Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 1, pp: (43-45), Month: January - April 2015, Available at: www.noveltyjournals.com

An Automated Teller Machine: Literature Review

[1]Nuthan K, [2]Nagarathna B M, [3]Sumana Nayaka R L, [4]Vidya Rathna B

[1,2] Department of Computer Science and Engineering, Srinivas School of Engineering, Mangalore, India
[3] Department of Computer Science and Engineering, Rajiv Institute of Technology, Hassan, India
[4] Department of Computer Science and Engineering, BNM Institute of Technology, Bangalore, India

Abstract: **In modern days money withdrawal via ATM (Automated Teller Machine) becoming a main part of our life. This paper provides the brief description of ATM system. It also explains the issues of ATM system. The security requirements of the ATM system are discussed. The problem of misusing the information related to the customer in ATM system is addressed.**

Keywords: **ATM, AES 256 Algorithm, OTP (One Time Password), Data Encryption Standard.**

I. INTRODUCTION

An automated teller machine or automatic teller machine (ATM) is a device that provides the clients of financial institutions with access to money transactions in a public space without the need of bank customers. The modern ATMs, the customer is identified by inserting a ATM card with a chip that contains a unique card number and some data such as an expiration date, CVV(Card Value Verification) code and customer name. Customer identification and authentication is provided by the customer providing a personal identification number (PIN). Using an ATM system, customers can access their bank accounts in order to make money withdrawals, debit card fund advances, and check their bank account balance.

Fraud against ATM system and people's try to use them takes several methods. Once customer's bank card is lost and the password is known, the hacker will draw all the money in the short span of time, which brings huge money losses to customer. Unlike bank system, ATMs does not require any person performing the transaction to present a his picture identification such as sign and his physical presence. If the bank card is stolen by the criminal and the PIN number is known, a criminal person can easily make an access to the bank account. There has also been lot of incidents of criminal by the Man-in-the-middle attacks, where criminals have attached card readers or fake keypads to the existing ATM machines. These fake keypads will be used to read customers' PINs and transaction password in order to make unauthorized access to the bank customers.

II. WORKING MECHANISM

ATM is device which will be used for the getting the cash without the absence of bank clerk or employer. The customer will be identified by a smart card which contains 16 digit card numbers. When the customer inserts the card inside the ATM machine card number will be read and it will ask the customer for a secret PIN and the amount to be debited. The card number and secret PIN will be encrypted and send to the server. At the server side the card number and secret PIN will be decrypted and if all the details matched with the particular customer then the customer is said to be authentic otherwise the transaction will be debited.

III. ISSUES IN ATM MACHINES

Currently the triple DES algorithm is used at the client side for the encryption of the PIN which will be transmitted to the server. The algorithm is sluggish in software's and it is very slow. The man-in-the-middle attacks where the criminals can

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 1, pp: (43-45), Month: January - April 2015, Available at: www.noveltyjournals.com

attach the fake keypads for the existing ATM machines. This fake key pad can be used to read the PIN of the customer. Using this PIN the transaction password which will be used for the online transaction can be stolen by the attacker. The attacker may fix the cameras in the place of the ATM machine. Using this camera he might be able to read the PIN no of the customer.

IV. USE OF AES ALGORITHM AND OTP FEATURE

AES (Advanced Encryption Standard) is the one of the strong and secure algorithm used for the encryption and as well as decryption.AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical.

It uses a massive combination of keys therefore the encrypted code is not easy to crack. The algorithm performs well in almost all the software's as well as hardware devices. Instead of Triple DES (Data Encryption Standard) which is currently use the AES algorithm can be used.

The use of OTP feature will increases the security of the current ATM machine system. The OTP can be generated based on the time during the transaction can be sent to the customer registered mobile number. The customer needs to enter the OTP which is sent by the bank during the transaction.

V. SECURITY REQUIREMENTS IN ATM SYSTEM

A. Authorization:

A transaction must always be authorized by the payer and needs payer authentication (physical, PIN, or digital signature). A payment may also need to be authorized by the bank.

B. Data confidentiality and authenticity:

The transaction data should be authentic and external parties should not have access to data. And some data need to be hidden even from participants of the transaction in ATM palce.

C. Availability and reliability:

A transaction infrastructure should always be available and centralized systems should be designed with care.

D. Privacy:

The customers should be able to control how their personal data is used by the other parties. The ATM transaction should provide the privacy of the data.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 2, Issue 1, pp: (43-45), Month: January - April 2015, Available at: www.noveltyjournals.com

VI. CONCLUSION

A brief explanation about the ATM is explained. The issues in ATM system are discussed. The important security requirements of ATM system are presented. The problem of misusing the data related to the customer is addressed.

VII. FUTURE WORK

The security of the ATM system can be further increased by the encrypting the 3D secure password and with the introduction of the OTP (One Time Password) feature. The various methods such as visual cryptography and steganography can be used to hide the customer data. An algorithm called Advanced Encryption Algorithm (AES) can be used since it provides the strong encryption of the PIN number.

REFERENCES

[1] Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), Nov 26, 2001.

[2] "Related-key Cryptanalysis of the Full AES-192 and AES- 256",Alex Biryukov and Dmitry Khovratovich, , University of Luxembourg, 29 May 2009.

[3] "Online Credit Card Transaction using fingerprint Recognition", M.Umamaheshwari, S.Sivasubramanian and B.Harish Kumar, International Journal of Engineering and Technology Vol. 2 (5), 2010, 320-322

[4] "ADVANCED BIOMETRIC ATM MACHINEWITH AES 256 AND STEGANOGRAPHY" *Rishigesh Murugesh*, IEEE- Fourth International Conference on Advanced Computing, ICoAC 2012