

GENERATION OF SECURE ONE TIME PASSWORD FOR ATM SECURITY AND THEFT PROTECTION

S.Pooranachandran¹, E.Aravind², D.Bharathipriya³, A.K.Gokul⁴,E.Karthika⁵,

Department of Electronics and Communication Engineering,

Velalar College of Engineering and Technology, Erode-12.

ABSTRACT: Automatic Teller Machines (ATMs) were originally developed as just cash dispensers, for bank related functions such as cash withdrawal, purchasing, etc. In existing system there is no security layer is implemented in the ATM card except pin number. It is very costly for the bank to include the fingerprint and Iris scanner. The main objective of the proposed system is used for security purpose and to detect the lost of ATM card through the SMS. This system proposes a one-time password (OTP) to the user's mobile number for further more 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.

Key terms: Automatic Teller Machine (ATM), One Time Password (OTP), Personal Identification Number (PIN).

I.INTRODUCTION

An embedded system is a combination of software and hardware to perform a dedicated task. Some of the main devices used in embedded products are Microprocessors and Microcontrollers .Microprocessors are commonly referred to as general purpose processors as they simply accept the inputs, process it and give the output. In contrast, a microcontroller not only accepts the data as inputs but also manipulates it, interfaces the data with various devices, controls the data and thus finally gives the result .Now a day's ATM plays a major role in every human's life in emergency situation for money withdrawal which is more complicated in earlier days because of queuing process. ATM allows a customer to make cash withdrawals, printing passbook and check account balance without the need for human teller. 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. It makes a financial losses of customer so there are chances of security threats in existing system like shoulder surfing, data skimming, card trapping. Now a days it is rarely happens that person having an ATM card but not having a mobile. The main purpose to use (one time password) OTP is for uniquely identify the mobile number registered by an individual on bank.

II. EXISTING METHODOLOGY:

There is no security layer is implemented in the ATM card except PIN number. It is very costly to include fingerprint and Iris scanner in normal transaction. ATM card falling into wrong hands, and the PIN number being cracked by a stranger. Then stranger can easily use the ATM card.

Functions involved in fingerprint reorganization:

- Fingerprint recognition: The masters' fingerprint information was used as the standards of identification. It must certify the feature of the human fingerprint before using ATM system.
- Remote authentication: System can compare current client's fingerprint information with remote fingerprint data server.
- Message alarming: different 4-digit code as a message to the mobile of the authorized customer without any noise, in order to access the Terminal.
- Two discriminate analysis methods: Besides the fingerprint recognition, the mode of password recognition can be also used for the system.

III.PROPOSED METHODOLOGY:

DISADVANTAGES OF EXISTING SYSTEM:

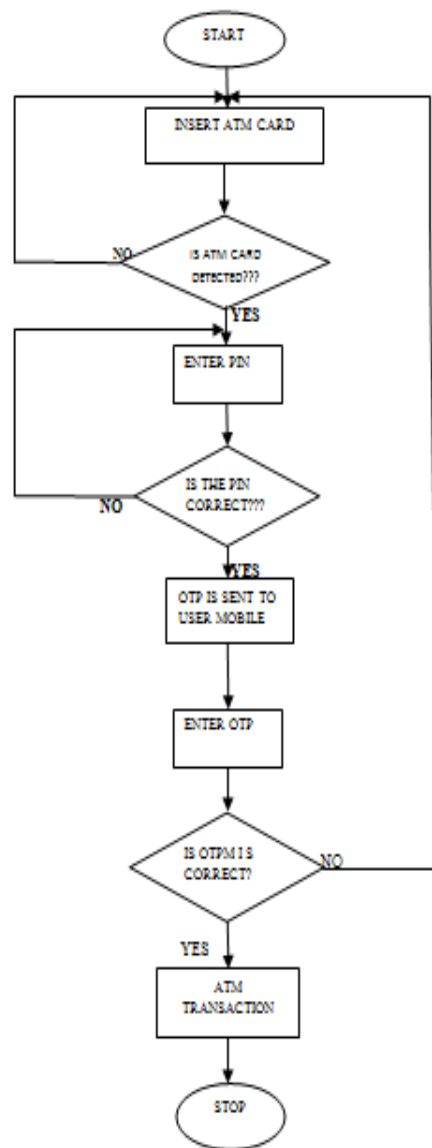
- Now a day there is no security layer available except pin number.
- In existing system (finger print based ATM transaction) maintenance cost is high.

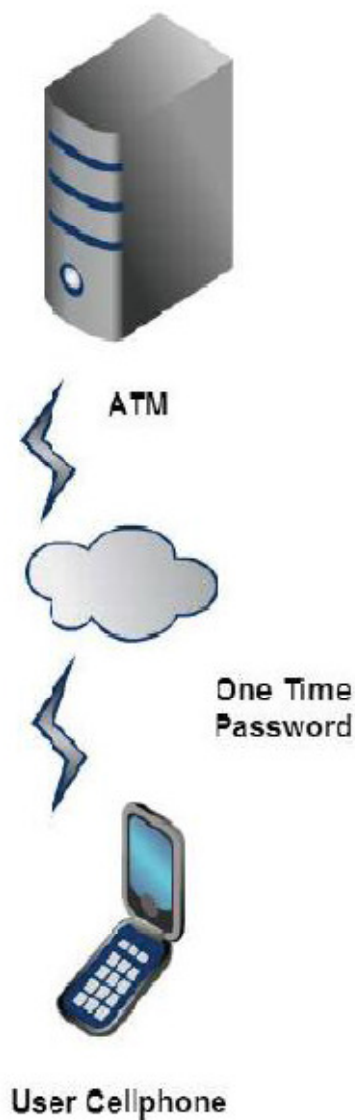
- And also it is not user friendly.

OBJECTIVE:

This project helps to overcome the problem of complexity and provides easiest way to secure the ATM transaction. Whenever person enters account number onto the ATM machine, the system requires PIN to authenticate the user. If the PIN number gets verified, the OTP is generated and sent to user's mobile number. The transaction will succeed only if the user enters valid OTP, otherwise transaction will fail. Again the user will repeat the above steps until valid OTP was entered. If the OTP entered is wrong more than a particular limit the card will be blocked. The flow diagram of existing system is shown in figure.

FLOW DIAGRAM:





ONE TIME PASSWORD:

If the user want to authenticate the transaction at any time ONE TIME PASSWORD is method more efficient one. OTP algorithm's security is very important because no one should be able to guess the next password in sequence. The sequence should be random to the maximum possible extent, unpredictable and irreversible.

Factors that can be used in OTP generation include names, time, seeds, etc. Several commercial two-factor authentication systems exist today such as RSA Secure ID.

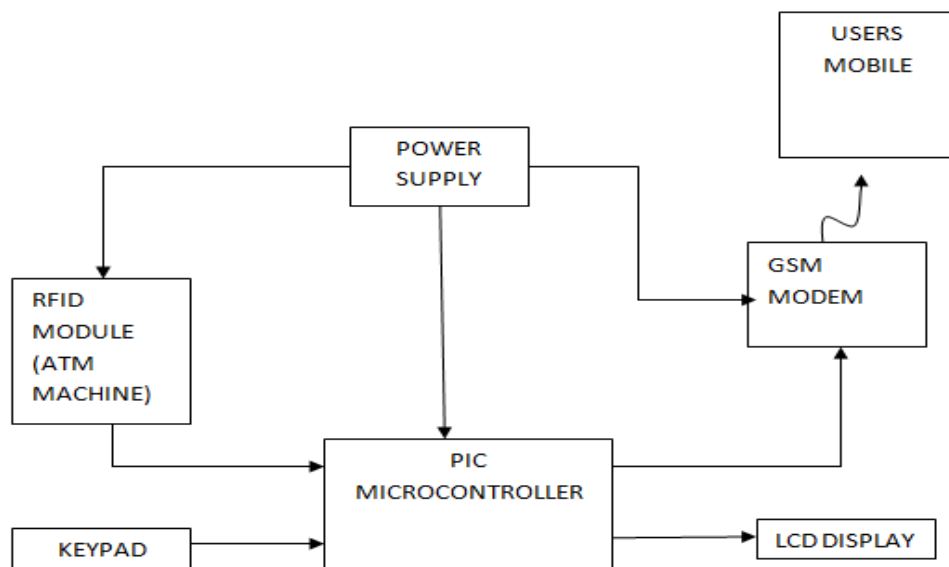
OTP has a advantages like a

- ☐ Smarter, more advanced security system to protect you and your money through ATM.
- ☐ OTPs are not vulnerable to replay attacks as they are valid just for a single login.
- ☐ Provides a stronger method for authenticating your ATM transactions.

- Acts as an extra level of protection should your Card Number and PIN be compromised.
- OTPs are generated at random and are valid only for a specific period of time, thus ensuring utmost security.
- SMS is the cheapest option to distribute OTP to the user.
- Delivering OTP to mobile phone is simple and secure, as the user carries the mobile phone at all times.
- There is no need for the user to carry an extra device, say a token, to view the OTP.
- SMS is familiar, has huge customer base and can reach almost every single user.
- SMS is available in all kinds of handsets.
- It's totally free, secure and easy to use.
- OTP through SMS effectively eliminates the need for users to create and maintain passwords and fails password-cracking efforts by phishers.

IV. BLOCK DIAGRAM OF PROPOSED SYSTEM:

IV.BLOCK DIAGRAM OF PROPOSED METHOD:



V.HARDWARE DESCRIPTION:

MICROCONTROLLER:

Microcontroller can be termed as a single on chip computer which includes number of peripherals like RAM, EEPROM, Timers etc., required to perform some predefined task. AVR is an 8-bit microcontroller belonging to the family of Reduced Instruction Set Computer (RISC). In RISC architecture the instruction set of the computer are not only fewer in number but also simpler and faster in operation. AVR microcontroller executes most of the instructions in single execution cycle. AVRs are about 4 times faster than PICs; they consume less power and can be operated in different power saving modes. Let's do the comparison between the three most commonly used families of microcontrollers. AVR follows Harvard Architecture format in which the processor is equipped with separate memories and buses for Program and the Data information. Here the proposed system uses the **PIC microcontroller**.

LCD:

A liquid crystal display (LCD) is a flat panel display, electronic visual display, video display that uses the light modulating properties of liquid crystals (LCs). LCs does not emit light directly. They are used in a wide range of applications, including computer monitors, television, instrument panels, aircraft cockpit displays, signage, etc. LCDs have displaced cathode ray tube (CRT) displays in most applications. They are usually more compact, lightweight, portable, less expensive, more reliable, and easier on the eyes. They are available in a wider range of screen sizes than CRT and plasma displays, and since they do not use phosphors, they cannot suffer image burn-in.

GSM MODEM:

GSM/GPRS module is used to establish communication between a computer and a **GSM-GPRS system**. **Global System for Mobile communication (GSM)** is an architecture used for mobile communication in most of the countries. **Global Packet Radio Service (GPRS)** is an extension of GSM that enables higher data transmission rate. **GSM/GPRS module consists of a GSM/GPRS modem assembled together with power supply circuit and communication interfaces** (like RS-232, USB, etc) for computer. The MODEM is the soul of such modules.

RFID MODULE:

Radio-frequency identification device (RFID) is the wireless non-Contact use of radio frequency [electromagnetic fields](#) to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered and read at short ranges (a few meters) via magnetic fields ([electromagnetic induction](#)). Others use a local power source such as a battery, or else have no battery but collect energy from the interrogating EM field, and then act as a passive transponder to emit microwaves or [UHF radio waves](#) (i.e., [electromagnetic radiation](#) at high frequencies). Battery powered tags may operate at hundreds of meters. Unlike a [bar code](#), the tag does not necessarily need to be within line of sight of the reader, and may be embedded in the tracked object.

KEYPAD:

Keypad is used to enter the characters or numbers to the system like a mobile phone.

VI.CONCLUSION:

Now a day's ATM security is a major problem in banking system. Now a day's security system used in ATMs is completely based on PIN security system which is vulnerable. Banks provide four digits PIN to the user which can be changed later by the user. After first use, user usually changes the password and keeps password quite guessable. This is the main drawback of this PIN type ATM system. When ATM card is lost or stolen it is required to close the ATM card by contacting the bank immediately. The paper indicates the strong authentication of ATM card with the help of One Time Password (OTP) on mobile device. So in this paper with

the help of Password authentication and OTP the system will be simple, cost-effective and security level will get increase in an ATM transaction.

VII. REFERENCES:

1. 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.
2. T. Phillips, T. Karygiannis and R. Kuhn, "Security Standards for the RFID Market," IEEE Security & Privacy, vol. 3, no. 6, pp. 85 - 89, Nov.- Dec.2005.
3. R. Weinstein, "RFID: A Technical Overview and Its Application to the Enterprise," IT Professional, vol. 7, no. 3, pp. 27 - 33, May - June 2005.
4. S.T.Bhosale, Dr.B.S.Sawant, "Security in E-Banking via Card Less Biometric ATMs", International Journal of Advanced Technology & Engineering Research, Vol.2, pp.9-12,2012.
5. R. Rasu, P. Krishna Kumar, M. Chandraman _Security for ATM Terminal Using Various Recognition Systems' International Journal of Engineering and Innovative Technology 4th October 2012.

