files to be downloaded to the microcontrollers/microprocessors where it needs to run. Embedded compilers give access to all resources which is not provided in compilers for desktop computer applications.

Embedded systems often have the real-time constraints, which is usually not there with desktop computer applications.

Embedded systems often do not have a console, which is available in case of desktop applications.

So, what basically is different while programming with **embedded C** is the mindset; for embedded applications, we need to optimally use the resources, make the program code efficient, and satisfy real time constraints, if any. All this is done using the basic constructs, syntaxes, and function libraries of 'C'.

CHAPTER 5

SYSTEM DESIGN

5.1 SYSTEM ARCHITECTURE

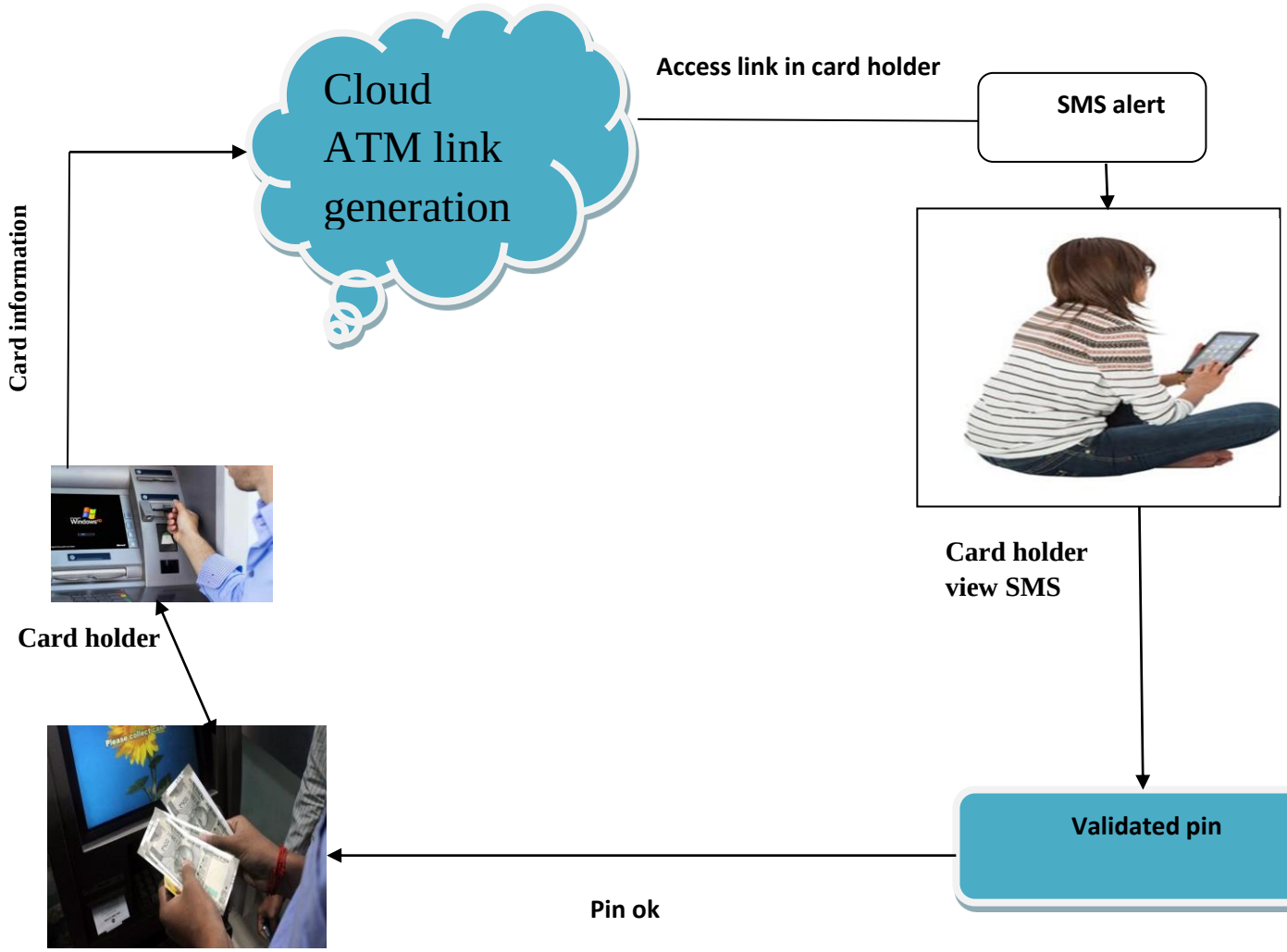

Fig 5.1

5.2 BLOCK DIAGRAM

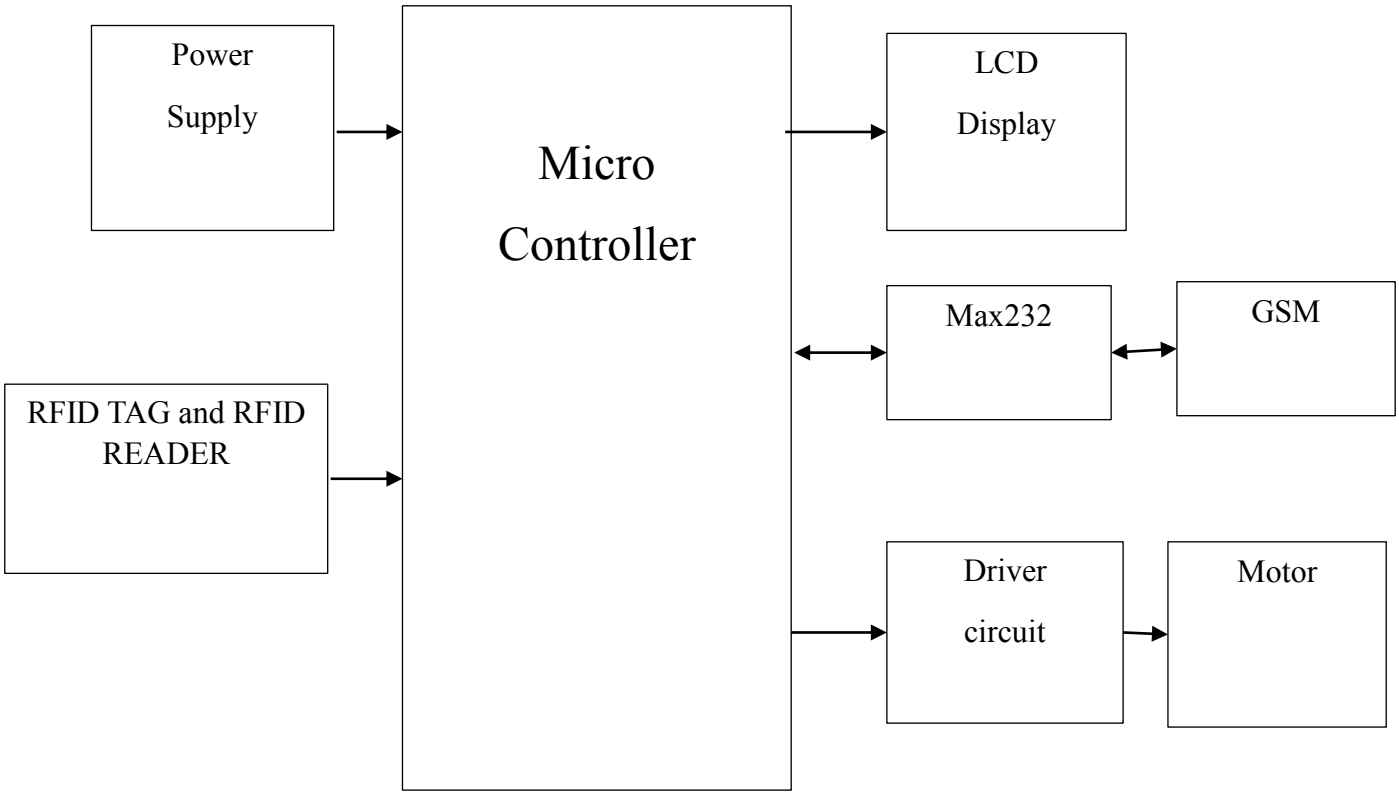

Fig 5.2

5.3 HARDWARE COMPONENTS:

- ATM module
- Buttons
- Micro Controller- Arduino UNO
- Web API
- Motors
- Mobile Phones / Personal Computer
- Wi-Fi Module –ESP8266/Node MCU E12
- LCD Display

5.3.1 ARDUINO MICROCONTROLLER

Arduino is a tool for making computers that can sense and control more of the physical world than your desktop computer. It's an open-source physical computing platform based on a simple microcontroller board, and a development environment for writing software for the board.

Arduino can be used to develop interactive objects, taking inputs from a variety of switches or sensors, and controlling a variety of lights, motors, and other physical outputs. Arduino projects can be stand-alone, or they can be communicate with software running on your computer (e.g. Flash, Processing, MaxMSP.) The boards can be assembled by hand or purchased preassembled; the open-source IDE can be downloaded for free.

The Arduino programming language is an implementation of Wiring, a similar physical computing platform, which is based on the Processing multimedia programming environment.

There are many other microcontrollers and microcontroller platforms available for physical computing. Parallax Basic Stamp, Netmedia's BX-24, Phidgets, MIT's Handyboard, and many others offer similar functionality. All of these tools take the messy details of microcontroller programming and wrap it up in an easy-to-use package. Arduino also simplifies the process of working with microcontrollers, but it offers some advantage for teachers, students, and interested amateurs over other systems:

- Inexpensive - Arduino boards are relatively inexpensive compared to other microcontroller platforms. The least expensive version of the Arduino module can be assembled by hand, and even the pre-assembled Arduino modules cost less than $50
- Cross-platform - The Arduino software runs on Windows, Macintosh OSX, and Linux operating systems. Most microcontroller systems are limited to Windows.
- Simple, clear programming environment - The Arduino programming environment is easy-to-use for beginners, yet flexible enough for advanced users to take advantage of as well. For teachers, it's conveniently based on the Processing programming environment, so students learning to program in that environment will be familiar with the look and feel of Arduino
- Open source and extensible software- The Arduino software is published as open source tools, available for extension by experienced programmers. The language can be expanded through C++ libraries, and people wanting to understand the technical details can make the leap from Arduino to the AVR C programming language on which it's based. Similarly, you can add AVR-C code directly into your Arduino programs if you want to.
- Open source and extensible hardware - The Arduino is based on Atmel's ATMEGA8 and ATMEGA168microcontrollers. The plans for the modules are published under a Creative Commons license, so experienced circuit designers can make their own version of the module, extending it and

improving it. Even relatively inexperienced users can build the breadboard version of the module in order to understand how it works and save money.

The Arduino microcontroller is an easy to use yet powerful single board computer that has gained considerable traction in the hobby and professional market. The Arduino is open-source, which means hardware is reasonably priced and development software is free. This guide is for students in ME 2011, or students anywhere who are confronting the Arduino for the first time. For advanced Arduino users, prowl the web; there are lots of resources. The Arduino project was started in Italy to develop low cost hardware for interaction design.

Fig 5.3.1. 1

With the Arduino board, you can write programs and create interface circuits to read switches and other sensors, and to control motors and lights with very little effort.

Many of the pictures and drawings in this guide were taken from the documentation on the Arduino site, the place to turn if you need more information. The Duemilanove board features an Atmel ATmega328 microcontroller operating at 5 V with 2Kb of RAM, 32 Kb of flash memory for storing programs and 1 Kb of EEPROM for storing parameters. The clock speed is 16 MHz, which translates to about executing about 300,000 lines of C source code per second. The board has 14 digital I/O pins and 6 analog input pins. There is a USB connector for talking to the host computer and a DC power jack for connecting an external 6-20 V power source, for example a 9 V battery, when running a program while not connected to the host computer. Headers are provided for interfacing to the I/O pins using 22 g solid wire or header connectors. The Arduino programming language is a simplified version of C/C++. If you know C, programming the Arduino will be familiar. If you do not know C, no need to worry as only a few commands are needed to perform useful functions. An important feature of the Arduino is that you can create a control program on the host PC, download it to the Arduino and it will run automatically. Remove the USB cable connection to the PC, and the program will still run from the top each time you push the reset button. Remove The battery and put the Arduino board in a closet for six months. When you reconnect the battery, the last program you stored will run. This means that you connect the board to the host PC to envelop and debug your program, but once that is done, you no longer need the PC to run the program.

1.1 What You Need for a Working System

1. Arduino Duemilanove board

2. USB programming cable (A to B)

3. 9V battery or external power supply (for stand-alone operation)

4. Solderless breadboard for external circuits, and 22 g solid wire for connections

5. Host PC running the Arduino development environment. Versions exist for Windows, Mac and Linux

5.3.2 Power supply

The ac voltage, typically 220V rms, is connected to a transformer, which steps that ac voltage down to the level of the desired dc output. A diode rectifier then provides a full-wave rectified voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting dc voltage usually has some ripple or ac voltage variation.

A regulator circuit removes the ripples and also remains the same dc value even if the input dc voltage varies, or the load connected to the output dc voltage changes. This voltage regulation is usually obtained using one of the popular voltage regulator IC units.

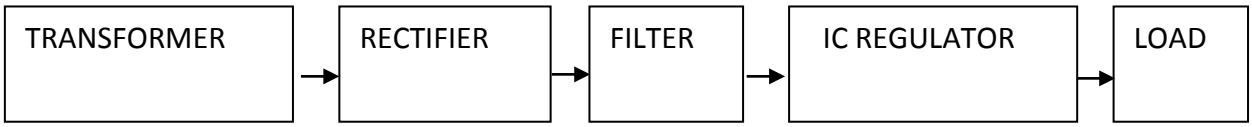

Fig 5.3.2.1 Power supply

5.3.3 Transformer

The potential transformer will step down the power supply voltage (0-230V) to (0-6V) level. Then the secondary of the potential transformer will be connected to the precision rectifier, which is constructed with the help of op–amp. The advantages of using precision rectifier are it will give peak voltage output as DC, rest of the circuits will give only RMS output.

5.3.4 Bridge rectifier

When four diodes are connected as shown in figure, the circuit is called as bridge rectifier. The input to the circuit is applied to the diagonally opposite corners of the network, and the output is taken from the remaining two corners.

Let us assume that the transformer is working properly and there is a positive potential, at point A and a negative potential at point B. the positive potential at point A will forward bias D3 and reverse bias D4.

The negative potential at point B will forward bias D1 and reverse D2. At this time D3 and D1 are forward biased and will allow current flow to pass through them; D4 and D2 are reverse biased and will block current flow.

The path for current flow is from point B through D1, up through RL, through D3, through the secondary of the transformer back to point B. this path is indicated by the solid arrows. Waveforms (1) and (2) can be observed across D1 and D3.

One-half cycle later the polarity across the secondary of the transformer reverse, forward biasing D2 and D4 and reverse biasing D1 and D3. Current flow will now be from point A through D4, up through RL, through D2, through the secondary of T1, and back to point A. This path is indicated by the broken arrows. Waveforms (3) and (4) can be observed across D2 and D4. The current flow through RL is always in the same direction. In flowing through RL this current develops a voltage corresponding to that shown waveform (5). Since current flows through the load (RL) during both half cycles of the applied voltage, this bridge rectifier is a full-wave rectifier.

One advantage of a bridge rectifier over a conventional full-wave rectifier is that with a given transformer the bridge rectifier produces a voltage output that is nearly twice that of the conventional full-wave circuit.

This may be shown by assigning values to some of the components shown in views A and B. assume that the same transformer is used in both circuits. The peak voltage developed between points X and y is 1000 volts in both circuits. In the conventional full-wave circuit shown—in view A, the peak voltage from the center tap to either X or Y is 500 volts. Since only one diode

can conduct at any instant, the maximum voltage that can be rectified at any instant is 500 volts.

The maximum voltage that appears across the load resistor is nearly-but never exceeds-500 v0lts, as result of the small voltage drop across the diode. In the bridge rectifier shown in view B, the maximum voltage that can be rectified is the full secondary voltage, which is 1000 volts. Therefore, the peak output voltage across the load resistor is nearly 1000 volts. With both circuits using the same transformer, the bridge rectifier circuit produces a higher output voltage than the conventional full-wave rectifier circuit.

5.3.5 IC voltage regulators

Voltage regulators comprise a class of widely used ICs. Regulator IC units contain the circuitry for reference source, comparator amplifier, control device, and overload protection all in a single IC. IC units provide regulation of either a fixed positive voltage, a fixed negative voltage, or an adjustably set voltage. The regulators can be selected for operation with load currents from hundreds of milli amperes to tens of amperes, corresponding to power ratings from milli watts to tens of watts.

5.3.6 RELAY

A relay is an electrically operated switch. Many relays use an electromagnet to operate a switching mechanism mechanically, but other operating principles are also used. Relays are used where it is necessary to

control a circuit by a low-power signal (with complete electrical isolation between control and controlled circuits), or where several circuits must be controlled by one signal. The first relays were used in long distance telegraph circuits, repeating the signal coming in from one circuit and re-transmitting it to another. Relays were used extensively in telephone exchanges and early computers to perform logical operations.

A type of relay that can handle the high power required to directly control an electric motor or other loads is called a contactor. Solid-state relays control power circuits with no moving parts, instead using a semiconductor device to perform switching. Relays with calibrated operating characteristics and sometimes multiple operating coils are used to protect electrical circuits from overload or faults; in modern electric power systems these functions are performed by digital instruments still called "protective relays".

5.3.7 BASIC DESIGN AND OPERATION:

A simple electromagnetic relay consists of a coil of wire wrapped around a soft iron core, an iron yoke which provides a low reluctance path for magnetic flux, a movable iron armature, and one or more sets of contacts (there are two in the relay pictured). The armature is hinged to the yoke and mechanically linked to one or more sets of moving contacts. It is held in place by a spring so that when the relay is de-energized there is an air gap in the magnetic circuit. In this

condition, one of the two sets of contacts in the relay pictured is closed, and the other set is open. Other relays may have more or fewer sets of contacts depending on their function. The relay in the picture also has a wire connecting the armature to the yoke. This ensures continuity of the circuit between the moving contacts on the armature, and the circuit track on the printed circuit board (PCB) via the yoke, which is soldered to the PCB.

When an electric current is passed through the coil it generates a magnetic field that activates the armature, and the consequent movement of the movable contact(s) either makes or breaks (depending upon construction) a connection with a fixed contact. If the set of contacts was closed when the relay was de-energized, then the movement opens the contacts and breaks the connection, and vice versa if the contacts were open. When the current to the coil is switched off, the armature is returned by a force, approximately half as strong as the magnetic force, to its relaxed position. Usually this force is provided by a spring, but gravity is also used commonly in industrial motor starters. Most relays are manufactured to operate quickly. In a low-voltage application this reduces noise; in a high voltage or current application it reduces arcing.

When the coil is energized with direct current, a diode is often placed across the coil to dissipate the energy from the collapsing magnetic field at deactivation, which would otherwise generate a voltage spike dangerous to

semiconductor circuit components. Some automotive relays include a diode inside the relay case. Alternatively, a contact protection network consisting of a capacitor and resistor in series (snubber circuit) may absorb the surge. If the coil is designed to be energized with alternating current (AC), a small copper "shading ring" can be crimped to the end of the solenoid, creating a small out-of-phase current which increases the minimum pull on the armature during the AC cycle.

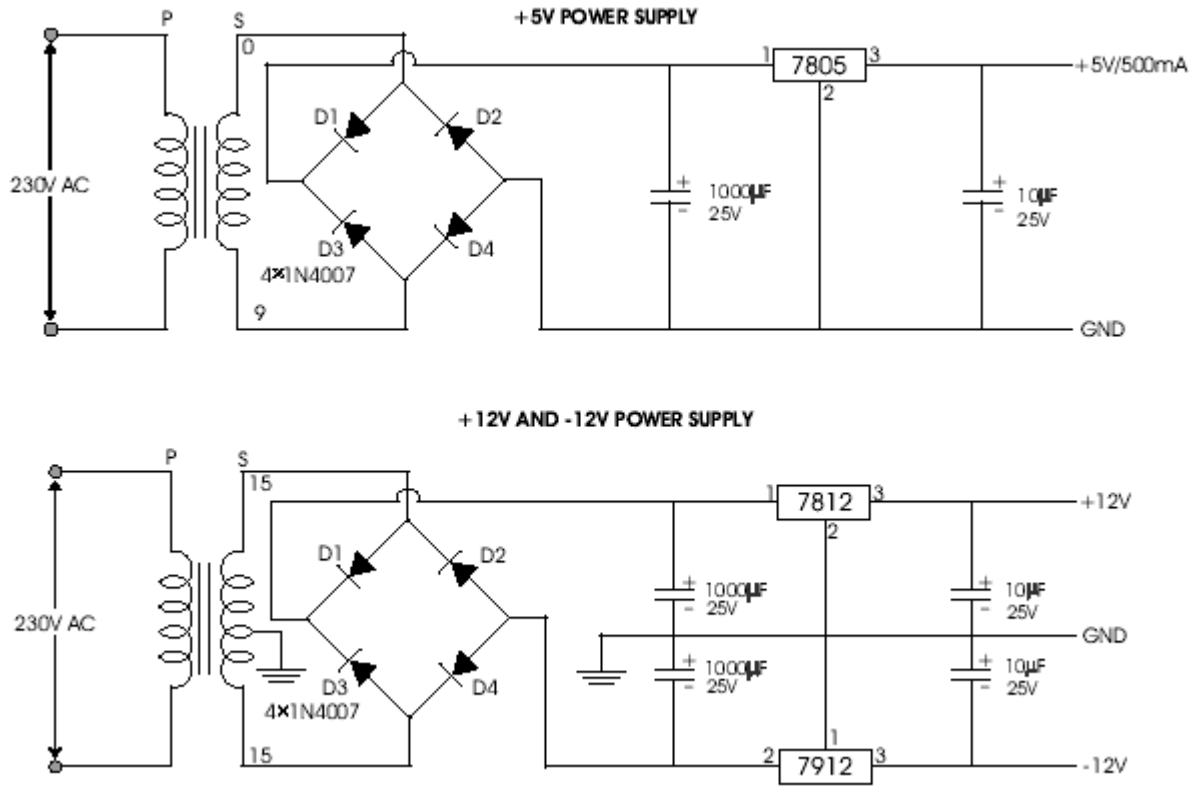

Fig 5.3.7.1 Circuit diagram (Power supply)

A fixed three-terminal voltage regulator has an unregulated dc input voltage, Vi, applied to one input terminal, a regulated dc output voltage, Vo, from a second terminal, with the third terminal connected to ground.

The series 78 regulators provide fixed positive regulated voltages from 5 to 24 volts. Similarly, the series 79 regulators provide fixed negative regulated voltages from 5 to 24 volts.

- For ICs, microcontroller, LCD --------- 5 volts
- For alarm circuit, op-amp, relay circuits ---------- 12 volts

5.3.8 LCD

A **liquid crystal display** (**LCD**) is a flat panel display, electronic visual display, or video display that uses the light modulating properties of liquid crystals. Liquid crystals do not emit light directly. LCDs are available to display arbitrary images (as in a general-purpose computer display) or fixed images which can be displayed or hidden, such as preset words, digits, and 7-segment displays as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements. LCDs are used in a wide range of applications including computer monitors, televisions, instrument panels, aircraft cockpit displays, and signage. They are common in consumer devices such as video players, gaming devices, clocks, watches, calculators, and telephones, and have replaced cathode ray tube (CRT) displays in most

applications. They are available in a wider range of screen sizes than CRT and plasma displays, and since they do not use phosphors, they do not suffer image burn-in. LCDs are, however, susceptible to image persistence.

The LCD screen is more energy efficient and can be disposed of more safely than a CRT. Its low electrical power consumption enables it to be used in battery-powered electronic equipment. It is an electronically modulated optical device made up of any number of segments filled with liquid crystals and arrayed in front of a light source (backlight) or reflector to produce images in color or monochrome. Liquid crystals were first discovered in 1888. By 2008, worldwide sales of televisions with LCD screens exceeded annual sales of CRT units; the CRT became obsolete for most purposes.

SPECIFICATION:

Important factors to consider when evaluating an LCD:

- **Resolution versus range:**

  Fundamentally resolution is the granularity (or number of levels) with which a performance feature of the display is divided. Resolution is often confused with range or the total end-to-end output of the display. Each of the major features of a display has both a resolution and a range that are tied to each other but very different. Frequently the range is an inherent limitation

of the display while the resolution is a function of the electronics that make the display work.

- **Spatial performance:**

LCDs come in only one size for a variety of applications and a variety of resolutions within each of those applications. LCD spatial performance is also sometimes described in terms of a "dot pitch". The size (or spatial range) of an LCD is always described in terms of the diagonal distance from one corner to its opposite. This is an historical remnant from the early days of CRT television when CRT screens were manufactured on the bottoms of glass bottles, a direct extension of cathode ray tubes used in oscilloscopes. The diameter of the bottle determined the size of the screen. Later, when televisions went to a more square format, the square screens were measured diagonally to compare with the older round screens.

Temporal/timing performance:

Contrary to spatial performance, temporal performance is a feature where smaller is better. Specifically, the range is the pixel response time of an LCD, or how quickly a sub-pixel's brightness changes from one level to another. For LCD monitors, this is measured in btb (black to black) or gtg (gray to gray). These different types of measurements make comparison difficult Further, this number is almost never published in sales advertising.

Color performance:

There are many terms to describe color performance of an LCD. They include color gamut which is the range of colors that can be displayed and color depth which is the color resolution or the resolution or fineness with which the color range is divided. Although color gamut can be expressed as three pairs of numbers, the XY coordinates within color space of the reddest red, greenest green, and bluest blue, it is usually expressed as a ratio of the total area within color space that a display can show relative to some standard such as saying that a display was "120% of NTSC". NTSC is the National Television Standards Committee, the old standard definition TV specification. Color gamut is a relatively straight forward feature. However with clever optical techniques that are based on the way humans see color, termed **color stretch**, colors can be shown that are outside of the nominal range of the display. In any case, color range is rarely discussed as a feature of the display as LCDs are designed to match the color ranges of the content that they are intended to show. Having a color range that exceeds the content is a useless feature

Brightness and contrast ratio:

Contrast ratio is the ratio of the brightness of a full-on pixel to a full-off pixel and, as such, would be directly tied to brightness if not for the invention of the blinking backlight (or burst dimming). The LCD itself is only a light valve, it does not generate light; the light comes from a backlight that is either a

fluorescent tube or a set of LEDs. The blinking backlight was developed to improve the motion performance of LCDs by turning the backlight off while the liquid crystals were in transition from one image to another. However, a side benefit of the blinking backlight was infinite contrast. The contrast reported on most LCDs is what the LCD is qualified at, not its actual performance. In any case, there are two large caveats to contrast ratio as a measure of LCD performance.

Color depth or **color support**

It is sometimes expressed in bits, either as the number of bits per sub-pixel or the number of bits per pixel. This can be ambiguous as an 8-bit color LCD can be 8 total bits spread between red, green, and blue or 8 bits each for each color in a different display. Further, LCDs sometimes use a technique called dithering which is time averaging colors to get intermediate colors such as alternating between two different colors to get a color in between. This doubles the number of colors that can be displayed; however, this is done at the expense of the temporal performance of the display. Dithering is commonly used on computer displays where the images are mostly static and the temporal performance is unimportant.

When color depth is reported as color support, it is usually stated in terms of number of colors the LCD can show. The number of colors is the translation from the base 2-bit numbers into common base-10. For example, 8-bit color is 2

to the 8th power, which is 256 colors. 24-bit color is 2 to the 24th power, or 256 x 256 x 256, a total of 16,777,216 colors. The color resolution of the human eye depends on both the range of colors being sliced and the number of slices; but for most common displays the limit is about 28-bit color LCD TVs commonly display more than that as the digital processing can introduce color distortions and the additional levels of color are needed to ensure true color

5.3.9 GSM

GSM TECHNOLOGY

GSM refers to second-generation wireless telecommunications standard for digital cellular services. First deployed in Europe, it is based on TDMA (Time Division Multiple Access) technology. GSM uses three frequency bands: 900 MHz, 1800 MHz and 1900 MHz. Dual-band phones operate on two out of three of these frequencies, while tri-band phones operate on all three frequencies.

GSM (**Global System for Mobile Communications**, originally **Groupe Spécial Mobile**),

It is a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones. The GSM standard was developed as a replacement for first generation (1G) analog cellular networks,

and originally described a digital, circuit switched network optimized for full duplex voice telephony.

This was expanded over time to include data communications, first by circuit switched transport, then packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution or EGPRS).Further improvements were made when the 3GPP developed third generation (3G) UMTS standards followed by fourth generation (4G) LTE Advanced standards."GSM" is a trademark owned by the GSM Association.

Mobile Station:

The mobile station (MS) consists of the physical equipment, such as the radio transceiver, display and digital signal processors, and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to all subscribed services irrespective of both the location of the terminal and the use of a specific terminal. By inserting the SIM card into another GSM cellular phone, the user is able to receive calls at that phone, make calls from that phone, or receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI), identifying the subscriber, a secret key for authentication, and other user information. The IMEI and the IMSI are

independent, thereby providing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

Base Station Subsystem

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the specified bus interface, allowing (as in the rest of the system) operation between components made by different suppliers.

The Base Transceiver Station houses the radio transceivers that define a cell and handles the radio protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTSs deployed. The requirements for a BTS are ruggedness, reliability, portability, and minimum cost.

The Base Station Controller manages the radio resources for one or more BTSs. It handles radio channel setup, frequency hopping, and handovers, as described below. The BSC is the connection between the mobile and the Mobile service Switching Center (MSC). The BSC also translates the 13 kbps voice channel used over the radio link to the standard 64 kbps channel used by the Public Switched Telephone Network or ISDN.

Network Subsystem

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and in addition provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjuction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the public fixed network (PSTN or ISDN), and signalling between functional entities uses the ITU Signalling System Number 7 (SS7), used in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call routing and (possibly international) roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The current location of the mobile is in the form of a Mobile Station Roaming Number (MSRN) which is a regular ISDN number used to route a call to the MSC where the mobile is currently located. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The Visitor Location Register contains selected administrative information from the HLR, necessary for call control and provision of the

subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, most manufacturers of switching equipment implement one VLR together with one MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, simplifying the signalling required. Note that the MSC contains no information about particular mobile stations - this information is stored in the location registers.

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel.

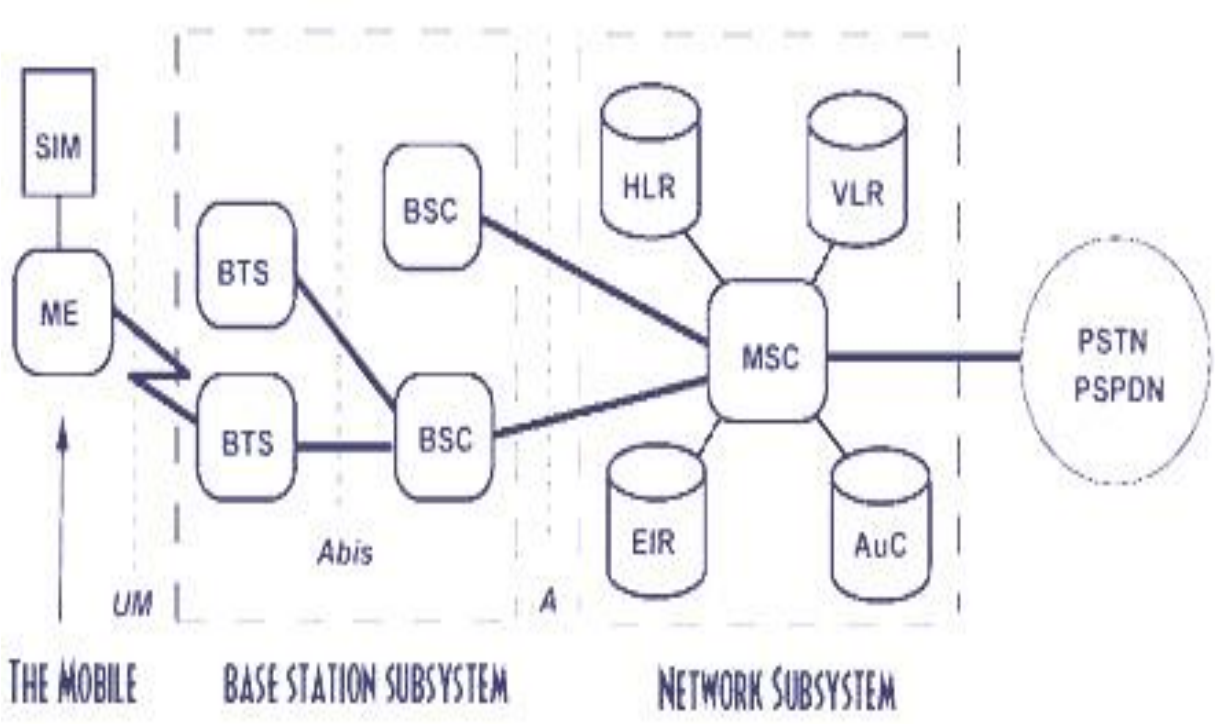

Fig 5.3.9.1

SIM Subscriber Identity Module

MS Mobile Station

BTS Base Transceiver Station

BSC Base Station Controller

MSC Mobile services Switching Center

VLR Visitor Location Register

HLR Home Location Register

VLR Visitor Location Register

EIR Equipment Identity Register

AC Authentication Center

PSTN Public Switched Telecomm Network

ISDN Integrated Services Digital Network

The Advantages of GSM:

GSM networks enjoy wide international coverage. The use of a SIM (Subscriber Identity Module) card makes it easy to switch between different handsets and allows for the quick and easy import of data such as contacts and text-messages.the amount of battery-supported ‘talk-time’ is generally higher on GSM phones.

CDMA technology

CDMA (Code Division Multiple Access) digital wireless technology employs a special coding scheme (whereby each transmitter is assigned a code), which allows multiple users to share common access to the network. Using ‘spread spectrum’ technology, a signal is spread across a broad spectrum of radio frequencies, allowing for a signal with wider bandwidth and increased resistance to interference.

The Advantages of CDMA

CDMA provides wider coverage than GSM and allows for a larger cell area. CDMA-enabled calls can be placed in low signal strength conditions, thus CDMA phones offer better reception/coverage in rural areas.

3G technology

Third generation (3G) technology is the newest and most innovative technology available today. 3G mobile-phones and networks offer high data

rates, wide bandwidth and increased capacity, all of which are required to support the new range of mobile-phone services. These include: internet access, multimedia applications, global roaming and access to such services as: sports news, the latest films, video messages, and online gaming.

Wireless technology features

When choosing a wireless service or device to use, you are advised to consider your requirement for the following features:

Optimum coverage

Both CDMA and GSM networks provide extensive metropolitan coverage.

'Roaming'

All the GSM networks in Kenya allow for 'roaming' (using the phone to 'roam' within different national networks) within East Africa. Not all mobile-phones purchased outside Kenya will work on the local GSM networks. CDMA phones have not been enabled to 'roam' in East Africa due to the fact that the necessary network agreements do not, as yet, exist.

5.3.10 MAX 232

The **MAX232** is an integrated circuit, first created by Maxim Integrated Products, that converts signals from an RS-232 serial port to signals suitable for

use in TTL compatible digital logic circuits. The MAX232 is a dual driver/receiver and typically converts the RX, TX, CTS and RTS signals.

The drivers provide RS-232 voltage level outputs (approx. ± 7.5 V) from a single + 5 V supply via on-chip charge pumps and external capacitors. This makes it useful for implementing RS-232 in devices that otherwise do not need any voltages outside the 0 V to + 5 V range, as power supplydesign does not need to be made more complicated just for driving the RS-232 in this case.

The receivers reduce RS-232 inputs (which may be as high as ± 25 V), to standard 5 V TTL levels. These receivers have a typical threshold of 1.3 V, and a typical hysteresis of 0.5 V.

The later MAX232A is backwards compatible with the original MAX232 but may operate at higher baud rates and can use smaller external capacitors – 0.1 μF in place of the 1.0 μF capacitors used with the original device.[1]

The newer MAX3232 is also backwards compatible, but operates at a broader voltage range, from 3 to 5.5 V

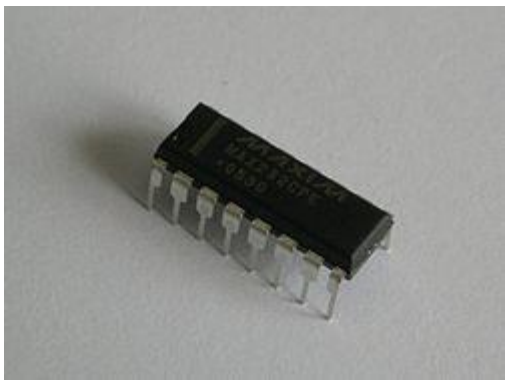

Fig 5.3.10.1

MAX232 CIRCUIT

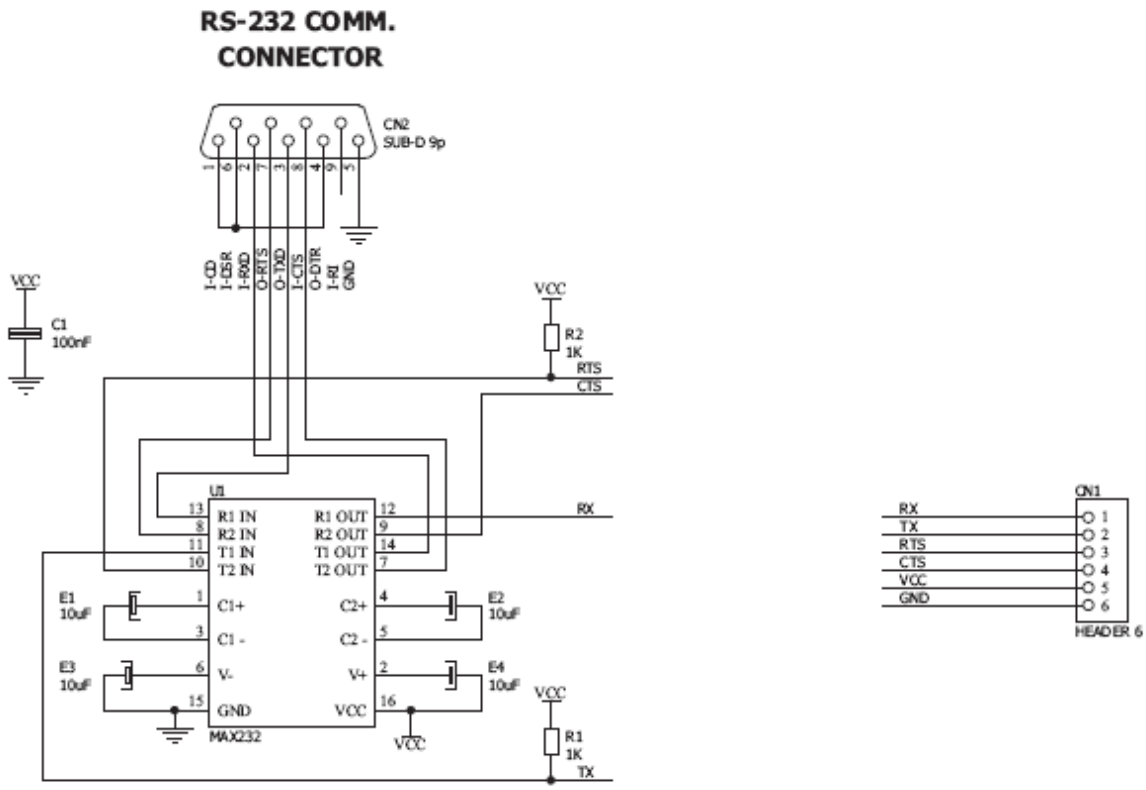

Fig 5.3.10.2

VOLTAGE LEVEL

It is helpful to understand what occurs to the voltage levels. When a MAX232 IC receives a TTL level to convert, it changes a TTL Logic 0 to between +3 and +15 V, and changes TTL Logic 1 to between -3 to -15 V, and vice versa for converting from RS232 to TTL. This can be confusing when you realize that the RS232 Data Transmission voltages at a certain logic state are opposite from the RS232 Control Line voltages at the same logic state. To

clarify the matter, see the table below. For more information see RS-232 Voltage Levels.

RS232 Line Type & Logic Level	**RS232 Voltage**	**TTL Voltage to/from MAX232**
Data Transmission (Rx/Tx) Logic 0	+3 V to +15 V	0 V
Data Transmission (Rx/Tx) Logic 1	-3 V to -15 V	5 V
Control Signals (RTS/CTS/DTR/DSR) Logic 0	-3 V to -15 V	5 V
Control Signals (RTS/CTS/DTR/DSR) Logic 1	+3 V to +15 V	0 V

CHAPTER 6

SCREENSHOTS

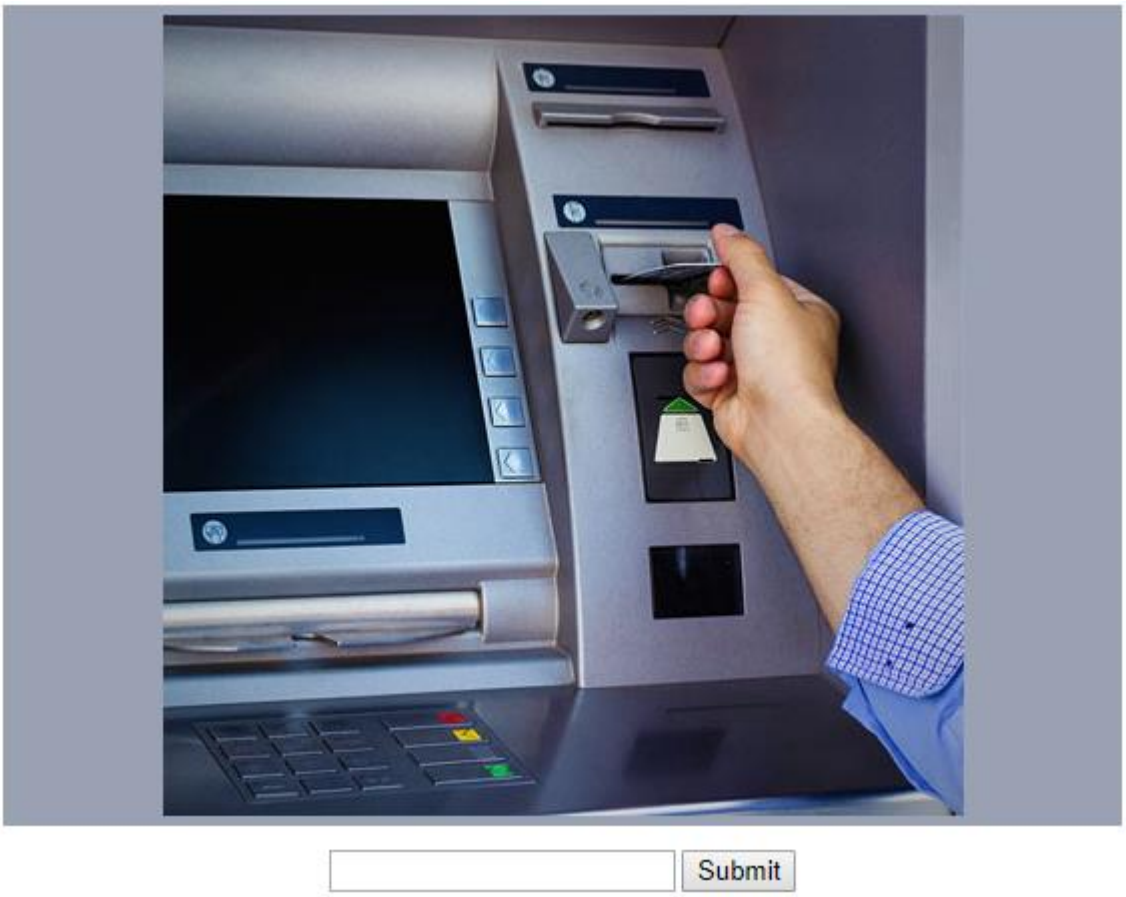

Fig 6.1 Insert ATM Card

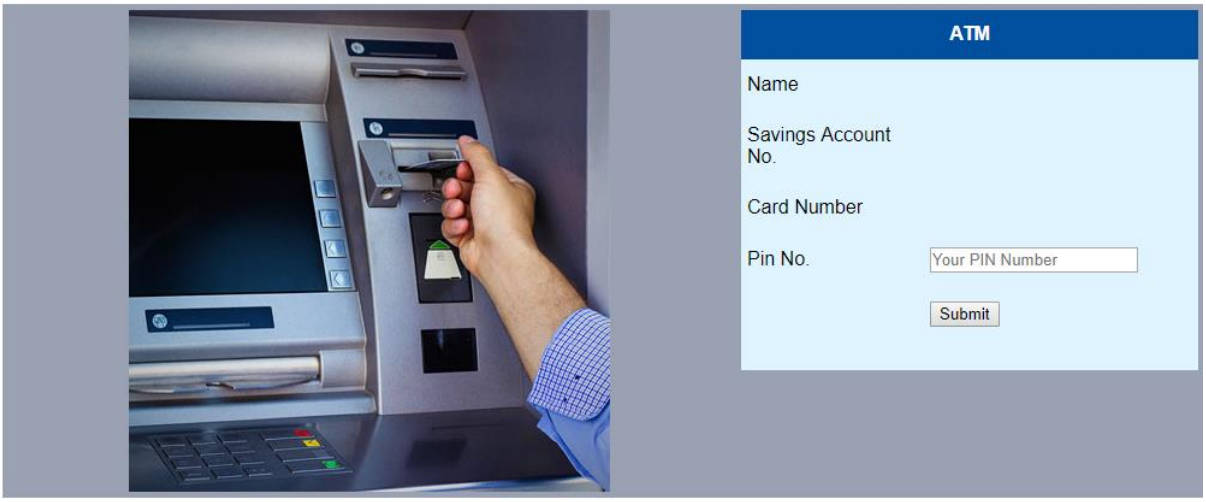

Fig 6.2 Enter PIN Number

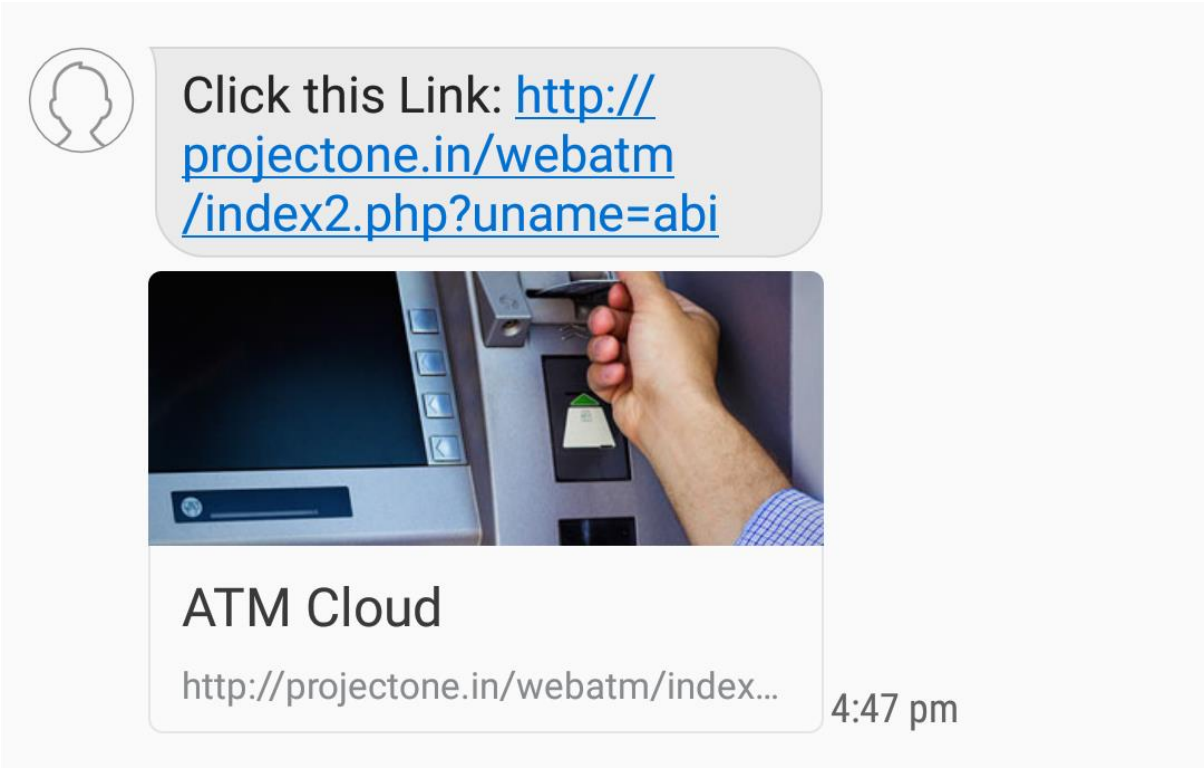

Fig 6.3 Send the LINK For Account Holder

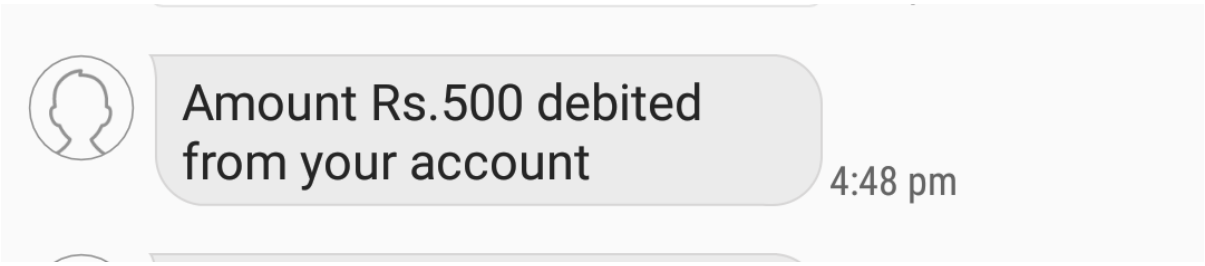

Fig 6.4 Send the Debited SMS for Account Holder

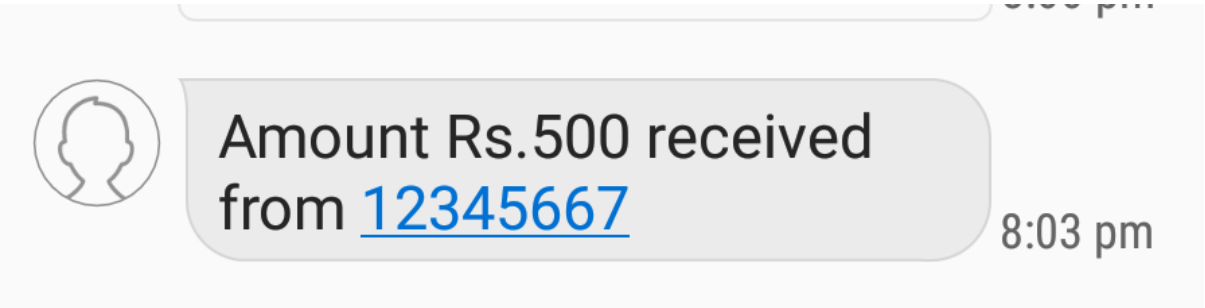

Fig 6.5 Send the Received SMS for Account Holder

CHAPTER 7

CONCLUSION AND FUTURE WORKS

7.1 CONCLUSION

This whole implementation ensures us a secured and authenticated transaction through RFID and GSM technique with lowest cost and minimum maintenance. Mankind will utilize new and secured type of money transactions. The only thing is that initial cost of RFID conversion of the entire system is the required one time investment. The value added service that this system provides increases the credibility of the financial institutions, the banks improves the convenience to its customer. Hence as the world progresses through the inevitable and an indomitable quest for knowledge, the aspect of security bound systems are bound to concede with the growing innovations and obviously more vulnerabilities. Hence our application might well solve the aspect of transaction security to a precise and great extent.

7.2 FUTURE WORKS

- It leads to help the physically disabled peoples for their transactions through ATM machines.
- Assist secure banking for all kind of users.
- User can access ATM banking without disclosing their PIN number to anyone. Promote remote systems for current ATM Environment .

APPENDIX

SOURCE CODE

Index.php

```
<?php

session_start();

include("dbconnect.php");

extract($_REQUEST);

$msg="";

/*if(isset($btn))

{

include "php_serial.class.php";

$serial = new phpSerial;

$serial->deviceSet("COM8");

$serial->deviceOpen();

$serial->sendMessage("B");

$read = $serial->readPort();

$serial->deviceClose();
```

```
$serial->confBaudRate(9600);

$un=$read;

$q1=mysql_query("select * from atm_user where uname='$un'");

$n1=mysql_num_rows($q1);

        if($n1==1)

        {

        $r1=mysql_fetch_array($q1);

        $mob=$r1['mobile'];

        header("location:index.php?act=ok&user=$un&mobile=$mob");

        }

        else

        {

        header("location:index.php?act=no");

        }

}*/

if(isset($btn))

{
```

```
$qry=mysql_query("select * from atm_user where card='".trim($card)."'");

$row=mysql_fetch_array($qry);

$mobile=$row['mobile'];

$data=$row['uname'];

$message="ClickthisLink:http://projectone.in/webatm/index2.php?uname=$dat
a";

/*if($card=="0003984108")//"0004118757){

$data="A";}

else if($card=="0004110597")//"0004158525"){

$data="B";}*/echo'<iframesrc="http://pay4sms.in/sendsms/?token=
b81edee36bcef4ddbaa6ef535f8db03e&credit=2&sender=RandDC&message='.$
message.'&number=91'.$mobile.'" style="display:block"></iframe>';?>

<script language="javascript">

alert("<?php echo $data." ".$card; ?> Input Accepted");</script>

<?php//$msg="Input Accepted";}?><!DOCTYPE html PUBLIC "-//W3C//DTD
XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title><?php include("title.php"); ?></title>
<link href="style.css" rel="stylesheet" type="text/css" />
</head><body>
<form id="form1" name="form1" method="post" action="">
  <div align="center" class="hd"><?php include("title.php"); ?></div>
  <div class="sd"><!--<a href="index.php">Home</a>-->
    <divalign="center"><ahref="index.php">Home</a>
<a href="login.php">Admin</a></div></div>
  <p> </p>
  <table width="42%" border="0" align="center" cellpadding="5"
cellspacing="0" bgcolor="#9AA1B3"> <tr>
 <th scope="col"><img src="images/feature.jpg" width="400"
height="400"/></th></tr>
 </table>  <p align="center"> <input type="text" name="card" />
```

<input type="submit" name="btn" value="Submit" />

  <?php include("title.php");
?>

</form>

</body>

</html>

REFERENCE

[1] G.Udaya Sree, M.Vinusha " Real Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM Terminal" ,*IJSETR, ISSN 2319-8885 Vol.02,Issue.12, September-2013, Pages:1223-1227.*

[2] Khatmode Ranjit P, Kulkarni Ramchandra V, "ARM7 Based Smart ATM Access & Security System Using Fingerprint Recognition & GSM Technology", *ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014***.**

.[3] M.R.Dineshkumar,M.S.Geethanjali,"Protected Cash Withdrawal in ATM Using Mobile Phone", *International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 4 April, 2013 Page No. 1346-1350.*

[4] Zaid Imran,Rafay Nizaami ,"Advance Secure Login", *International Journal For Science and Research Publications, Volume 1,Issue 1,December 2011.*

[5] M. Ajaykumar and N. Bharath Kumar," Anti-Theft ATM Machine Using Vibration Detection Sensor", *IJARCSSC Volume 3, Issue 12, December 2013 ISSN: 2277 128X.*

[6] SURAJ B S and Dr. R GIRISHA, " ARM7 based Smart ATM Access System", *International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 5.*

[7] K.annan K, “Microcontroller Based Secure Pin Entry Method For ATM”, *International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013 ISSN 2229-5518.*

[8] Hyung-Woo Lee,“Security in Wireless Sensor Networks: Issues and Challenges*”, ICACT, ISBN 89-5519-129-4, Feb. 20-22, 2006.*