ATM System with OTP Authentication

Aditi Badnore[*1], **Umarani C.**[*2]

[1,2]*Department of MCA, Jain University, Bangalore, Karnataka, India.*

aditibadnore@gmail.com

Abstract—*In today's date money is an essential thing to be carried out whether it is shopping, travelling or any health emergencies. But, at the same time it gets annoying when you need to carry huge amount of cash in your pockets. This is where ATM is important. Bank has provided ATM machines which can provide money anywhere you want. ATM is an easy way for withdrawal of money, just need to insert the card and enter the pin, after that the transaction proceeds. But what if someone will keep your card and somehow, he/she will know your password, it will grant him/her full access to your money. That raises question on present security and demands something new in the system that can offer second level of security. One-time password (OTP) is password that authenticates an authentic user for only one login to the respective system. This paper gives the new method towards the security of Automatic Teller Machine (ATM) system.*

Keywords**:** *ATM, OTP, Security, System*

I. INTRODUCTION

Usual ATM systems do not contain the OTP feature for money withdrawal. The ATM consists of Card reader, Keypad, Display screen, Speaker, Receipt printer, Cash Dispenser.

- Card Reader. Its purpose is to store all the account information through a magnetic strip which is present at the backside of the card. The data retrieved is passed on to a host processor, which in turn is able to interpret the information and retrieve the customer's account information.
- Keypad. This allows users to give an input in the system. It can PIN or any type of transaction a user wants to do. It only consists of numbers/digits which is only used to enter the pin.
- Display screen. Allows users to view what transaction they are carrying out.
- Speaker. Speaker allows additional information or directing voice from the system regarding the transaction the user is processing.
- Receipt printer. It allows users to give a printed receipt of the transaction, which can include amount withdrawn, account number, account balance, name of the user etc. It is advisable not to ask for printed receipt or tore it out once completed.
- Cash dispenser. The main purpose of an ATM is for a user is to acquire cash; therefore this is the most important part. The cash dispenser is a pivotal part and a part that is highly sophisticated.

OTP is a system-generated numeric string of characters that authenticates the user for a single transaction. Once you enter the amount that you wish to withdraw, the ATM screen will display the OTP screen. If an attacker manages to get hold of ATM card/Account number and the pin number he may easily use it to withdraw money. Firstly, the user will be asked with account number and ATM pin, after that the user will receive an OTP on his registered mobile number. After entering the OTP, the user will be asked for withdrawal or deposition of money. If he wants to withdraw money, the OTP will be verified then only further transaction can take place. Thus our system provides a totally secure way to perform ATM transactions with security structures. To overcome the security, this paper proposes second level security for ATM systems. An ATM is an IT enabled Electro-mechanical system that has connectivity to the accounts of a banking system.

II. LITERATURE REVIEW

In recent years, bank crimes are seen worldwide, this is not only a loss for customers but also for the bank operators. Lot of criminals tamper ATM cards and get access to the customer's credentials by some illegal means. Once the ATM card is lost and the pin is stolen, the attacker can easily get access to the user's account and vulnerability of attacking increasing. Despite warnings people choose to keep their pin guessable like their birth days, vehicle numbers etc., in such case OTP (One Time Password) plays a major role where the OTP will be sent to user's registered mobile number which won't be accessible by the attacker. The One-time password (OTP) system security is very important because no one should be able to guess the next password in sequence. The sequence should be random to maximum possible extend, unpredictable and irreversible. The OTP approach entails the user to use different password for each login it is widely accepted for two factor authentications. The otp system generator passes the user secret pass-phrase along with a seed received from the server as part of the challenge through multiple iterations of secure hash functions to produce a one-time password. After each successful verification, the number of secure hash function iterations is reduced by one. Thus, a unique sequence of password is generated. The server validates the one-time password predictable from the generator by calculating the secure hash function once and comparing the result with the previously accepted one-time password. The OTP principle highlights that each time the user tries to login, the algorithm produces pseudorandom output, thus improving the security. An OTP is a password that is only valid for a single login or a single transaction.

III. EXISTING SYSTEM

The ATM allows users to complete basic transactions without any use of bank operators. When a user inserts the card and enters pin there is no other level of security seen. In case, the card is stolen and the pin is cracked by any attacker by means of shoulder surfing, mutual friends, family etc. once he gets access to it there is no means anyone can stop him from stealing money from the bank. Existing ATM system is not the safest system for the most important asset of human being i.e. Money. There is a necessity of some new system which is easy to adapt and more secure.

IV. PROPOSED SYSTEM

The objective is to deliver second level security to the ATM systems, which can be done through OTP (One Time Password) which is secured and trusted way to add security to the systems. The OTP would be sent to user's registered mobile number which would be present in the database. This systems provides safest way to do ATM transactions. Whenever person enters account number onto the ATM machine, the system needs 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. If the OTP entered is incorrect more than a particular limit the card will be blocked. At the period of opening account, the bank system will ask about mobile registration of the mobile number of the user. This information will be kept in the bank database for further reference. When User goes to any ATM machine, he/she has to swipe card to machine after that machine and bank server will check validation and authentication of that card, if card and its information is accurate machine will ask the PIN of the user. That card detail and PIN will be confirmed on the banking system. After verification of the card owner and PIN, system will access the user details from database and generate the OTP that will be further send to the mobile number of the user. When user gets OTP code on mobile, he/she has to enter that code on the screen in similar way as PIN. But here unintended problem arises for example dead battery of mobile, no network coverage or delayed SMS delivery. If entered OTP is accurate then ATM system will allow access to user for transaction.

OTP adds next layer of security beyond pin. OTP generation algorithms typically make use of pseudo randomness or randomness, making a prediction of successor OTPs by an attacker difficult, and also cryptographic hash functions, which can be used to derive a value but are hard to reverse and therefore attacker cannot retrieve the data that was used for hash. This is necessary because, it would be easy to predict future OTPs by observing previous ones.

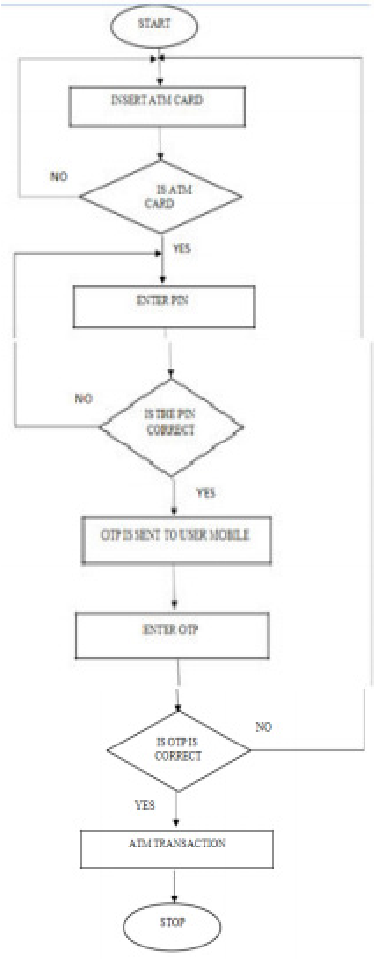

Fig: Flowchart

V. OTP WORKING

For any bank transaction OTP is considered as most efficient way to do so. It is efficient because no one will be able to guess the OTP received on user's mobile number. The OTP can be any random number sent by the bank to the user which is not easily crackable by any hackers.

i. OTP Working-

An OTP is a 4-digit number received on a user's registered mobile number with the bank. OTP is preferred over an email because people staying in rural areas use simple phones, where internet connection may not be available and email facilities won't be available in some areas. The user will receive an OTP immediately after the pin verification. User needs to enter that 4-digit OTP into the system, if correct it will move on for the transaction process. If not, the system will give only 3 chances for the user to enter the OTP even after 3 attempts the OTP is incorrect the system will block that particular account and the notification will be sent to user's registered mobile number.

ii. Advantages of otp-

- SMS is easily available on any mobile devices.
- Acts as an extra security layer to protect your money in the bank.
- SMS is a cheapest option than any other alternatives.
- They are totally free and secure to use.
- SMS can easily reach users in any area.
- No need to carry any extra device, for example a token.
- Provides a stronger method for authenticating your ATM transactions.

iii. Limitations of OTP-

- Delay in Delivery
- Coverage areas/unavailability of service
- Unavailability of devices
- Susceptible to real-time replay and social engineering attacks

VI. FUTURE SCOPE

In this Paper, we are dealing with ATM System with OTP System for withdrawal of cash from account. Future scope can be face recognition or Iris recognition to withdraw cash for more security. System when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines.

VII. CONCLUSION

Nowadays, ATM system is a key problem due to security issues and can be vulnerable too. Banks deliver four digits PIN to the user which can be changed later by the user. After first use, user generally changes the password and keeps password quite guessable. This is the main disadvantage of this PIN type ATM system. Use of OTP is best and easy way to deal with these security threats. That OTP will be transfer on registered mobile number of the user. And that OTP will be used toward access ATM transactions. Another significant point in proposed system is that it demands lesser changes to the present system of Bank and ATM. That means minor overhead will be required to change the whole system with enhanced security.

VIII. REFERENCES

[1] Sruthi. M; S. M. (2019). Secure and Smart Future ATM with One Time Password. *IJESC*, 1-3.

[2] Aruna R; Sudha V; Shruthi G; Rani R; & Sushma V. (2018). ATM Security using Fingerprint Authentication and OTP. *IFERP*, 4.

[3] Parag Achaliya; Govind Bidgar; Hrutika Bhosale; Prasad Dhole; Kajal Gholap. (2021). Securing ATM using Face Recognition Authentication. *Ijaresm*, 8.

[4] Mr.S.Vijay sarathi; S.Akash; I.Nihilkumar; M.Nirmal; M.Muthukumaran.(2019). A Novel Methodology Of Integrated ATM Security. IJIRT, 7.

[5] Leslie Lamport. (1981) Password Authentication with Insecure Communication Communications. ACM 24.11, 4

[6] G.Jayandhi; S.Elphin Samuel; A.Govardhan; A.Logesh; A.Vishnukumar.(2018). Secure Pin Authentication as a Service for ATM. IJAREEIE, 7.

[7] Shivam Kumar Rajput; Aniket R. Patne; Amit Varma; Girish Vishe. (2019). Enhanced fingerprint recognition and OTP to improve ATM Security. IJARIIT, 4.

[8] Shyamsundar Bhairam; Deepak Agrawal.(2019). Method and System for Performing Card Less Cash Money Withdraws in ATM Machine. IJMERT, 4.

[9] Bodagoddu Sharath Chandra Kumar; Jally Venkatesh. (2020). A Paper on Enhanced PIN Security for SBI ATM through Aadhaar Linked OTP or Biometric. IRJET, 5.