A Project Report

On

“Implementation of Automated Teller Machine**”**

Submitted in partial fulfillment of the requirements for the award of degree of

Bachelor of Engineering in Electronics and Communication Engineering

Submitted By

**Abhijeet Shinde 2GI14EC001**

**Chetan Bedarekar 2GI14EC020**

**Chetan Walvekar 2GI14EC021**

**Nagpritam Naik 2GI14EC047**

Under the guidance of

**Prof. Roopa Kulkarni**



***Department of Electronics and Communication Engineering***

# Acknowledgements

It is a great pleasure to acknowledge all those who have contributed towards the conception, origin and nurturing of this project “Implementation of Automated Teller Machines (ATMs)”.

I would like to extend thanks to many people, who so generously contributed to the work presented in this report and like to place on record my grateful heartfelt thanks to each one of them who helped me in this project whichever and whenever needed.

This ARM Microcontroller workshop has been an amazing experience for me and I would like to thank all the well-wishers wholeheartedly, not only for their tremendous academic support, but also for giving me so many wonderful opportunities.

Special mention goes to my enthusiastic supervisor, Mr Sarath, (external guide) and similar, profound gratitude goes to Ms. Roopa Kulkarni, Asst. Professor, GIT (internal guide) both of them have been truly dedicated mentors. I am particularly indebted to them for their constant faith in my project work and for their support when it is needed.

My sincere heartfelt gratitude to our HOD Professor, P Patvardhan.

## Special mention goes to all the faculties in GIT, my friends, and some unknown persons for giving immense support and motivation.

# Abstract

## In this project a highly secured ATM transaction system has been developed with the help of visual basic programming and Embedded C. The authenticator (Bank) generates a random number and provides that to the card user whenever the user inserts his card on the ATM machine. The random generated code will be send to the card user with the help of GSM technology. The user can provide this code on the ATM machine and can continue his transaction. Whenever they entered code gets wrong the door of the ATM machine gets locked and security alarms will bang. This system will help the user to secure his transaction and prevents the unauthorized usage of the card.

An easy cash drawing system, Automated Teller Machine (ATM) has become an integral part of our society. Implementing ATMs in Treasury will be an added advantage for the Treasury itself and it will be a convenient cash drawing mechanism for the customers. This is one step forward to the Treasury department in their transforming stages.

This Project work is centred on the design of a computerized automated teller machine with the aim of achieving the proper and swift implementation of the use of machine in withdrawing money from the accounts of account holders. It describes about the stakeholders, existing and proposed system analysis, feasibility study, scope of business improvements, core banking networks, recommendations and suggestions etc. It also gives a very good idea about the security systems of ATMs that should be followed for the business continuity as well as for the project success.

# ****Introduction****

ATM is a computerized telecommunication device that enables the clients to perform the financial transactions like deposit, transfers, balance enquiries, mini statement and withdrawal etc without any need for a cashier or human clerk**.** There are two types of ATM: first one is a simple one which is used for cash withdrawal and to receive a receipt of account balance and second one is complex which is used for deposits and money transfer. The first one ATM is most widely and frequently used by people **[3].** Now a days, crimes at ATMs have been extensively increasing. In ATM, identification of people is done with the help of PIN number which is confidential. In such cases there is possibility of hacking passwords and personal information is more and some time it is difficult to remember the PIN number. The security of customer account is not guaranteed by PIN. Suppose by mistake if the card of customer is lost and the password stolen, then the criminal draw all the money in the shortest time. Many people are unlikely to memorize the PIN. So there is need of security in ATM transactions. The PIN is the 4 digit number given to all ATM card holders. The PIN numbers are different from each others. The password is only way to identify the customer when they have the card and correct password. Once the password and ATM card is stolen by the culprit they can take all money from the account in the shortest time.

**Outline of the Project Report**

The cash in transit or stored in the ATM safe has been the asset traditionally targeted by ATM criminals, sometimes in rather violent ways. However, in the last years, attackers have turned their attention equally to soft assets present in the ATM, such as PINs and account data.

Criminals use this stolen information to produce counterfeit cards to be used for fraudulent transactions—increasingly around the world— encompassing ATM withdrawals, purchases with PIN at the point of sale, and purchases without PIN tin card-not-present environments. PINs and account data are assets belonging to cardholders and issuers. They are inevitably in ― clear‖ form at the ATM, when the card and PIN are entered. By attaching, for example, a pinhole camera and a skimmer to the ATM, a criminal can steal PINs and account data before they can be securely processed by the ATM. These attacks require a relative low attack potential, in terms of both skills and material that is commercially available. The latest generations of skimmers and cameras are unnoticeable to untrained eyes and can be quickly installed and removed from the ATM without leaving any trace. In high traffic ATMs, dozens of PINs and associated account data sets can be stolen in a few hours.

The first line of defense to these attacks has to be offered by the ATM itself. Counter measures at device level include detection of attached alien objects, disturbance of magnetic-stripe reading near the entry slot, etc. Alarms generated by the device should be acted upon promptly and complemented with inspections of the ATM, more frequently at higher-risk installations. Taking all these parameters under consideration a secured ATM transaction system is proposed using microcontroller which will effectively stop the misuse of ATM system & also to take the necessary action against the culprit

**Existing method**

Security in ATM network is necessary because ATM is widespread and many areas such as financial or medical applications, network administration, etc. Require very sensitive handling of the transmitted data. If we look at other fields of interest we see that ATM channels might be used for billing .Misuse of the ATM network, manipulation of the transmitted data, spoofing or repudiation would be fatal in billing-/ accounting system. Therefore the ATM forum, the most important committee in developing and enforcing new standard concerning ATM, introduced the ATM security specification 1.0 in 1998. The specification contains mechanism to protect transmitted data in the user- and the control plane. The management plane will be treated in phase two of the specification. The ATM security specification describes the securities that are necessary to protect the user and the control plane. Confidentially, data integrity, accountability and access control are the main objectives. In the ATM security Framework ten necessary function AF-SEC-1 to AF-SEC-10.

AF-SEC-2: controlled Access and Authorization;

AF-SEC-3: Protection of confidentially;

AF-SEC-4: protection of data Integrity;

AF-SEC-5: strong Accountability;

AF-SEC-6: Activity logging;

AF-SEC-7: Alarm Reporting;

AF-SEC-8: Audit;

AF-SEC-9: Security Recovery;

AF-SEC-10: Management of security.

However not all of those security requirement will be discussed. AF-SEC-6 to AF-SEC-8 are mainly logging - function that are not subject of this review. AF-SEC-5 is essentially accomplished using authentication and authorization; thus it will be mentioned together with AF-SEC-1 to AF-sec-2.

## PROBLEM DEFINITION

The system will service one customer at a time. A customer will be required to insert an ATM card and enter a personal identification number (pin) –both of which will be sent to bank for validation as part of each transaction. The card will be retained in the machine until the customer indicates that he/she desires no further transactions, at which point it will be returned.

**HARDWARE REQUIREMENT**

• GSM Modem

• IR Sensor

• Personal computer

• Microcontroller

• RFID Reader

• Driver

• Relay

• Motor

• Keypad

• Power supply

**Software Requirement**

• Embedded c

• Visual Basic

**Working methodology**

## In our developed system whenever the transaction has to be done, once the card is inserted

inside the ATM machine a massage is received to the mobile phone of the actual card holder with a pin number of four digit. This number is entered in the ATM machine using 4\*4 keypad. It moves on to the next process if the password is correct, otherwise sends a wrong massage if the password doesn’t match. On the password being right it moves on to the next level of money transaction asking for the money withdrawal. There also would be a web camera which captures the photo for further clarification in future if any. After the transaction is over it display the balance amount in the account. In the scenario where the password doesn’t match the card would be blocked. There would be 2 dc motors where one works on the next process if the password is right for processing the money and another dc motor works closing the door if the password is wrong. If the account holder wants to continue with the next transaction a randomly generated password reaches his mobile entering which he can continue the same.

First of all, it is necessary to learn about the need of this costly project, for that different questionnaires were prepared for different stakeholders especially to citizens and employees. The data collected from them was analysed with the current similar system in the Banking and Financial sectors and confirmed the need of the project.

Then, collected information about the functions of ATM systems from various sources, about the securities needed for the smooth and successful functioning of the system after implementation, studied and analysed about the latest available hardware and software technologies in the market, collected data about ATM management, cash management and card management from vendors and similar system installed institutions, visited many ATMs and Banks to know about the functionality of different branded ATMs and collected data was analysed, then, recommendations and suggestions are put forward for taking a decision.

A common international standard security system and software, hardware technological features are suggested to avoid vendor locking in the future.

Project process includes:

1 Current system study

1. Problem identification

2. Feasibility study

3. Process identification

4. Process Re-engineering

5. Identification of Best system practices

6. Recommendations and Suggestions

7. Future scope of the project

8. Conclusion

**Limitations of the project**

Accuracy of data may be a little bit variable because of:

o Time limit.

o People are reluctant to give data.

o Vendors are giving only approximate values.

o Some people who could provide information are not approachable.

## Flowchart



**Flow Description**:-The flow of diagram is shown in fig (2). In this flow, when a person enters in the ATM, first swaps the ATM card then using GSM module, message will send to card holder. In this message, there is three option ―YES‗/NO‗/ACTION‖. If the person reply YES‗, then transaction will take place and process will ―STOP‗. If reply is ―NO‗, then transaction will cancel and process will STOP‗. If reply is ―ACTION‖, then card will block and door will be locked automatically and blow an alarm and then message will be sent to control room as well as the card holder using GSM module and process will STOP.

****

**Block Diagram Description**

## The block diagram of ATM security system is shown in fig (2). In this system, RFID card is the input of micro-controller. When a person swaps the RFID card through RFID Card scanner which is connected with controller and user data will fetch in PC and communication is performed using serial driver IC. After, the same user data is transferred to GSM module with the help of serial driver IC and using GSM module the message will send to card holder. In this message there is three option ―YES‗/ NO‗/ACTION‖. If card holder doesn‗t want to do a transaction, then simply reply ―NO‖ and transaction will stop. And if he want to do transaction then reply YES‗ and if the person knows his card is missing and someone making misuse of this card, then reply ‗ACTION‗ and at that moment the ATM door will be locked automatically with the help of EM lock and blow an alert alarm so the outside peoples can take some action. And also a message send to a police control room as well as card holder along with the ATM machine location and area code by using GSM module, so the necessary action can be taken against them. An electromagnetic lock is a locking device that consists of an electromagnet and an armature plate.

**Implementation Details**

## Software modues/GUI etc.

.

## *i) Control Unit*— The AT89C51 is a low-power, high- performance CMOS 8-bit microcomputer with 4Kbytes of Flash programmable and erasable read only memory (PEROM). The device is manufactured using Atmel‗s high-density nonvolatile memory technology and is compatible with the industry-standard MCS-51 instruction set and pinout . The on-chip Flash allows the program memory to be reprogrammed in-system or by a conventional nonvolatile memory programmer. By combining a versatile 8-bit CPU with Flash on a monolithic chip, the Atmel AT89C51 is a powerful microcomputer which provides a highly flexible and cost-effective solution to many embedded control applications. The AT89C51 provides the following standard features: 4K bytes of Flash, 128 bytes of RAM, 32 I/O lines, two 16-bit timer/counters, a five vector two-level interrupt architecture, a full duplex serial port, on-chip oscillator and clock circuitry. In addition, the AT89C51 is designed with static logic for operation down to zero frequency and supports two software selectable power saving modes. The Idle Mode stops the CPU while allowing the RAM, timer/counters, serial port and interrupt system to continue functioning. The Power-down Mode saves the RAM contents but freezes the oscillator disabling all other chip functions until the next hardware reset.

## *Features*

## • Compatible with MCS-51™ Products

## • 4K Bytes of In-System Reprogrammable Flash Memory – Endurance: 1,000 Write/Erase Cycles

## • Fully Static Operation: 0 Hz to 24 MHz

## • Three-level Program Memory Lock

## • 128 x 8-bit Internal RAM

## • 32 Programmable I/O Lines

## • Two 16-bit Timer/Counters

## • Six Interrupt Sources

## • Programmable Serial Channel

## • Low-power Idle and Power-down Modes

***ii) GSM Module:-*** The Real Time Devices GSM35 wireless GSM modem unit provides adirect and reliable GSM connection to stationary or GSM 900/1800 mobile fields around the world. GSM connectivity is achieved using the Siemens TC35 engine. This unit works in the 900/1800MHz band supporting GSM02.22 network and service provider personalization . Connect any standard GSM antenna directly to the OSX connector of the GSM35. The antenna should be connected to the TC35 using a flexible 50-Ohm antenna cable. In IDAN installations the antenna connection is brought to the front side of the IDAN-frame. The antenna used should meet the following specifications: **Frequency** : 890-910MHz (TX), 935- 960MHz (RX); Impedance :50 Ohms; **VSWR** 1,7:1 (TX) 1,9:1 (RX); **Gain** : <1,5dB references to 1/2-dipole; 1W **power** (cw): max 2W peak at 55 degrees Centigrade. GSM35 8 RTD Finland OyA SIM-card socket is located on the solder side of the module. The card can only be removed while the TC35 has been placed in shutdown mode. The GPRS35 is also available using the MC35 GPRS Modem. It supports all the features of the GSM35 and, on top, the advantages of the fast GPRS technology. The MC35 based GPRS modem GPRS35 is available now..

*Features*

 Low power Dual band Siemens TC35 cellular engine, GSM900/1800Mhz

 9,6/14,4 kbit/s datarate, group 3 faxes, SMS and

 SMS cell broadcast

 Onboard SIM-card socket for 3V standard cards

 16C550 UART interfaces to host computer

 Supports COM1,COM2,COM3,COM4 or COMx

 Available IRQ‗s 2,5,6,7,10,11,12,14,15

 Status LED indicating GSM activity and status

 16 TTL I/O‗s 8 outputs 8 inputs

 +5V only operation, 2.3W typical

 Wide operating temperature range –20 to + 70C

 guaranteed

 Onboard temperature ensor

 Fully PC/104 compliant, IDAN versions available

## iii)APR Module

*General Description* ***:*** The APR9600 device offers true single-chip voice recording ,non-volatile storage, and playback capability for 40 to 60 seconds. The device supports both random and sequential access of multiple messages.Sample rates are user-selectable,allowing designers to customize their design for unique quality and storage time needs. Integrated output amplifier ,microphone amplifier, and AGC circuits greatly simplify system design. the device is ideal for use in portable voice recorders, toys, and many other consumer and industrial applications. APLUS integrated achieves these high levels of storage capability by using its proprietary analog/multilevel storage technology implemented in an advanced Flash non-volatile memory process, where each memory cell can store 256 voltage levels. This technology enables the APR9600 device to reproduce voice signals in their natural form. It eliminates the need for encoding and compression, which often introduce distortion.

*Features :*

 Single-chip, high-quality voice recording & playback solution

- No external ICs required

- Minimum external components

- Non-volatile Flash memory technology

- No battery backup required

 User-Selectable messaging options

- Random access of multiple fixed-duration messages.

- Sequential access of multiple variable-duration messages

- User-friendly, easy-to-use operation

- Programming & development systems not required

- Level-activated recording & edge-activated play back switches

 Low power consumption

- Operating current: 25 mA typical - Standby current: 1 uA typical - Automatic power-down

 Chip Enable pin for simple message expansion.

## 

**Test Cases**

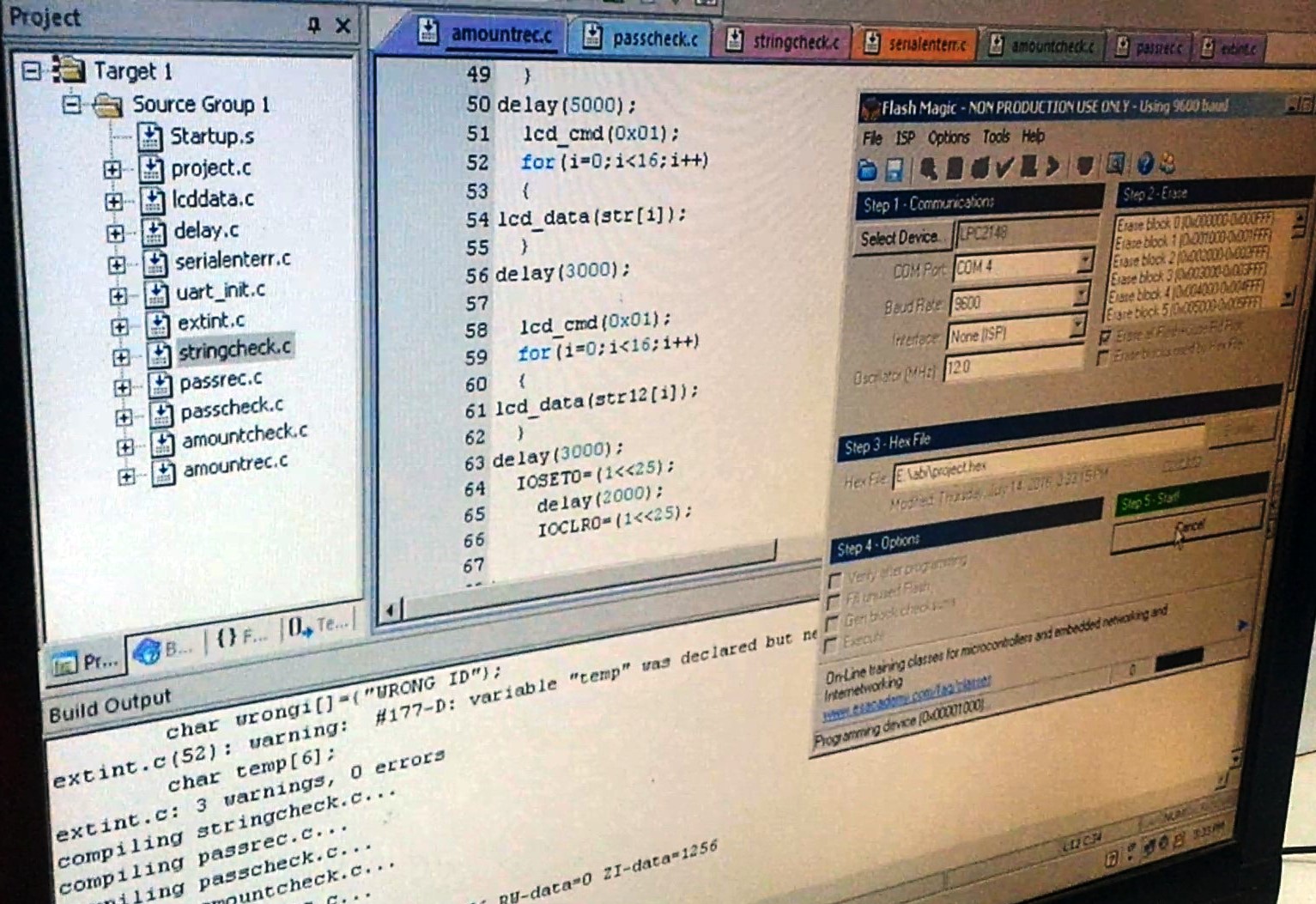
## We are using Visual Basic 6.0.software in Front End and Assembly Language in Back End. RIDE software is Resonance Integrated Development Environment that provides seamless integration and easy access to all development tools. RIDE is based on a fast multi-document editor designed to meet the specific needs of programming. In simple language it is used for writing the program and also to stimulate the program after exeution Flash Magic is an application developed by Embedded Systems Academy to allow you to easily access the features of a microcontroller device. With this program you can erase individual blocks or the entire Flash memory of the microcontroller. Using Flash Magic, you are able to perform different operations to a microcontroller device, operations like erasing, programming and reading the flash memory, modifying the Boot Vector, performing a blank check on a section of the Flash memory and many others

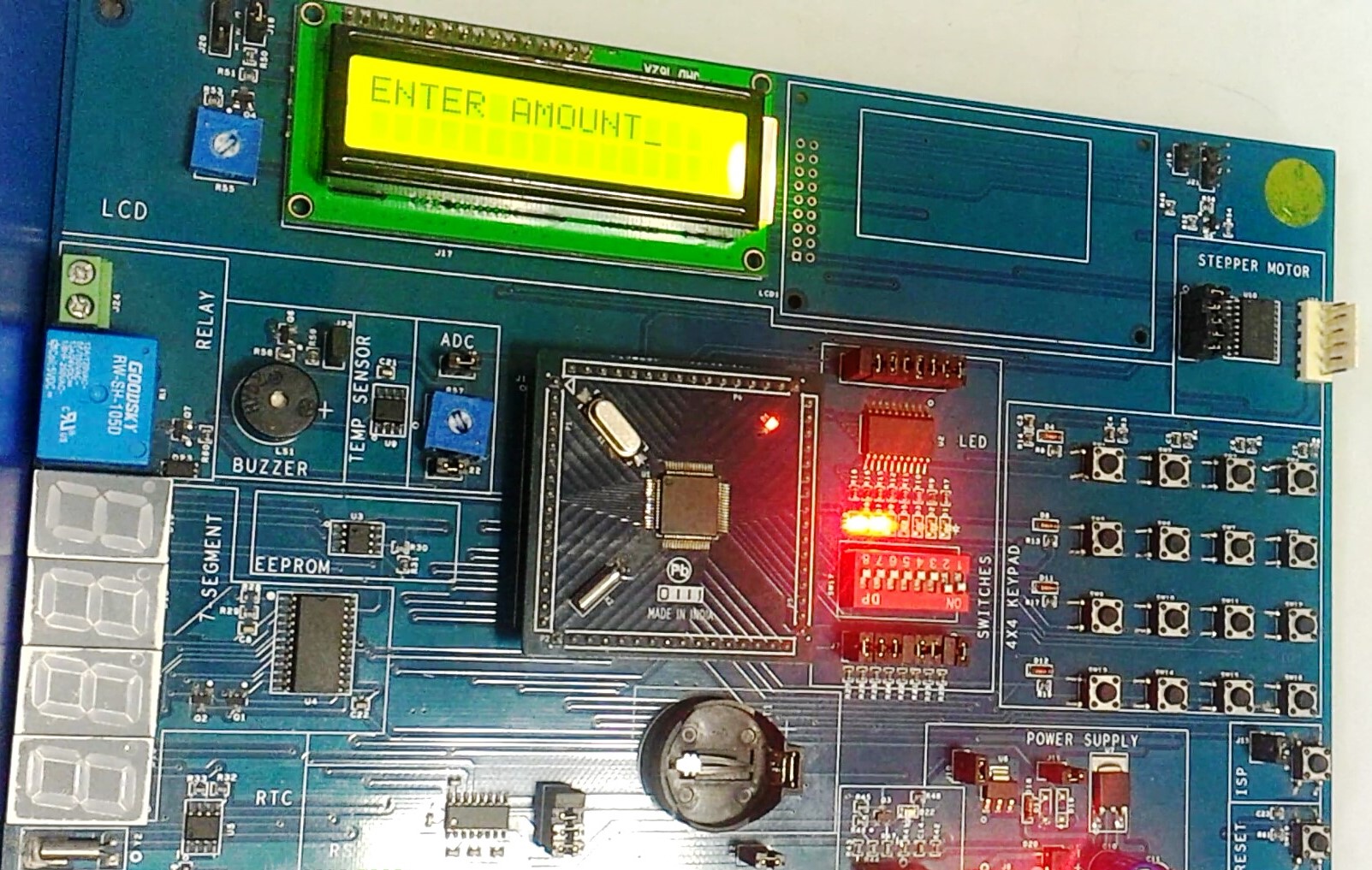
**SNAPSHOTS**

## Picture 1

## 

Picture 2



Picture 3****

**CONCLUSION AND FUTURE SCOPE**

# The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords birthdays, phone numbers and social security numbers. This paper may solve this problem and useful for detecting a fraud . It is used in Bank sector and any ATM related security. It is also called as thief tracking system. As there is a scope for improvement and as a future implementation we can add a tracking chip on ATM card for tracing the location of card which will help in providing users assistance

## CONCLUSION

The progress in science &technology is a non-stop process. New things and new technology are being invented. As the technology grows day by day, we can imagine about the future in which thing we may occupy every place.

The proposed system based on Atmel microcontroller is found to be more compact, user friendly and less complex, which can readily be used in order to perform several tedious and repetitive tasks. Though it is designed keeping in mind about the need for security purpose, it extended for other purposes such as industrial & research applications. Due to the probability of Embedded technology and GSM technology made this project(“MICROCONTROLLER BASED SECURE PIN ENTRY METHOD FOR ATM”) a fully software controlled with less hardware circuit. The feature makes this system is the bass for future system. The principle of the development of science is that “nothing is impossible”. So we shall look forward to a bright & sophisticated world.

# REFERENCES

Antovski, L. and Gusev,M.(2003) ‘A pin-Entry Method Resilient Against Shoulder Surfing’, vol. 04, pp. 236-245.

Stevenson, D. N. and Byrd, G. (1995) ‘Secure Communications in ATM networks’ vol. 38, pp. 45-52.

Kuhn, S. And Wollenweber, R. (1999) ‘ATM-encryption with 155 Mbit/s in ATM Workshop. Institution Electrical and Electronic Proceedings, PP. 307-312.

Zhang, p.and Dou, j.h, and Pan, M(2008) ‘In Information Theory, Institution Electrical and Electronics Engineers, Transactions on, volume 13, pages 21-27.

1) ―ATM security System using fingerprint biometric identifier: An Investigative Study‖ ,By- Saatci, V avsanogh, M. Purser. Year of publishing pape r 2009-2010 IEEE. 2) ATM Textbooks [DL95] H. Dutton and P. Lenhard, "Asnchronous Transfer Mode (ATM) Technical Overview",2nd Ed., Prentice Hall, 1995. 3) ― Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System‖‖ ,By S.S, Das and J. Debbarma, International Journal of Information and Communication Technology Research,vol.1, no. 5, pp.197-203,2011. 4) ― An Overview of ATM Security Using Biometric Technology‖ By Jaspreet Kaur , Sheenam Malhotra International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 3, March 2014 , ISSN: 2277 128X. 5) Padmapriya V, Prakasam S. ―*Enhancing ATM Security Using Fingerprint and GSM Technology,*‖ International Journal of Computer Application (IJCA), ISSN: 0975-8887, Vol. 80, pp: 43-46, Issue No. 16, October 2013