*International Journal for Modern Trends in Science and Technology*, 8(11): 87-89, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0811014
Available online at: http://www.ijmtst.com/vol8issue11.html

# Security in Bank ATM PIN System

**Vishnu J Nair**

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

**To Cite this Article**
Vishnu J Nair. Security in Bank ATM PIN System. International Journal for Modern Trends in Science and Technology 2022, 8(11), pp. 87-89. https://doi.org/10.46501/IJMTST0811014

**Article Info**
Received: 12 October 2022; Accepted: 02 November 2022; Published: 11 November 2022.

## ABSTRACT

***This research paper is about how secure are bank ATM pins are. Are they safe? and how can it be bypassed by using different sort of attacks from a hacker's end. It will also be suggesting different ways by which we can secure the system along with which we can make safe transaction. Based on data collected from different sources it will be providing details different adaptive measures that we can take to stop fraudulent transaction.***

***KEYWORDS : ATM, Pins, Two Step Authentication, Attacker, OTP, UPI, Biometric Authentication.***

## INTRODUCTION

In 2020 the amount Cyber-crimes sky rocketed after the world started facing COVID-19. One of the main reason for this is unemployment and monetary crisis that followed the pandemic.

Several people lost their money in countless ways. One on this was ATM card frauds. Hackers came up with new ways to hack into people's data. Our system are getting more vulnerable for attacks, so are ATM machines. Most ATM scams involve criminal theft of debit card numbers and PINs from the innocent users of these machines. One of such scam occurred in Gurgaon on November 27th 2021 where fraudster swiped out 2.24 Lakhs from 22 customer's bank account by replicating their card and withdrawing money from the ATM. This occurred in a nationalised bank in Gurgaon. The scammer was able to withdraw money without customers sharing them any info. This whole fraud took place within 3 hours, wherein 29 transactions were done.

Similar case occurred in Bhandup on September 17th 2022 where 2 cousins used same method of duping ATM and looted 2.58 lakhs.

There is one thing common in both of these attacks, the attacker was able to easily withdraw money just by entering victim's PIN which is easy to obtain.

All of these things are inevitable but we can always have a preventive measure to safeguard our money and bank details, which will be further discussed in this research paper.

## HISTORY OF ATM

According to history.com the First ATM was built in September 2nd 1969 for Chemical Bank in USA. It was designed to dispense a fixed amount of money in exchange for inserting a specially encoded card in it.

During the time it was introduced there were no pin system. The Owner of the card can use it by just inserting the card in the machine. Soon did the people started exploiting this thing and banks have to come up with the **Personal Identification Number** (PIN system). The

inventor of ATM **John Shepherd-Barron**Designed pin system which comprised of unique 6 digit PIN. Although his wife could only remember 4 digits hence the 1st generation of pin was only four digit long.

ATM was considered to be one of the safest method to withdraw cash until 1st ATM fraud occurred in Manchester in the year 1993. A criminal gang called Buckland Boys install the fake ATM in a shopping mall in Manchester City. This ATM was designed to collect card details and PINs from the user. This shows how easy it is to steal your card details and PIN.

**HOW DOES ATM PIN WORK?**

When the person inserts his/ her ATM card in the system it fetches all the essential details like account number. After this it enables us to choose the actions like withdrawing cash, changing PIN etc. While withdrawing cash it requests the user for PIN. The PIN is usually 4 digit number. An attacker usually finds your pin using Brut Force Attack and compares it with the hash-code in the database. Security of a pin can be calculated by calculating the number of attempts it will take to crack the code. The probability of crack 4 digit pin is 1 in 10^4 i.e. 1/10000. We can increase this by 100x by just adding 2 more digit to the existing pin. This will make a probability of 1 in 10^6 i.e. 1/1000000. But this don't solve our problem completely.

A good computer can easily go with each and every permutation combination and help the attacker to find your PIN.

**HOW TO STOP AND PREVENT SUCH ATTACKS?**

By examining the general pattern of attack we can understand that the main vulnerability is not authenticating the user. And the hackers usually exploit this.

There are multiple methods that we can used to authenticate the user. Some of them are:

- Adding Multi Factor Authentication
- Biometric Authentication
- Card-less Withdrawal of Cash

Let's see how these methods can be implemented.

**IMPLEMENTING MULTI FACTOR AUTHENTICATION**

Multi factor authentication is one of the commonly used authentication methods. In this method the user receives an On Time PIN (OTP). An OTP is a random unique PIN which is generated for a particular session (transaction). Hacker can replicate the card and pin but they can't bypass OTP unless the user (Victim) provides them the OTP.

This system is already in use within UPI transaction securing it way better than the traditional PIN system.

**IMPLEMENTING BIOMETRIC AUTHENTICATION**

Biometric authentication as the name suggests uses some part of your physical makeup to authenticate you. This could be done by installing various types of scanning devices within the ATM. The new model ATM's are already loaded with fingerprint scanners which could be put into use for authentication purposes.

Another way of biometric authentication includes iris scanning. In this method an iris scanner is installed in the ATM machine which fetches the image of our iris and authenticate the user.

**DRAWBACKS OF BIOMETRIC AUTHENTICATION**

As you know in biometric authentication we need to install particular scanners within the ATM. We also have to collect more information about the users such as their fingerprints and their iris image in order to authenticate them which will cost us lots and lots of resources and data.

**IMPLEMENTATION OF CARD-LESS WITHDRAWAL OF CASH**

As we all know India is leading towards cashless payments (transactions). But we still relay on the old traditional method of withdrawing cash using ATM card.

According to the survey conducted by RBI almost 80% off Indian citizens how a bank account but only 65% of them own a debit card out of which 22% are females and 43% are males. This means 35% of bank users don't have ATM cards.

A QR based Transaction system can be introduced in which the user can withdraw cash by making UPI payments to the bank.

This can make it easier for people to withdraw cash without using cards. This system is quicker, safer & eco-friendly compared to rest of the methods.

## CONCLUSION

The answer to the question whether our ATM pin are safe is that they are not. There are certain vulnerabilities in authentication of the user that needs to be fixed. This could be attained by implementing any of the three methods suggested. But these are no permanent remedies as Attackers (Hackers) evolve with technology and they always finds a way to break the system and breach within the system. But as of now the following methods are enough to stop Fraudsters from making fraudulent transactions using ATM.

### Conflict of interest statement

Authors declare that they do not have any conflict of interest.

## REFERENCES


[1] https://www.drasintrisk.com/post/emerging-challenges-automated-teller-machine-atm-frauds#:~:text=The%20first%20recorded%20instance%20of,shopping%20mall%20in%20Manchester%20city

[2] https://indiaforensic.com/atmfraud.htm

[3] https://www.mid-day.com/mumbai/mumbai-news/article/mumbai-cousins-held-for-looting-rs-2-58-lakh-from-atm-23247364

[4] https://www.business-standard.com/article/finance/80-of-indians-now-have-a-bank-account-so-why-is-financial-inclusion-low-118051700150_1.html

[5] https://www.nabard.org/auth/writereaddata/tender/1608180417NABARD-Repo-16_Web_P.pdf