Volume 4, Issue 4, April 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secured ATM Transaction System Using Micro-Controller

Mrs.S.P.Balwir[1], Ms.K.R.Katole[2], Mr.R.D.Thakare[3], Mr.N.S.Panchbudhe[4], Mr.P.K.Balwir[5]

[1,2,3,4] Asst. Professor ,Dept. of Electronics, DBACER Nagpur

[5]:S.D.E. BSNL, India

Abstract— The main objective of the system is to develop an Embedded system , which is used for ATM SECURITY purpose/application. The System uses serial communication with the computer to scan the data base of the card holder and automatically generates every time message to a mobile of the authorized customer through GSM module connected to a microcontroller 89C51 . The RFID card reader is used as an identity for a particular users . If the identity (serial number of the tag) of the user is matched with the one already stored in this system, he gets immediate access through it and then the transaction is done .If the false identity is recognized then the card holder simply reply "ACTION'' then the transaction will stop and at that moment ATM door will be locked automatically by EM Lock and blow an alarm so the concerned authority can take some action. And also a message will be sent to a card holder along with the ATM machine by using GSM module.

Keywords—ATM , microcontroller 89c51,GSM Module, RFID Reader, EM Lock

I 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.

1) ATM Security Overview

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 .The flow diagram is as proposed below

Flow Diagram:-

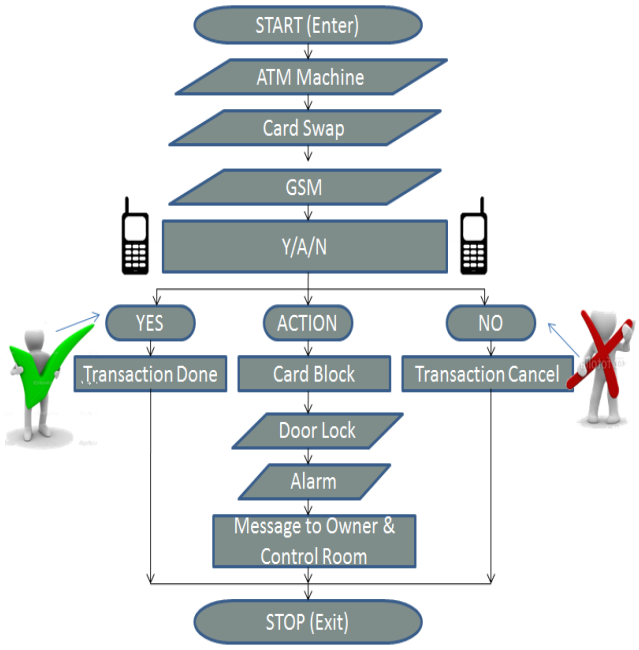

Fig. 1 Flow Diagram for ATM Security system

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.

II Block Diagram

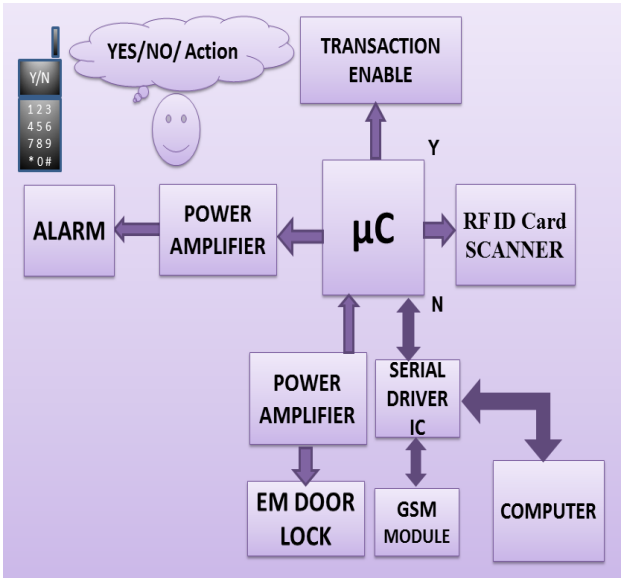

Fig. 2 Block diagram of ATM Security System.

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.

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.

III SOFTWARE IMPLEMENTATION

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

IV RESULTS

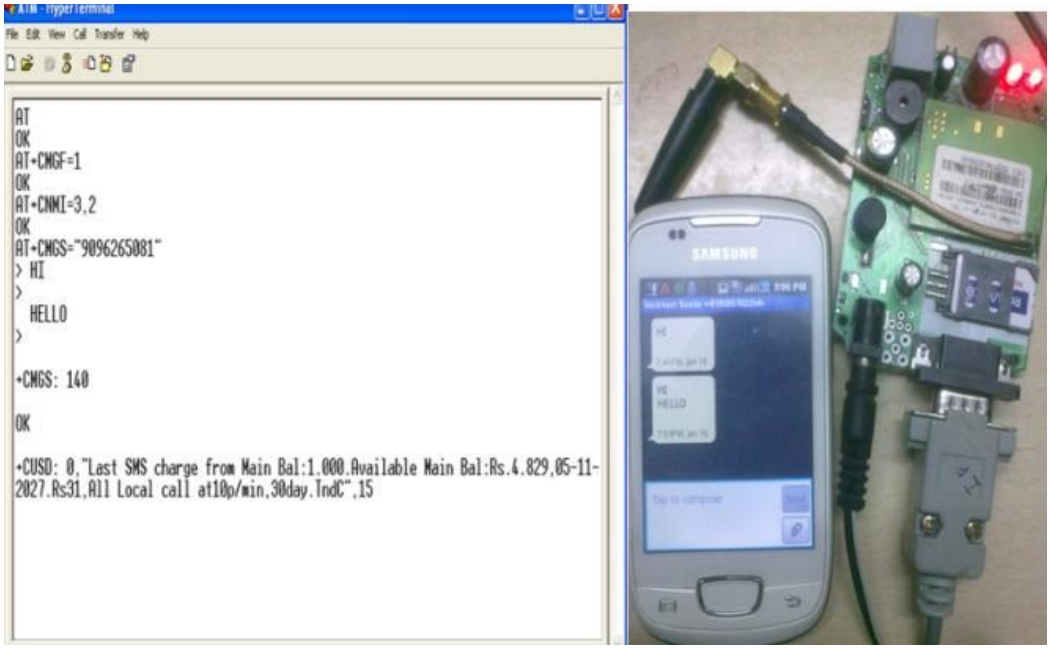

Fig 3) Output Of GSM Module

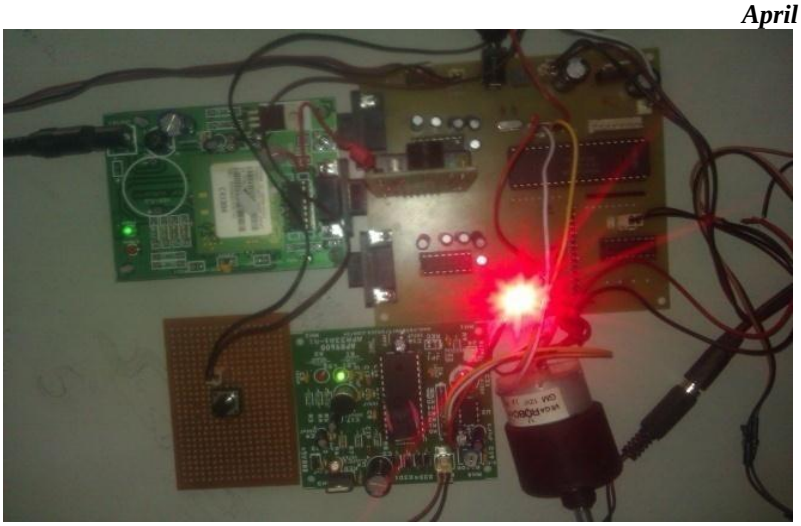

Fig 4**)** Complete Hardware Development For ATM Security System

V CONCLUSION

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.

REFERENCES:

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 Systemǁ" ,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 .

