Double Authentication In ATM Machine To Prevent Fake ATM Machine Fraud

Darshan Bodawala, Pradeep Laxkar

Abstract—Today, ATM has become an irreplaceable channel between the bank and its customers. On the other hand nowadays ATM skimming are increased. The biggest skimmers of all is FAKE ATM MACHINES. This paper is hoped to describe a general picture of ATM crime. When someone uses this fake ATM machine they got failure message for their requested transaction but the ATM card information and the PIN are stored in that fake machine. In this paper the mechanism is described by which authentication of the customer and the machine both are done and by which customer can recognize that whether the ATM machine is fake or real. So, by applying this method we can prevent the fake ATM machine attack.

Index Terms—Fake ATM, RSA, PIN, ATM Card, ATM, Skimmers, Skimming, Fraud, Double Authentication.

IJSER

I. Introduction

What Is ATM (Automated Teller Machine :
An electronic banking outlet, which allows customers to complete basic transactions without the aid of a branch representative or teller. There are two primary types of automated teller machines, or ATMs. The basic units allow the customer to only withdraw cash and receive a report of the account's balance. The more complex machines will accept deposits, facilitate credit card payments and report account information. To access the advanced features of the complex units, you will usually need to be a member of the bank that operates the machine [2].

Different Attacks On ATM Machine:

Card skimming:

Magnetic card information details are compromised by a disguised card reader known as skimming device which is normally installed in front of card reader entry slot or some ATM room-door lock. Skimming is by far the most popular method of ATM network attack, accounting for over 80% of ATM fraud, or around $800 million in 2008 full year. The main reason makes it popular is high ROI (Return On Investment)
from this attack. After Card Skimming, skimmer makes duplicate card and tries to draw money from it [1].

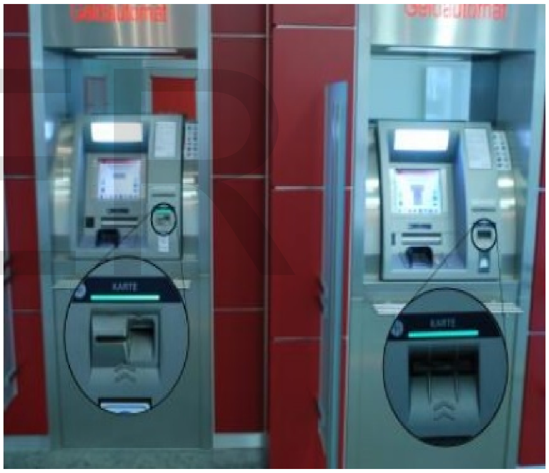


Fig. 1 Comparison between skimmed slot and real slot

Card trapping :

Trap or jam the card by placed wire, tapes or other mechanism in the card entry slot. The thieves have used techniques such as the “Lebanese loop”, a plastic strip they insert into the cash machine to capture bank card [1].

A **Lebanese loop** is a device used to commit fraud and identify theft by exploiting automated teller machines (ATMs). In its simplest form, it is a strip or

- *Darshan Bodawala*
  Pursuing Bachelor of Engineering in Computer Science and Engineering,
  ITM Universe,
  Vadodara, India.
  E-mail: darshanbodawala@gmail.com
- *Pradeep Laxkar*
  Head of Department,
  Computer Science and Engineering,
  ITM Universe,
  Vadodara, India.
  E-mail: pradeep.laxkar@gmail.com

sleeve of metal or plastic which blocks the ATM's card slot, causing any inserted card to be apparently retained by the machine, allowing it to be retrieved by the fraudster when the card holder leaves [3].

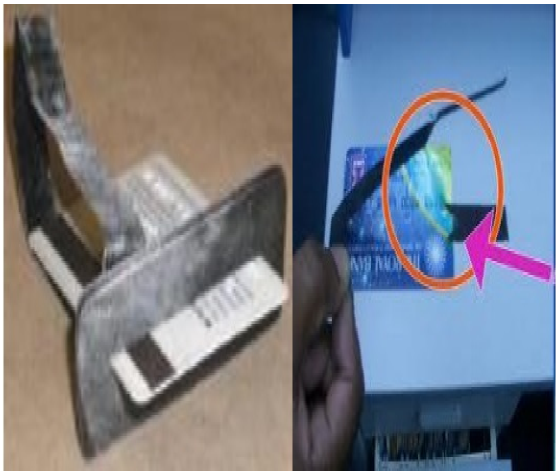


Fig. 2 Lebanese Loop, commonly used for card trapping

PIN PAD Overlay:

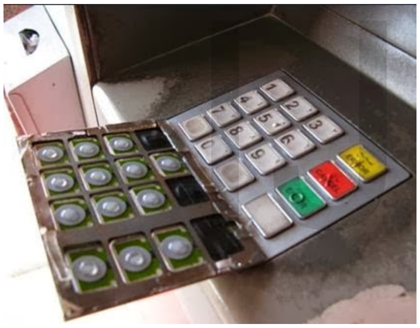


Fig. 4 Fake Key Pad

Place a false plastic PIN pad on the original one and text PIN when customer enters. Then the PIN number of the customer is stored by the thieve [1].

Spy camera:
Install a fake advertising box or mailbox with small convert camera inside to observe PIN entry. With the wireless technology developing, the captured PIN can be real-time transited to allowing producing counterfeit card immediately, compared with old stand-still capture method [1].

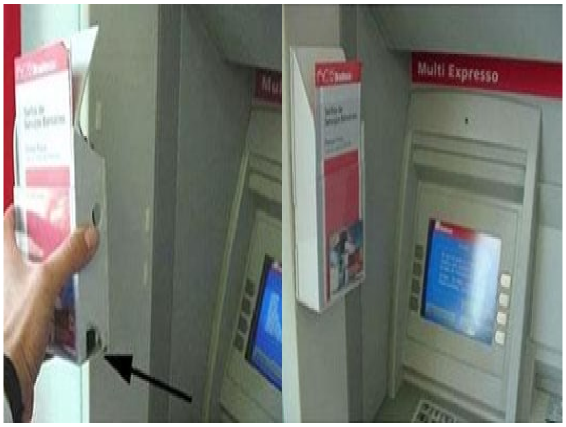


Fig. 3 Hidden Camera

Cash trapping:
Criminals fix a false withdrawal shutter slot, causing cashes to get stuck inside when customers attempt to do a withdrawal. The customer leaves assuming that the machine is out of order or goes inside the bank to report the incident and the thieves return to retrieve the cash [1].

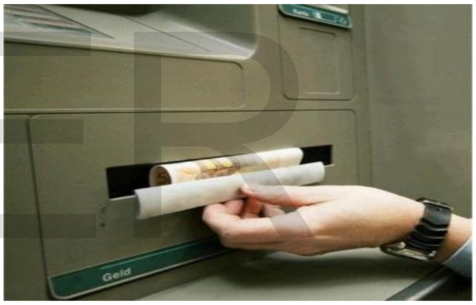


Fig. 5 Cash Trapping

Fake ATM Machine:
The organization also is tracking a skimming trend reported by three countries (mainly in Latin America) in which thieves are fabricating fake ATM fascia and placing them over genuine ATMs, like the one pictured below (Fig. 6). After entering their PIN, cardholders see an 'out-of-order' message. European ATM Security Team (EAST) said the fake fascia include working screens so that this type of message can be displayed. The card details are compromised by a skimming device hidden inside the fake fascia, and the PINs are captured via the built-in keypad, which overlays the real keypad underneath [4].

IJSER

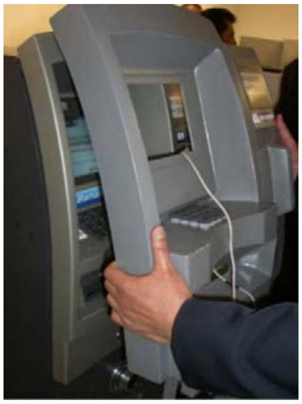


Fig 6. Fake ATM Machine

II. Related Work

1. Diebold's prominence in the financial security business for over 100 years allows their customers to depend on Diebold to provide solutions and recommended approaches to contain such issues as ATM fraud. Diebold boasts a world-class service organization with professional ATM service technicians that are trained to be cognizant of the new ATM fraud techniques and to conduct a detailed evaluation of key ATM components to ensure there has been no tampering or additions to the fascia [5].

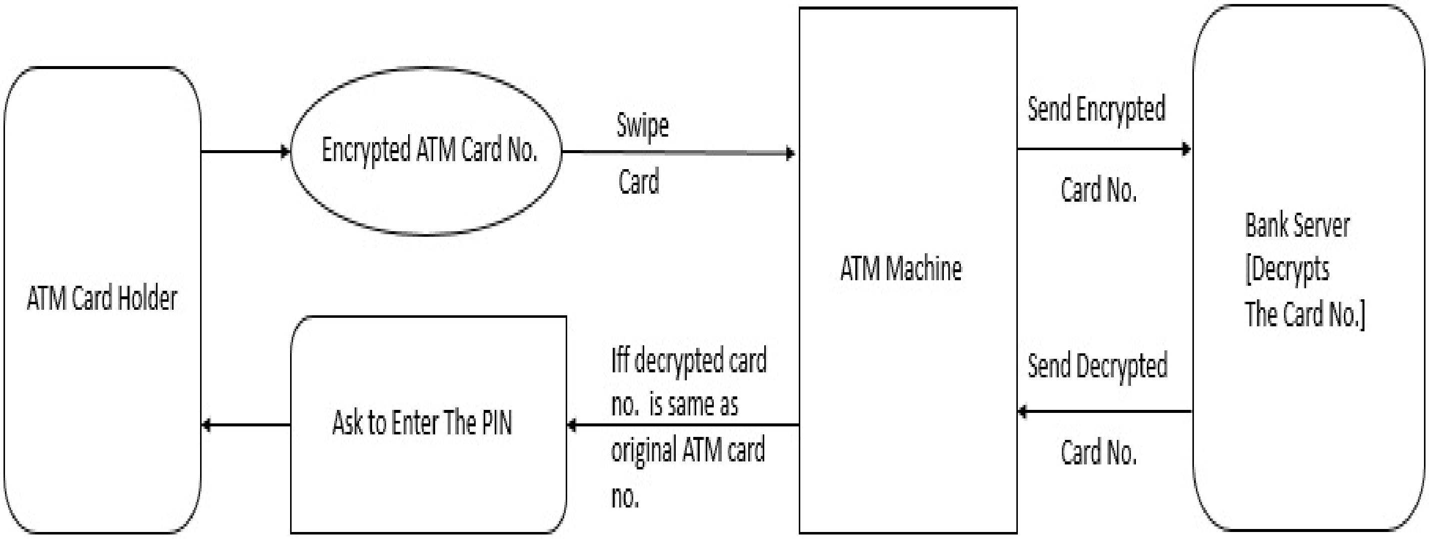
2. A multi-layered approach to ATM security—combining technologies such as video surveillance and monitoring, remote ATM management and foreign object detection as well as common sense management practices aimed at deterring crime—are providing FIs with an edge in the fight against fraud and keeping the self-service industry at least one step ahead of fraudsters [6].

3. The main reason for introducing biometric systems is to increase overall security. Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, biometrics can replace or supplement the existing technology. In others, it is the only viable approach. Decision-makers need to understand the level of security guaranteed through the use of biometric systems and the difference that can exist between the perception and the reality of the sense of security provided. The biometric system is only one part of an overall identification or authentication process, and the other parts of that process will play an equal role in determining its effectiveness [7].

4. ATM security provides strong protection of the user's data and offers the possibility to make a network secure. Authentication, confidentiality, and data integrity are the foundations of a security framework that fulfills the user's needs for secure communication. Furthermore a context-agile encryptor at an ATM-aggregation point satisfies not only security concerns of virtual private networks but also brings cost-savings [8].

IJSER

III. Methodology



In this method, first of all the ATM card no. of the card holder is encrypted by card holder's private key in RSA algorithm and stored on the ATM card's magnetic stripe by the bank.

Now the card holder goes to the ATM machine and swipe his/her ATM card. By swiping, the encrypted ATM card no. is sent to the bank server by the ATM machine. At the bank server that ATM card no. is decrypted by card holder's public key (i.e. bank has both keys.) in RSA algorithm.

Now server sends the decrypted ATM card no. to the ATM machine. At the ATM machine, card holder verifies the decrypted ATM card no. with his/her actual ATM card no. which is written at the front side of the ATM card. If card holder finds the decrypted ATM card no. and actual card no. same then and only then the card holder is supposed to enter his/her PIN, otherwise he/she will not enter the PIN.

By applying this method we can prevent the fake ATM machine attack. As if the machine is fake then it will not have the public key of the card holder and it will not decrypt the encrypted ATM card no. on the ATM card. So, the card holder will know that the machine is fake or something wrong with it and he/she will not enter his/her PIN and leaves that fake ATM machine.

So, we can stop skimmers from doing this type of skimming by using this method.

IJSER

IV. Implementation

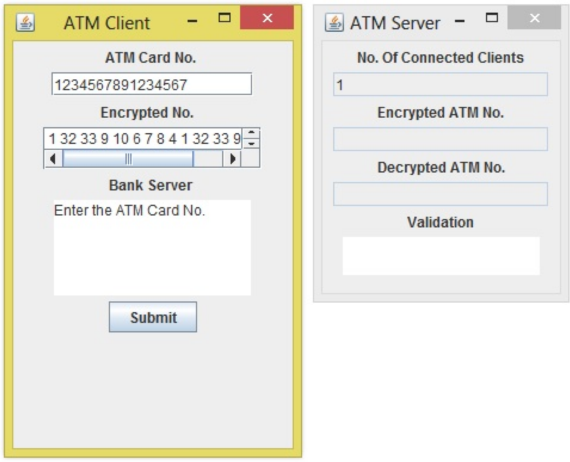
Following are the values which are used for encryption

In RSA algorithm:

p = 5, q = 7, n = 35,

f (n) = 24, e = 5, d = 5.

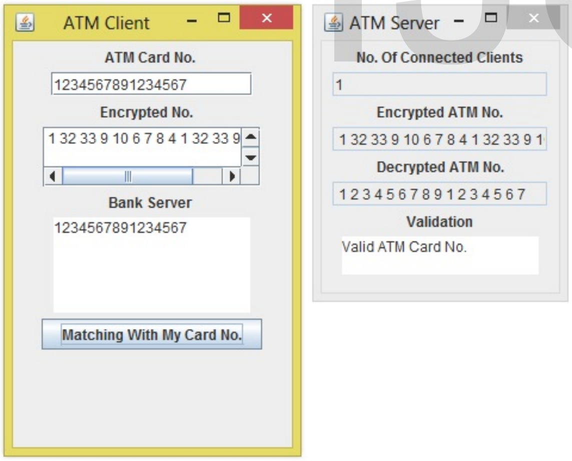
1) Input of Customer ATM Card Number:



ATM Card No.
1234567891234567
Encrypted No.
1 32 33 9 10 6 7 8 4 1 32 33 9
Bank Server
Enter the ATM Card No.

No. Of Connected Clients
1
Encrypted ATM No.
Decrypted ATM No.
Validation

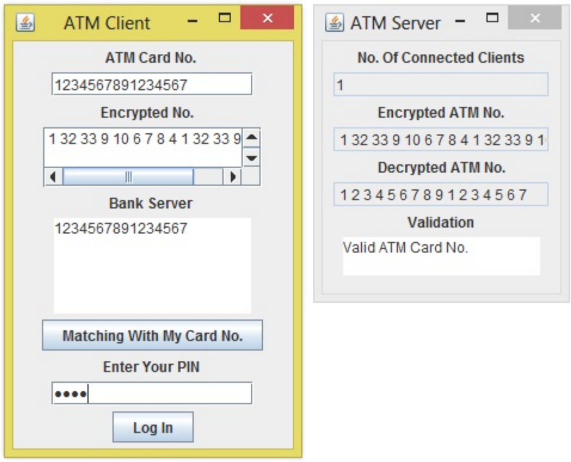
2) Bank Server Sends The Decrypted ATM Card No. :



ATM Card No.
1234567891234567
Encrypted No.
1 32 33 9 10 6 7 8 4 1 32 33 9
Bank Server
1234567891234567

No. Of Connected Clients
1
Encrypted ATM No.
1 32 33 9 10 6 7 8 4 1 32 33 9 1
Decrypted ATM No.
1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7
Validation
Valid ATM Card No.

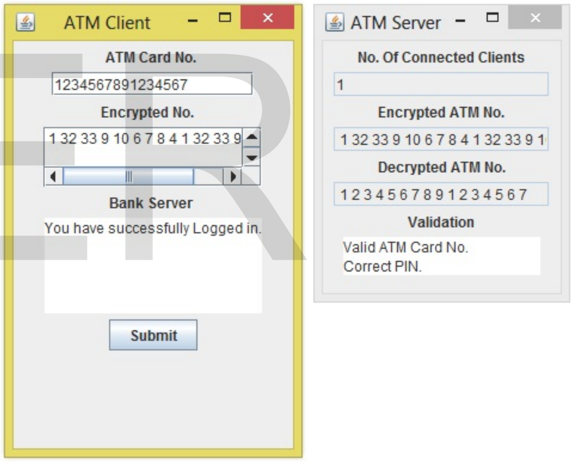
3) After Verification of The ATM Card No., ATM Card Holder Enters The PIN:



ATM Card No.
1234567891234567
Encrypted No.
1 32 33 9 10 6 7 8 4 1 32 33 9
Bank Server
1234567891234567
Enter Your PIN
••••

No. Of Connected Clients
1
Encrypted ATM No.
1 32 33 9 10 6 7 8 4 1 32 33 9 1
Decrypted ATM No.
1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7
Validation
Valid ATM Card No.

4) Successful Log In If PIN IS Correct:



ATM Card No.
1234567891234567
Encrypted No.
1 32 33 9 10 6 7 8 4 1 32 33 9
Bank Server
You have successfully Logged in.

No. Of Connected Clients
1
Encrypted ATM No.
1 32 33 9 10 6 7 8 4 1 32 33 9 1
Decrypted ATM No.
1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7
Validation
Valid ATM Card No.
Correct PIN.

IJSER

V. Conclusion

So, by applying above described mechanism we can prevent the skimming of fake ATM machine and from this we can stop skimmers from getting the customer's money.

And so customers will feel safe about their money transaction in ATM.

References

[1]http://www.grgbanking.com/en/exh/images/Best%20Practice%20for%20ATM%20Security%20-GRGBanking.pdf

[2] http://www.investopedia.com/terms/a/atm.asp

[3] http://en.wikipedia.org/wiki/Lebanese_loop

[4] http://krebsonsecurity.com/tag/fake-fascia/

[5] DIEBOLD-ATM Fraud and Security White Paper - Authored by: Anna C. Istnick and Emilio Caligaris

[6] ATM Fraud And Security White Paper - Diebold, Incorporated, File number 98-192

[7] ENHANCED ATM SECURITY SYSTEM USING BIOMETRICS - Prof. Selina Oko1 and Jane Oruh

[8] Introduction to ATM Security - Josef Kolbitsch

IJSER