



## Enhancement of ATM Security and Theft Protection with the Use of One Time Password

Prof. (Dr.) Prashant P. Pittalia

MCA Department, SJPIBMCA,  
Gandhinagar, India

---

**Abstract** – In today's world Credit card fraud is a major issue. Financial institutions have registered major losses till today due to users being exposed of their credit card information. Card skimming, video recording with hidden cameras while users perform PIN-based authentication at ATM terminals are a common attacks in now a days. Researchers have struggled to come up with secure solutions for secure PIN authentication. In this paper, I propose a One Time Password (OTP) and Barcode scheme as PIN authentication protocol for ATM. This approach protects the user from shoulder-surfers and partial observation attacks, and is also resistant to relay, replay, and intermediate transaction attacks.

**Keyword** - PIN, One Time Password, ATM

---

### I. INTRODUCTION

Today as we all seen ATM has been used in our daily lives, as they are used for ease in transaction which was somewhat difficult in early times where there were long queues in bank for printing passbook, withdrawals money and depositing money. 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 Bank ATM card and PIN (Personal Identification Number) which user can change at any time through ATM machines. 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. Various Shoulder surfing resistant PIN entry methods have been proposed for secure PIN entry but they are not success in stop recording attack. Magnetic Stripe technology is most commonly used in which, when the person inserts his card into the card reader, the skimmer captures the card information with the help of skimming devices which is placed upon the reader, so various chances of skimming attacks has been seen. 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 of a mobile number registered by an individual on bank.

### II. AUTOMATIC TELLER MACHINE

An automated teller machine (ATM) is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space. With the use of an ATM, customers can access their bank accounts for cash withdrawals and check their account balances. Nowadays Automated Teller Machines is considered as very common technology for dispensing notes to cash-holders. The ATM structure for cash withdrawal differs across countries. The first ATM was installed in the USA in 1969. ATMs have a positive effect on the nominal currency growth, but this effect is not very robust. Among all services of bank ATM is consider as more profitable service because it attract number of non-bank customers. The structure of ATM comprise on main components such as CPU, magnetic chip card, PIN pad, Secure crypto processor, function keys and vault. Since the introduction of the first automated teller machine (ATM) in 1967, perpetrators have been devising ways to try to steal the cash inside. Because ATMs eliminate the need for round-the clock human involvement and tend to be located in places that make them more vulnerable to attack, they are often attractive targets for perpetrators. ATM crime is not limited to the theft of cash in the ATM. Many ATM attacks seek to obtain a consumer's personal information, such as their card number and personal identification number (PIN). While these types of identity theft attacks take more effort to net cash for perpetrators, the result is the same—illegally obtaining money. According to estimates by Retail Banking Research, there are more than

2.2 million ATMs deployed worldwide. This is a figure forecasted to exceed 3 million by 2016. As the number of ATMs in use increases, so do the frequency and sophistication of security threats, making the development of fraud prevention measures a top priority for financial institutions (FIs) and ATM manufacturers. ATM fraud is not confined to particular regions of the world. To further complicate matters, perpetrators and victims are often on different continents, and the problems of one region can quickly become the problems of another.

### **III. IMPORTANCE OF ONE TIME PASSWORD**

In currently, withdrawing money from an ATM machine uses two factor authentication: the ATM card (what you have) and the personal identification number (what you know). Passwords are known to be one of the easiest targets of hackers. Therefore, most companies are searching more ways to protect their customers and employees. Biometrics is known to be very securing, but is used only in special organizations given the expensive hardware needed and their high maintenance costs. As an alternative, banks and companies are using tokens as a way of two-factor authentication. A token is a physical device that generates passwords needed in an authentication process. Tokens can either be software or hardware. Hardware tokens are small devices that can be easily carried. Some of these tokens store cryptographic keys or biometric data. Anytime a user wants to authenticate in a service, he uses the onetime password displayed on the token in addition to his normal account password. Software tokens are programs that run on computers and provide a onetime password that it is changed after a short amount of time. 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.

The OTP system generator passes the user's secret pass-phrase, along with a seed received from the server as part of the challenge, through multiple iterations of a secure hash function to produce a one-time password. After each successful Authentication, the number of secure hash function iterations is reduced by one. Thus, a unique sequence of passwords is generated. The server verifies the one-time password received from the generator by computing the secure hash function once and comparing the result with the previously accepted one-time password.

### **IV. BENEFITS OF ONE TIME PASSWORD**

When you need to perform an ATM transaction, you will be required to enter an OTP as a second level of authentication to confirm that the transaction is authorized by you. This OTP can be delivered to you via SMS, generated through the Bank mobile app or Bank Token. You will only need one OTP per session.

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.

### **V. FLOW CHART OF PROPOSED MODEL**

The existing system based on card or pin based security system. There are some disadvantages of existing system. Because sometimes card could be lost or stolen and pin could be easily hacked or forgotten. But the proposed System based on GSM security. in this system first the person enter use name and password if the User name and password matches then send the code on person mobile through GSM and ask for code on ATM if this code matches then the Transaction is performed. So the proposed system is more secure than existing system. The generalized flow chart of proposed system is shown below.

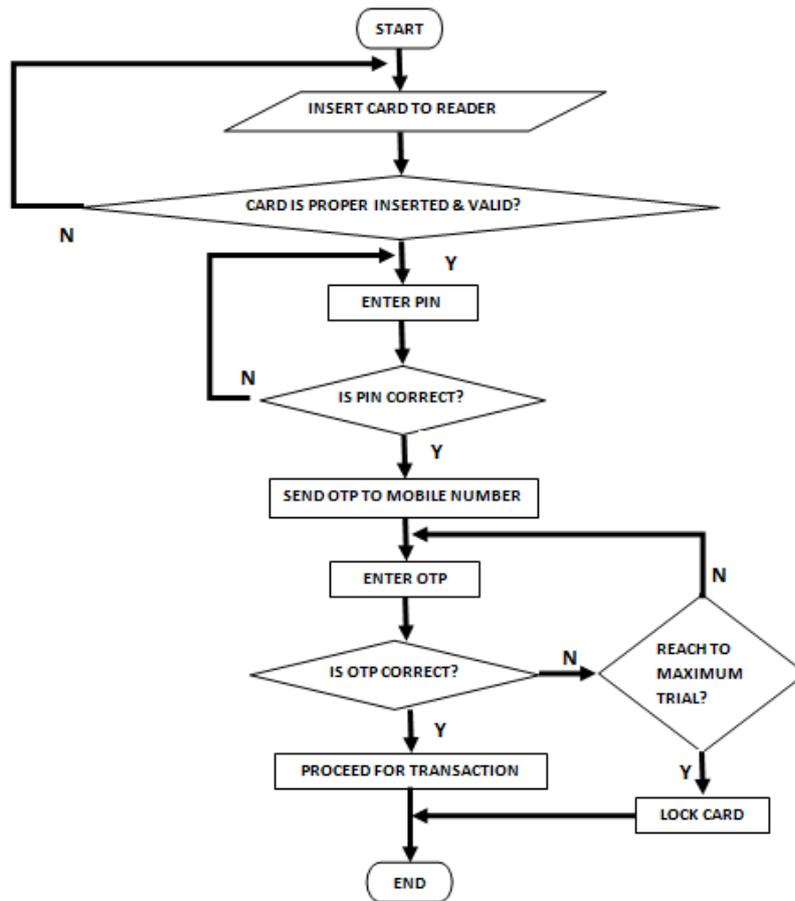


Fig. 1 Flowchart of proposed model

## VI. CONCLUSION

According to latest scenario ATM fraud is a very grave problem for banks. This project leads to establish authentication results which can be used by banks as well as various organizations. 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, as cell phone number is unique to every user. The method used in this paper is of significant use. As a result of the work proposed there will be benefit to human beings for the purpose of ATM security.

## 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] M.Ajaykumar, N.BharathKumar, "Anti-Theft ATM Machine Using Vibration Detection Sensor", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.3, pp.416-418,2013
- [3] Mun - Kyu lee 'Security notations and advanced method for human shoulder- surfing resistant PIN entry' *IEEE trans. on information forensics and security*, vol. 9, no. 4, April 2014
- [4] 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
- [5] [www.atmsecurity.com](http://www.atmsecurity.com)
- [6] <https://www.eurocontrol.int/articles/atm-security>
- [7] <http://www.rbrlondon.com/events/security>
- [8] <https://www.3sisecurity.com/industries-solutions/industries/atm/>