ATM Cloning and Skimming

Vaibhav Srivastava [1], Dr. Devesh Katiyar [2]
[1]Student of MCA,[2]Asst.Professor
Department of computer science

DSMNRU

Lucknow, Uttar Pradesh.

Abstract:

In this modern era,the way society handles and performs major transactions has been changed completely. The world is going towards digital arena resulting in the increased use of ATM cards.With sudden upsurge in use of e-transactions,many fraud transactions are also on rise with each passing day. ATM skimming has become a normal problem. Thisresearch paper gives a general answer for financial fraud done by false ATM card.

Keywords:*ATM,ATM skimmer,card-cloning,OTP (one-timepassword).*

I. Introduction

A Debit/Credit card has amagnetic strip which contains the personal and banking details of cardholder. Security of the cardholder's privateand financialinformation can easily be compromised by tricking the user. Cloning of debit card is a big Problem. Criminals create a duplicate copy of ATM Card containing same details. Pin capturing is a next problem.Most of the times, Fraudsters gets access to the cardholder's PIN by hidden camera placed on the keypad panel of the ATM. Later these details are usedfor makepurchasesor other wrong activities without the real cardholder's knowledge.Therefore, it is required to maintain the protected, dependable and trust-worthy electronic transaction. Thispaper is proposed to reduce ambiguity and increase authenticity & confidentiality.

II. Starting of an ATM Era

Any normal card issued by the banks for withdrawing money is known as ATM cards.Sometimes it is also called as Cash cards, moneyaccess cards, bank cards etc. These cards have a great importance in financial area. During late 1960s, John A. Shepherd - Barron gave asolution aboutcash providing machines.The idea was accepted by a London Bank and anATMwasestablished at the bank's local branch.

*Uses of ATMs***:**

. There are some uses of ATM as follows-

- The life of the normalpersonhas become easy because there is no need tostanding long
queues for money withdrawal.
- It is easy to get information of balance in the bank account.
- The ATM services are available for 24*7 to their customers.
- You can deposit, withdraw, and fund transferanytime from the ATM.

However, there are number of other services given by the ATMs, but cash dispensingis mostly used service of all.

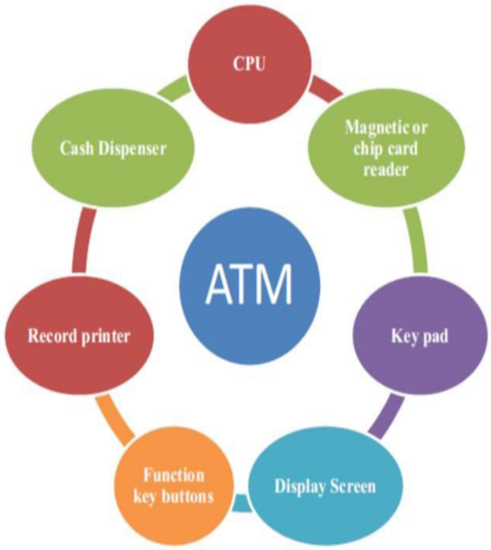
III. Components of ATM

A. The Hardware of the ATM:

- ***CPU:***To monitor the whole process and the transaction devices. It is the main part of the machine.
- ***Card Reader****:*To read the detailsof the card.
- ***Keypad****:*To interact and communicate with the Software. Also, use for input the pin codes.
- ***Display screen****:*To see the entire process of the transactions.
- ***Speaker****:* To hear the actions that aredone on the display screen. Generally, it is enabled in ATM.
- ***Receipt printer****:To* provide the details of bank balance on paper. Mostly, processes involved inATM transaction are digital, however, some may require mini statement as a hard copy.
- ***Cash dispenser***: To dispense the cash.It is paramount for anyATM.

B. The Software of the ATM:

Mostof the ATMs works onWindowsOS, fundamentally *Windows XPProfessional*or*Windows XP Embedded*. Some ATM are still running on earliertype of WINDOWS OS such as Microsoft WINDOWS 2000 or Microsoft WINDOWS NT.



IV. What is ATM Cloning?

Today, people are so much aware ofadvanced technology. ATM cloning is basically a process in which cloning is done in such a way that all the essential data saveon the user's card is copied and used for committing transactions using fraud transactions by the attacker.

In this process, a device which appearssimilar toATM's part is attached to the ATM that collectsthe card details. This device is known as skimmer. When user slide his card into the ATM that has Skimmer attached the card gets cloned and information is compromised.

V. Types of ATM Cloning

Broadly, ATM cloning is of following two types-

1. The first type includes the one in which skimmers are used to scan the data placed on the cards.

2. In second type of ATM cloning, asemi-operational,used ATM which generallycan't dispense the cash is attached to record the **information**, and placed in ATM machine.

VI. Existing Model

Skimming is a method by which a fraudstercan capture all your personal informationstored in the magnetic strip of an ATM Card. Skimmer device is fixed in ATM, whenever the ATM card is enteredin the ATM debit/credit card information gets copied and skimmed. To acquire the full access of the customer's account, not only card no. is required but also the PIN Code is required. So,a spy camera is also placed in such a way that it focusses on the keypad of the ATM.

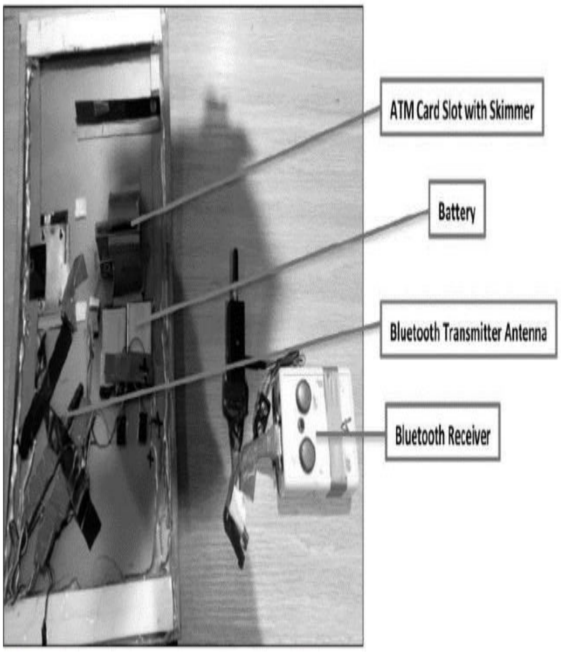


Fig1. Underside of ATM overall

The cloning ofcard takes place without cardholder's knowledge. Persongets to know about the committed transactions when they get the statement of transaction from the bank about their account balance.

For past few years,Banks strictly follow the authentication procedure for electronic transaction.

A PIN is a security password of digits.Unfortunately, an ATM PIN is a combination of numerical digit only as it uses a limited number of keys to operate.

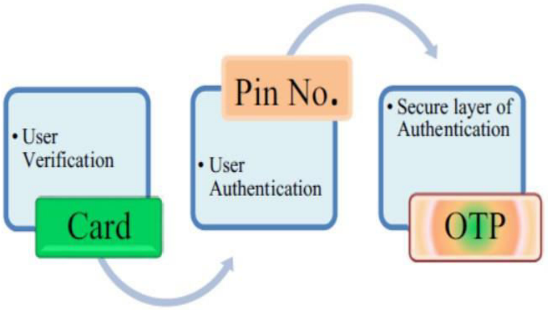
A **magnetic strip** fixed on the ATM cum debit card which holds some information about the user such as his Account details suchas PIN, IFSC code etc. After insertion of card in provided card slot, If the card is found valid, the ATM prompts for the PIN. If the entered PIN is correct, the card holder can proceed for further transaction.

Pseudocode for current ATM transaction

```
1. Insert card into an ATM machine.
2. POP-UP input field to check (for human being).
3. Choose language.
4. Enter PIN no.
5. Prompt for choose A/C type
6. Select the activity choice
7. Enter the transaction amount
8. Receive transaction amount
```

VII. Proposed Model

This paper provides a new security feature which is OTP(One TimePassword). Simple ATM card and PIN number are not sufficient for the security purposes. So, it is mandatory to include OTP feature of ATM security feature is totally new for ATM withdraw.



:

Fig2. Securelayer transaction Mechanism For ATM

OTP is secured layer of ATM transaction that increases the security in terms of both authorization/authentications. OTP could be received onmobile number registeredwith user's bank account. In case, ifhacker tries to use cloned card then the probability of withdrawing money is low.

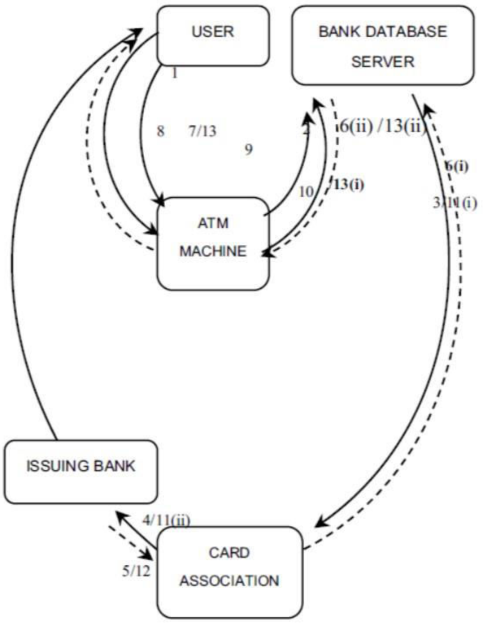


Fig. 3: Secure layer transaction Model of ATM

A. **Secure layertransaction Model: -**Itcan be described as-

1. Card holder uses ATM card as a payment mode.
2. After swiping of card & entering the PIN, machine sends all the necessary details to the bank database server.
3. These detailsare sent to the card-association by bank server.
4. Then association sends these details to the associated bank for authorization.
5. The bank that has allotted thatATM card, does the validation of the details of the customer for the transaction.
6. Card association checks whether the request id coming from authenticated bank server or not.If the authentication is successful, details aresentwithout delay.
7. ATM machine notify to collect the withdrawal money.

If conditions fulfilled for generating OTP then-

8. Bank generates the OTP and sends to user.
9. User manually enters the OTP.
10. ATM machine sends the details to the Bank server.
11. These details are sent to the bank for the validation of OTP.
12. The bank validates the OTP to the card association.
13. Card associationthen validates the bank server which is finally transferred to the ATM machine.
14. Transaction procedure is completed.

For OTP, a mobile no. should be registered in the user's bank. The bank needs to declare a threshold limit for OTP. Suppose the threshold limit is Rs.5000, then two cases arise-

CASE 1)OTP for first transaction for an amount-

- Transaction is true; withdrawal amount is RS.5000.
  No OTP is required.
- Transaction is true; withdrawal amount is RS.3000.
  No OTP is required.
- Transaction is true; withdrawal amount is RS.10000.
  OTP required because amount is greater than threshold limit.

CASE 2) OTP for second transaction for an amount-

If card details and PIN no. are true then transaction process begins. Threshold limit for OTP is verified for OTP transmission.

- Transaction is true; withdrawal amount is Rs.5000.
  No OTP is required.
  In first condition, withdrawal money is under threshold limit.
  OTP will not be transmitted.
- Transaction is true; withdrawal amount is Rs.10000.
  OTP is required.

If cardholder wants to do second transaction, he crosses his threshold limit i.e. Rs 5000 and exceeds by Rs. 10000(5000+10000=15000). Now withdrawal amount is greater than threshold limit i.e. Rs.5000.OTP will be send here.

VIII. Advantage

By using this security approach, banks can reduce fraud transactions, ATM cloning and skimming. It could provide better risk management. It could increase theloyalty and self-confidence of card-holder.

IX. Limitations

This methodology is not completely feasible in context of time and availability of mobile network. Here after, network complexity could be reduced and user-friendly environment could be developed.

X. Conclusion

The ATM transaction is playing a very crucialrole in our daily life. Basically, the authentication and authorization processare based upon credit /debit card and PIN which is not that much reliable. So, we need a better solution of processing the transaction so that the user's hard earn money is safe.

Therefore, anOTP based transaction mechanism is proposed here. So that card-holder feels safe and comfortable while using ATM card. Hence, there will be a greatlevel of a self-confidence in user while committing the transaction from ATM.

XI. References

1. G. Bond, Mike, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, and Richard Anderson, "Chip and Skim: cloning EMV cards with the pre-play attack", In Security and Privacy (SP), 2014 IEEE Symposium on, pp. 49-64. IEEE, 2014.

2. Card skimming theft [online] Available http://www.identitytheft.info/credit-card-skimmerpictures. aspx.

3. ATM Card Skimmers, Debit Card Skimmers and Credit Card Skimmers images http://www.banking.org.za/consumerinformation/ bank-crime/card-skimming-theft

4. Barker, Katherine J., Jackie D'Amato, and Paul Sheridon. "Credit card fraud: awareness and prevention." Journal of Financial Crime 15, no. 4 (2008): 398-410.

5. Law, Eric Chun Wah, and Lap Yam. "Single onetime password token with single PIN for access to multiple providers." U.S. Patent Application 11/376,771, filed March 15, 2006.

6.Skimming the surface, a research paper by Dr. Darren R. Hayes of Pace University sponsored by ACCA USA February 14,2014.