Enhancement of Security for ATM Transactions Using Near Field Communication

[1] P.Subbulakshmi [2] K.Venkatesh [3] M.Karuppasamy [4] S.Paramasivam
[1][2] Department of Information Technology
National Engineering College, Kovilpatti, Tuticorin District, Tamilnadu, India
Anna University Chennai,
[1] subbu.psk@gmail.com [2] vijayvenkatesh95@gmail.com [3] karuppasamy127@gmail.com
[4] karthiparama@outlook.com

Abstract: **ATMs are predominantly used all over the world. However, the safety of any money transaction is always a concern, no matter how many technologies are developed to protect the transaction. The idea of this project is to develop the prevention of theft of the ATM card and to control the usage of the ATM card by unauthorized person. Conditional security is provided with protocol data unit. The additional feature of this project is that no transaction can be done without the knowledge of the respective card holder for the cause that NFC transactions are being implemented. Whenever the transaction has to be done, ATM machine and NFC devices are made to interact with some of the legacy systems. Granting that NFC device is found to be accurate, an authentication is received to the mobile phone of the rightful proprietor with a pin number. In case of password being correct it moves on to the next level of money transaction, asking for the money withdrawal.**

Keywords**— NFC (Near Field Communication), ATM (Automated Teller Machine), RFID (Radio Frequency Identification)**

I. INTRODUCTION

Embedded Systems are devices which are used to control, monitor or assist the operation of an equipment, machinery or plant. The term—control‖ defines the main function of Embedded System because their purpose is to control an aspect of a physical system such as pressure, temperature and so on. Also the term —monitor‖ defines t he progress of activities.

An embedded device can range from a relatively simple product for example a toaster to complex mission critical applications such as those used in avionics. A typical embedded device will have both hardware and software components. The hardware could be micro components such as embedded microprocessor or microcontroller. Microcontroller is relatively small, has an on chip memory, an I/O controller and other supported modules to do processing and controlling tasks. The software consists of applications that perform dedicated tasks and may run on Real time operating system.

Embedded System may be either an independent system or a part of a large system. It is specialized computer system but not a general purpose workstation like a desktop or a computer. Such kind of systems is housed on a single microprocessor board with programs which are stored in ROM (Read Only Memory) embedded system is usually a compact, portable and mass produced electronic devices.

An automated teller machine or automatic teller machine, also known as an automated banking machine (ABM, Canadian English), cash machine, cash point, cash line, or colloquially hole in the wall (British and South African English), is an electronic telecommunications device that enables the customers of a financial institution to perform financial transactions without the need for a human cashier, clerk or bank teller. On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smart card with a chip that contains a unique card number and some security information such as an expiration date or CVVC (CVV). Authentication is provided by the customer entering a personal identification number (PIN). Using an ATM, customers can access their bank deposit or credit accounts in order to make a variety of transactions such as cash withdrawals, check balances, or credit mobile phones. If the currency being withdrawn from the ATM is different from that in which the bank account is denominated the money will be converted at an official exchange rate. Thus, ATMs often provide the best possible exchange rates for foreign travelers, and are widely used for this purpose.

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.

II. PROBLEM STATEMENT

In the last decade each and every ATM card uses the magnetic stripe where the data are stored by making some changes in the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. Using skimmer device attackers easily read the magnetic stripe card. It is not an securable method for the money transaction. Hackers will easily hack the user data. Later there was the introduction of RFID which means Radio Frequency Identification. Here the user need not swipe the card into the machine instead reader will sense the card and allow the user for transaction purpose. In RFID based ATM card also has drawbacks. RFID is used for speed transaction but it didn't have securable algorithm. In addition to that RF tag is read by two RF readers so it is not safety.

III. 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 presently used ATMs was produced usually more than
10 years ago. They are outdated worldwide. Think of their operating system, the Windows XP Embedded, which support is going to end in 2016. Therefore, the time has come to develop the next ATM generation. The first innovative step would be equipping the ATMs with NFC card readers. My goal was to let users operate withdraws and other transactions e.g. with their Smartphone's via NFC. This must seems like a science fiction, but the technology is available now. We will use ATMs without touches on it in the near future. 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

IV. OBJECTIVE

The main objective of this project is to move the security to the next level to introduce the latest technology and also to have secured transactions for the user. In the previous method there are some security purposes but also the attackers work is so simple to hack and to steal the money from the user. But in this project it is very much difficult to hack due to high security. It helps a secured money transaction for the user.

4.1 Flow Diagram

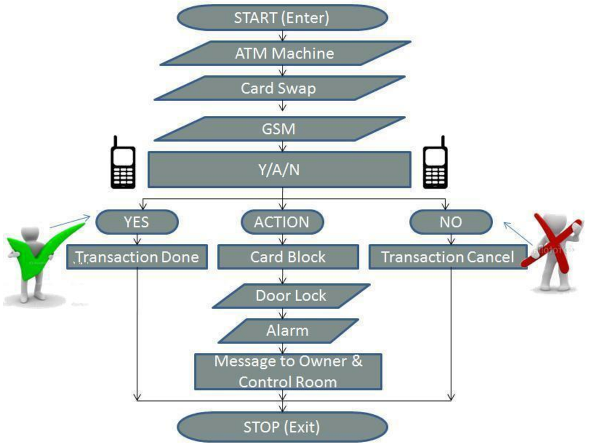

Fig. 1 Flow Diagram for ATM Security system

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 replies YES_, then transaction will take place and process will ―STOP_. If reply is ―NO_, then transaction will cancel and process wills 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.

V. PROPOSED METHODOLOGY

The proposed method of ATM transaction is based on NFC and Android devices.NFC (Near field communication) is a technology that enables contactless transfer of information between devices. Connection between two devices is established just by holding the devices close to each other or by touching them together.

When the user enters into ATM room, our smart phone Bluetooth is connected with ATM machine. When the user access NFC based smart card with ATM, it read card number securely. The ATM sends authentication message to the user's mobile phone. In authentication the user have to enter a password. This password sends to ATM via Bluetooth. If password match, it goes to money transaction otherwise ATM ignore the card.

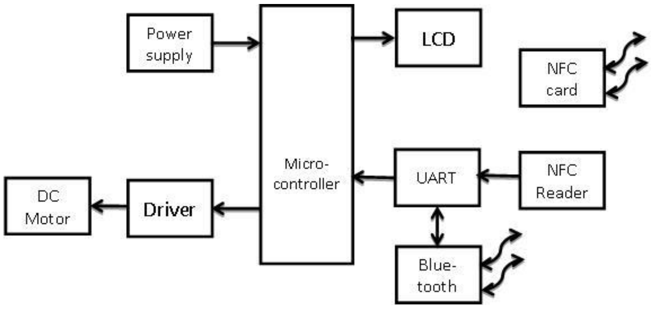

Fig. 2 Block diagram of ATM Security System

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. If card holder doesnot want to do a transaction, then simply reply and transaction will stop. And if he want to do transaction then reply and if the person knows his card is missing and someone making misuse of this card, then reply 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 people 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.

5.1 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 pin out . 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

5.2 GSM Module:-

The Real Time Devices GSM35 wireless GSM modem unit provides a direct 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.

5.3 NFC – Technology:

NFC has been spreading among Smartphone since last few years. Thanks to Broadcom Company, who integrates it with other wireless technologies into a single chip. It is worth to buy because manufacturers can produce Smartphone with more capabilities in low price. NFC stands for Near Field Communication. NFC standards cover communications protocols and data exchange formats, and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and FeliCa Near field communication (NFC) is the set of protocols that enables Smartphone and other devices to establish radio communication with each other by touching the devices together or bringing them into proximity to a distance of typically 10 cm (3.9 in) or less.

VI. 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 foruse 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.

VII. SOFTWARE IMPLEMENTATION

The Keil C51 C Compiler for the 8051 microcontroller is the most popular 8051 C compiler in the world. It provides more features than any other 8051 C compiler available today. The C51 Compiler allows the programmer to write 8051 microcontroller applications in C that, once compiled, have the efficiency and speed of assembly language. Language extensions in the C51 Compiler give you full access to all resources of the 8051.The C51 Compiler translates C source files into reloadable object modules which contain full symbolic information for debugging with the µVision Debugger or an in-circuit emulator. In addition to the object file, the compiler generates a listing file which may optionally include symbol table and cross reference information. The Android SDK includes a mobile device emulator a virtual mobile device that runs on your computer. The emulator lets you develop and test Android applications without using a physical device.

VIII. CONCLUSION

This project deals with the design and implementation of NFC based secure transaction system in ATM machines. This system consists of two modules, the ATM and the Mobile module in order to provide high end security for the ATM users and the service providers. The password for transaction is send to the cardholder's mobile phone with the help of wireless technology, which is an added advantage. In conclusion, it is expected that the proposed method will help users to protect their privacy and use personalized services. It will contribute to the promotion of mobile payment services through NFC.

REFERENCES

1) ATM security System using fingerprint biometric identifier: An Investigative Study, By- Saatci, V avsanogh, M. Purser. Year of publishing paper 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