RESEARCH ARTICLE OPEN ACCESS

Preventing Shoulder Surfing Attacks in ATM Using Base Pin and Base Character

K.Manoj*, S.Thiyagaraj**,S.Sathyamoorthi***
**(Department of Electrical and Electronics Engineering, Sasurie College of Engineering, Vijayamangalam-56)*
*** (Department of Electrical and Electronics Engineering, Sasurie College of Engineering, Vijayamangalam-56)*
****(Assistant Professor, Department of Electrical and Electronics Engineering, Sasurie College of Engineering, Vijayamangalam-56)*

ABSTRACT
Authentication is a critical part of any trustworthy computing system which ensures that, only individuals can to log on to the system. Here ATM Security has always been one of the most prominent issues. ATM machines generally authenticates by using ATM card and PIN number to perform transactions. This papers discusses design of ATM system that will improve the authentication of customer while using ATM. Here is possible scenario that an individual's ATM card falling into wrong hands by knowing PIN number and forget ATM card is difficult to perform ATM transaction. So to clear all these problems we are implementing this system using "Base Character" and "Personal Identification Number (PIN)" combination in order to improve authentication of customer using ATM machine to perform transaction without having any ATM cards.

Keywords **–** Automatic Teller Machine (ATM), Global System Module (GSM), Personal Identification number (PIN),Radio Frequency Identification(RFID).

I. INTRODUCTION

The ATM was invented to solve the problem of long queue in banks and to improve the quality of banking services to customers. With the ATM, customers can access their bank accounts in order to make cash withdrawals and check their account balances as well as purchasing mobile phone prepaid credit. Being a machine, it is important that it authenticates the user each time he/she applies for access to ATM Services. This is usually done by the insertion of an ATM card which contains a unique card number and security information such as a PIN number which is unique to every user. Anybody can be in the possession of the card and the person may have knowledge of the users PIN. This makes this approach vulnerable to ATM fraud.

1.1 How Do Atms Work?

ATM is communicate with central host processor by Internet Service Provider has a gateway where all ATM networks available to user. Here ATM machines connected to central host processor are by telephone lines or normal phone line using modem. When customer wants to perform transaction provide PIN details and ATM card. ATM machine forwards to central host processor, where ATM request to customer's bank. If customer request cash, central host processor initiates electronic funds transfer from customer bank to ATM central host processor account. Once transfer complete to central host processor, it sends approval code to ATM machine to dispense cash.

But authentication of ATM during transactions are also unsecure because with help of clone of original cards by replicas of ATM machine card slots with built-in magnetic strip readers. The reader capture data embedded in the magnetic strip and store it. By placing small wireless surveillance cameras in ATM center to track the PIN to cash withdrawal. To overcome this, I proposed using base pin and base character to authenticate the ATM transactions in ATM'S.

1.2 Unimodal Biometrics System

Biometrics is derived From the Greek word "bio" means life and "metrics means measure. Biometrics refers to identity of an individual based upon physical characteristics or behavioural traits. Where identity of a person by password, PIN provides first level of security, fingerprint templates are encoded into smart card memory, to identify his/her fingerprints are compared against the digital templates in card memory. In Traditional methods to identify persons base on knowledge or token-based mechanism, but easily lost, shared or stolen. So, to overcome all these we introduced biometric system like fingerprint, Iris, Retina, Palm print, Face recognition. Limitations Problems in biometric systems are noise in sensed data, lack of individuality, .Intra-class variations, spoofing.

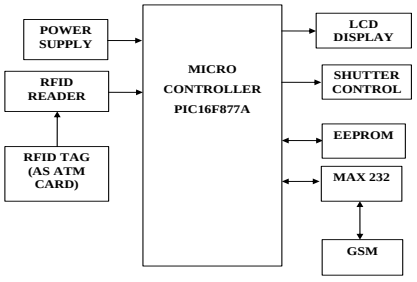
1.3 Crypto-Biometric System

In this Crypto-Biometric [9] system at the time of transaction retinal image is captured and blood vessel tree is extracted. From that blood vessel tree selective feature points extracted using Harris Corner detection [9] to generate 256 bit key. With help of User's bio-key user's password is encrypted. Encrypted password transform to central server where image is decrypted. Advantages of Crypto-Biometric mechanism increase of reliability and identification quality, reducing error rates. Limitation using Crypto-Biometric mechanism, if biometric fails due to presence of noise in the biometrics, the FRR [9] (False Reject Rate) increases. Increases cost effectively due to installation of additional hardware.

1.4 Authentication in ATM System by Base Character

Using base character to provide more security for the user. The user will be provided with a secret alphabet which will act as a base character. The total number of letters in the corresponding word will be counted and it will be added to the base pin which acts as a pin.

II. BLOCK DIAGRAM



2.1 Block diagram description

The proposed system consists of PIC16F877A, Power supply, Vibration sensor, LCD and GSM Modem. RFID tag acts as an ATM card and RFID reader is used to read the data when the car is swiped. The GSM module is used to send the message to the police station when someone tries to misuse the card.MAX232 is used as a power translator. The GSM module works in the 13V power supply and the microcontroller works in the 5V supply. So to regulate the voltage this is used. Shutter controller is used to close the door whenever the unauthorized person tries to access the ATM card. The LCD display is used to display the random words that are being used as a base character.

2.2 Microcontroller PIC16F877A

PIC 16F877 is a 40-pin 8-Bit CMOS FLASH Microcontroller from Microchip. The core architecture is high-performance RISC CPU with only 35 single word1 instructions. Since it follows the RISC architecture, all single cycle instructions take only one instruction cycle except for program branches which take two cycles. 16F877 comes with 3 operating speeds with 4, 8, or 20 MHz clock input. Since each instruction cycle takes four operating clock cycles, each instruction takes 0.2 micro seconds when 20MHz oscillator is used.

It has two types of internal memories: program memory and data memory. Program memory is provided by 8K words (or 8K*14 bits) of FLASH Memory, and data memory has two sources. One type of data memory is a 368-byte RAM (random access memory) and the other is 256-byte EEPROM (Electrically erasable programmable ROM). The core feature includes interrupt capability up to 14 sources, power saving SLEEP mode, and single 5V In-Circuit Serial Programming (ICSP) capability. The sink/source current, which indicates a driving power from I/O port, is high with 25mA. Power consumption is less than 2mA in 5V operating condition.

2.3 Vibration Sensor

The vibration sensor are used to sense any misuse occurrence once if any signal is send to microcontroller then the microcontroller will send information to nearest respective bank and police station via message through GSM modem. The vibration / shock sensor detects shock intensity caused by sudden knocks or hits and continuous vibration due to any obstacles on ATM's. The shock levels and monitoring durations can be set for each individual sensor, enabling a user-defined profile for up to tolerance level.

2.4 GSM

GSM networks operate in a number of different frequency ranges (separated into 31TGSM frequency ranges31T for 2G and 31TUMTS frequency bands31T for 3G). Most 31T2G31T GSM networks operate in the 900 MHz or 1800 MHz bands. GSM-900 uses 890–915 MHz to send information from the 31Tmobile station31T to the 31Tbase station31T (uplink)

2.5 RFID system

Radio frequency identification (RFID) is wirelessly, using radio waves. In an RFID system, the RFID tag which contains the tagged data of the object generates a signal containing the respective information which is read by the RFID reader, which then may pass this information to a processor for processing the obtained information for that

particular application. An RFID reader consists of an antenna, transceiver and decoder, which sends periodic signals to inquire about any tag in vicinity. On receiving any signal from a tag it passes on that information to the data processor. These tags can be either active or passive. While the active tags have on chip power, passive tags use the power induced by the magnetic field of the RFID reader. Thus passive tags are cheaper but with lower range (<10mts) and more sensitive to regulatory and environmental constraints, as compared to active tags.

2.6 Liquid crystal display (LCD)

Liquid crystal displays (LCD's) have materials, which combine the properties of both liquids and crystals. These modules can be interfaced with a 4-bit or 8-bit microprocessor /Micro controller. The LCDs used exclusively in watches, calculators and measuring instruments are the simple seven-segment displays.

III. CONCLUSION

Thus we have reviewed several authentication algorithms like PIN, biometric system to perform the ATM transaction lot of security concerns, increases hardware. So, with help of Base character and PIN combination we can reduce the ATM banking system security problems, reduces hardware and software cost. Using these methods we can perform the ATM transaction no chance for theft of ATM cards.

3.1 Advantages

- Previous methods are hard to remember for the user
- No additional hardware required
- Easy to implement
- User friendly

REFERENCES

[1]. Binachi.A, Oakley.I and Kwon.D.S, "Using mobile device screens for authentication", In Proceedings of the 23rd Australian Computer Human Interaction conference, OzCHI'11, ACM (NY, USA), pp. 50-53,2011.

[2]. A.D.Luca, M.Langerich and H.Hussmann, "Towards understanding ATM security: a field of real world ATM use", In Proceedings of the sixth symposium on Usable Privacy and Security, ACM: Redmond, Washington, pp. 1-10, 2010.

[3]. Panjwani.S and Cutrell.E, "Useably Secure, low cost authentication for mobile banking", In Proceedings of the sixth symposium on Usable Privacy and Security, SOUPS'10, ACM (Redmond, Washington), ACM ID: 1837116, pp. 4:1-4:12, 2010.

[4]. Kumar, K.Shailaja, G.Shailaja, A.Kavitha and A.Saxena, "Mutual authentication and key agreement for GSM", International Conference on Mobile Business (ICMB'06), pp. 25-26, 2006.

[5]. Zaslavskv.V and Strizhak.A, "Credit card fraud detection using self-organizing maps", Information and Security, pp. 48-63, 2006.

[6]. Z.Li, Q.Sun, Y. Lian and D.Giusto, "An association based graphical password design resistant to shoulder surfing attack", IEEE International Conference on Multimedia and Expo, China, pp. 245-248, 2005.

[7]. [7] Boyd.J, "Here comes the wallet phone", IEEE Spectrum.42, Vol.11, pp. 12-14, 2005.

[8]. Hamilton.D.J, Whelan.J, McLaren.A, MacIntrye.I, Tizzard.A, "Low cost dynamic signature verification system", IEEE conference Publication 408, England, pp. 202-206, 1995. [10] T.S.Messengers, E.A.Dabbish and R.H.Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks", IEEE Trans. Computers, Vol.51, no.5, pp.541-552, May 2002.

[9]. Furnell.S.M, Morrissey.J.P, Sanders.P.W, Stockel.C.T, "Applications of keystoke analysis for improved login security and continuous user authentication", Proceedings of Information Systems Security, pp. 283-294, 1996.