Multi Authentication ATM Theft Prevention Using iBeacon

Manoj V[1], MouliSankar R[2], Sasipriya S[3], Usha Devi E[4], Devika T[5]

[1,2,3,4]UG Student, Knowledge Institute of Technology, Salem-637403
[5]Assistant Professor, Knowledge Institute of Technology, Salem-637403

---***---

Abstract-In this modern world, money is required at anytime or anywhere for travelling, shopping and health emergencies we need to carry money. It increases the risk of robbery at any instant. where bank is the safest place to keep our money. It provides Automated Teller Machine(ATM) which can provide money at any time at any location.ATM is the easiest way to get the money, we just need to insert the card and enter password and we can get the money in few minutes. But if someone steal our card and password, they can easily access our money. This motivates us to increase user security by adding the secondary stage of prevention to the existing system by using GSM module to generate OTP and verify whether the specified person is using .User only get the money by entering the respective OTP via SMS..In case if there is a less coverage of network at specified location. There is no possibility of OTP through GSM at this time we use iBeacon Module for getting OTP and verify the specific card holder details.

Keyword: ATM machine, PIC 16F877A microcontroller, GSM and iBeacon module.

I.　Introduction

We belong to the edge of digitized and smart world. People are getting smarter day by day with the help of new technology, new innovations. Main reasons behind the up gradation of new technologies are nothing but to overcome the existing problems. A smart step towards economy is the introduction of Automated teller machine (ATM), for faster and easier money transfer with the typical offering high-quality 24 hours service for customer. In this era of technology, ATM (Automated Teller Machine) card is the essential part of life. To have transaction ATM pin number is necessary and it must be secure. But a group of people do malpractices over this ATM system to put people, organization or bank into a million pounds of loses. The present ATM system uses the ATM card along with PIN number only. If a thief has stolen the ATM card and if he/she knows the password, he/she can misuse the ATM card. In some cases it may be happen the attackers make a card as your ATM card and mischief with the Bank account.

To skip this problem we propose a concept of setting cash limit, where one has to present one' OTP only if one wants to withdraw the predefined cash limit condition is found to be true else cash withdrawal without OTP sends an alert message to the user mobile through GSM technology. It also guarantees security as each ATM has its cash limit and bank has its transaction limit. So, in case of card misuse, this embedded system developed will prevent withdrawal of large cash. Low amount transaction is secured by the OTP in order to increase security and to save the user time. It will also limit the maximum amount that can be withdrawn by unauthorized person in case. When there is a network problem in GSM technology, instead of GSM we use Bluetooth connection with ATM, Which generates OTP reference through user mobile. Then it verifies the OTP and transfers the amount.

II.　Literature survey

[1]Security of ATM System Using Biometric and OTP

Reshma Begum, Dr.BasavarajGadgay*et al* describes about increase user security in ATM by adding the biometric and OTP to the existing system. It also put forward some issues which include sensor durability and time consumption. We introduce a constraint on transactions by ATM involving biometric (finger print) to improve the system performance and to solve the issues. We are adding a limit on amount of cash, if the entered amount is more than the limit, it is necessary to present biometric. If one need to withdraw the minimum cash, biometric scanning is not mandatory only will enter the OTP for user authentication.

[2]Fingerprint Based Biometric ATM Authentication System

DhirajSunehra describes the Biometrics technology is rapidly progressing and offers attractive opportunities. In recent years, biometric authentication has grown in popularity as a means of personal identification in ATM authentication systems. The prominent biometric methods that may be used for authentication include fingerprint, palm print, handprint, face recognition, speech recognition, dental and eye biometrics. In this paper, a microcontroller based prototype of ATM cashbox access system using fingerprint sensor module is implemented.

[3] Generation of Secure One Time Password for ATM Security and Theft Protection

S.Pooranachandran, E.Aravind*et al* describes the system which is used for security purpose and to detect the lost of ATMcard through the SMS. This system proposes a one-time password (OTP) to the user's mobile number for furthermore secure authentication system process. This system protects the user from shoulder-surfers & partial observation attacks and is also resistant to relay, replay and intermediate transaction attacks.

[4]**ATM Security using finger print authentication and OTP**

Rathishala Rajendran, Kavita Anandraj al describes the primary step to verify currently provided fingerprint with the fingerprint which is registered in the Bank's database at the time of account opening. If the two fingerprints get matched, then a message will be delivered immediately to the user's mobile number which is the random 10 digit pin number called as One Time Password (OTP). This OTP can be used only once, thus this avoids various problems associated with the present system. For every transaction, new OTP will be sent to account holder's mobile number, thus there will not be fixed PIN number for every transaction. Thus, PIN number will vary during each transaction assuring security.

III. Existing Method

In existing systems, where systems have been secured the atm user transaction information by using OTP and biometric. Where they used RFID card as ATM card, followed by 4-Digit Secret code entered in number pad and OTP is generated and sent to the registered mobile number by using GSM, As a Secondary Authentication they used finger print scanner to verify the authorized person and the output of the overall system is displayed on the LCD. In addition with this a tilt sensor is used for the security of the atm machine, if anybody try to steal the machine then there will be tilting which is sensed by tilt sensor interfaced to the atm machine and is indicated by the buzzer alert.
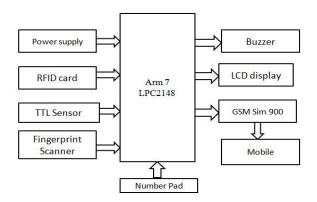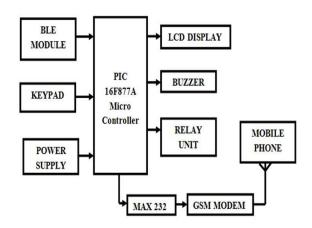

Fig: 1 Existing Block Diagram

IV. Proposed Method

In this proposed method we have designed a new method in improving the ATM theft prevention by using iBeacon module. After entering the correct four digit pin number, security alert message have triggered to respective mobile number through GSM module. Then OTP is generated to our mobile. Using this OTP we can authorize our presence and control the money limitation via sms. Incase if there is no availability of mobile signal in any specified location. we can authenticate via iBeacon module(advanced BLE) and verify the OTP to take money.

Fig:2 Block Diagram

IV.A. PIC Microcontroller

A family of Harvard architecture microcontrollers made by Microchip Technology, PIC16F877A belongs to a class of 8bit microcontrollers of RISC architecture. The integrated circuits(IC) contained both processor and peripherals (Timers, ADC, USART, EEPROM, I2C, SSP, PSP) are inbuilt is called PIC microcontroller.

Features of PIC:

High performance RISC CPU

Operating speed: DC (4 – 20) MHz clock input Only 35 single word instructions to learn Up to 8K x 14 words of FLASH Program Memory. Up to 368 x 8 bytes of Data Memory (RAM).

Up to 256 x 8 bytes of EEPROM Data Memory Wide operating voltage range: 2.0V to 5.5V

Interrupt capability (up to 14 sources) Eight level deep hardware stack

Direct, indirect and relative addressing modes Programmable code protection

IV.B. GSM modem

A GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone. When a GSM modem is connected to a computer, this allows the computer to use the GSM modem to communicate over the mobile network. While these GSM modems are most frequently used to provide mobile internet connectivity, many of them can also be used for sending and receiving SMS and MMS messages. GSM modems can be a quick and efficient way to get started with SMS, because a special subscription to an SMS service provider is not required. In most parts of the world, GSM modems are a cost effective solution for receiving SMS messages, because the sender is

paying for the message delivery. A GSM modem could also be a standard GSM mobile phone with the appropriate cable and software driver to connect to a serial port or USB port on your computer.

Fig:3 GSM modem

Features of GSM kit:

GSM is a highly flexible plug and play quad band GSM modem integration to RS232 Supports features like voice, data/fax, SMS, GPRS and integrated TCP/IP stack Control via AT commands(GSM 07,07,07,05 and enhanced AT commands) Use AC-DC power adapter with ratings are DC voltage 12V/1A Current consumption is 250mA.

IV.C. Bluetooth

Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions in the ISM band from 2400-2480 MHz) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. Created by telecoms vendor Ericson in 1994 it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization.

Bluetooth uses a radio technology called frequency- hopping spread spectrum, which chops up the data being sent and transmits chunks of it on up to 79 bands (1 MHz each; centered from 2402 to 2480 MHz) in the range 2,400-2,483.5 MHz (allowing for guard bands). This range is in the globally unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency band.

V.   CONCLUSION

The problem of ATM Theft and misusing of ATM Card has become a major social problem in the society. So many people lost their amount without their knowledge and it also difficult to retain the money to the card holder. We proposed the paper to overcome the problem by automatic security system. Importantly the money can be withdrawn only by the card holder's permission via mobile.

REFERENCES

[1] [1] Maninder Singh, Shahanaz Ayub and Raghunath Verma, "Enhancing Security by averaging multiple fingerprint images," Proc. International Conference on Communication Systems and Network Technologies, IEEE 2013

[2] [2]Pennam Krishnamurthy & M. Maddhusudhan Reddy, —Implementation of ATM Security by Using Fingerprint recognition and GSM —International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249–071X, 2012.

[3] S.T. Bhosale and Dr. B.S.Sawant "SECURITY IN E-BANKING VIA CARD LESS BIOMETRIC ATMS", International Journal of Advanced Technology & Engineering Research, Volume 2, Issue 4, July 2012.

[4] D. Vinod kumar, & Prof.M R K Murthy "Fingerprint Based ATM Security by using ARM7" IOSR Journal of Electronics and Communication Engineering ISSN : 2278-2834 Volume 2, Issue 5 (Sep-Oct 2012), PP 26-28.