A SURVEY ON THEFT PREVENTION DURING ATM TRANSACTION WITHOUT ATM CARDS

Sistu Sudheer Kumar[1], A. Srinivas Reddy[2]

[1]*Dept. of Computer Science and Technology, GITAM Hyderabad University, Hyderabad, India*
[2]*Dept. of Computer Science and Technology, GITAM Hyderabad University, Hyderabad, India*

Abstract

Authentication is a critical part of any trustworthy computing system which ensures that, only individuals can to log on to the system. Here ATM Security has always been one of the most prominent issues. ATM machines generally authenticates by using ATM card and PIN number to perform transactions. This papers discusses design of ATM system that will improve the authentication of customer while using ATM. Here is possible scenario that an individual's ATM [1] card falling into wrong hands by knowing PIN number and forget ATM card is difficult to perform ATM transaction. So to clear all these problems we are implementing this system using "One Time Password (OTP)" and "Personal Identification Number (PIN)" combination in order to improve authentication of customer using ATM machine to perform transaction without having any ATM cards.

Keywords— *Automated Teller Machine (ATM), One Time Password (OTP), Personal Identification Number (PIN), Card Verification Value (CVV), Cipher Block Chaining (CBC).*

----------***----------

1. INTRODUCTION

ATM's have not only changed the banking perspective of the world, but a general perspective as well. An **automated teller machine** (**ATM**) is a computerized telecommunications device that provides the customers is able to conduct many banking services like cash withdrawal, deposit, and check book printing and money transfer other accounts in a public space without physical interaction with bank staff. Generally in ATMs customer is authenticate by ATM card with magnetic stripe that contains unique card number and security information such as an expiry date, Card Verification value (CVV) by entering Personal Identification Number (PIN).

How Do ATMs Work?

ATM is communicate with central host processor by Internet Service Provider has a gateway where all ATM networks available to user. Here ATM machines connected to central host processor are by telephone lines or normal phone line using modem.

When customer wants to perform transaction provide PIN details and ATM card. ATM machine forwards to central host processor, where ATM request to customer's bank. If customer request cash, central host processor initiates electronic funds transfer from customer bank to ATM central host processor account. Once transfer complete to central host processor, it sends approval code to ATM machine to dispense cash.

But authentication of ATM during transactions are also unsecure because with help of clone of original cards by replicas of ATM machine card slots with built-in magnetic strip readers. The reader capture data embedded in the magnetic strip and store it. By placing small wireless surveillance cameras in ATM center to track the PIN to cash withdrawal. To overcome this, I proposed using One Time Password and PIN to authenticate the ATM transactions without ATM cards.

2. LITERATURE SURVEY

The idea behind to develop ATM was to reduce workload of a bank. A Turkish born inventor working in America called George Simijan started building an earlier and not-so-successful version of an ATM in the late 1930's. In 1965 a Scottish man called James Goodfellow was given a project to develop an automatic cash dispenser.

In present ATM system to perform ATM transaction we must enter card and PIN details to verify authentication. In case of losing ATM card/ forget ATM card no chance to perform ATM transaction. In present days this type of technology is not sufficient to secure ATM transaction form intruders. Here are methods to improve lot of security to overcome the difficult in ATM transaction. Methods to improve the security in ATM Banking system are:

2.1 Unimodal Biometrics System

Biometrics is derived From the Greek word "bio" means life and "metrics means measure. Biometrics refers to identity of an individual based upon physical characteristics or behavioural traits. Where identity of a person by password, PIN provides first level of security, fingerprint templates are encoded into smart card memory, to identify his/her fingerprints are compared against the digital templates in card memory.

In Traditional methods to identify persons base on knowledge or token-based mechanism, but easily lost, shared or stolen. So, to overcome all these we introduced biometric system like fingerprint, Iris, Retina, Palm print, Face recognition.

Limitations

Problems in biometric systems are noise in sensed data, lack of individuality, .Intra-class variations, spoofing.

2.2 Crypto-Biometric System

In this Crypto-Biometric [9] system at the time of transaction retinal image is captured and blood vessel tree is extracted. From that blood vessel tree selective feature points extracted using Harris Corner detection [9] to generate 256 bit key. With help of User's bio-key user's password is encrypted. Encrypted password transform to central server where image is decrypted.

Advantages of Crypto-Biometric mechanism increase of reliability and identification quality, reducing error rates.

Limitation using Crypto-Biometric mechanism, if biometric fails due to presence of noise in the biometrics, the FRR [9] (False Reject Rate) increases. Increases cost effectively due to installation of additional hardware.

2.3 Authentication in ATM System by One Time Password

Here to perform ATM transaction, place ATM card into system, enter PIN along with the One Time Password it will get to the registered mobile number. But problem with the OTP is if we lost our mobile or OTP may visible to all other's.

2.4 Encryption Techniques Use in ATM Systems for Secure Data Communication [8]

Encryption method that has been a national standard since 1977 is DES (Data Encryption Standard). It uses single secret key to encrypt the PIN at the ATM and decrypt PIN after received by central host processor, to verify customer. DES (Data Encryption Standard) is a symmetry algorithm here Cryptographic algorithm is used- which is called the Data Encryption Algorithm (DEA). DES is a 64 bit block cipher which means that it encrypts data 64 bits at a time, for encryption and decryption uses the same key. The key size used is 56 bits; however a 64 bit key is actually input. But in 1998 Electronic Freedom Foundation group breaks DES.

Triple-DES

Triple-DES offers significantly higher level of security rather than DES, but it is based on the same single DES algorithm.

Encryption and Decryption in Triple-DES:

O = EK1 (DK2 (EK1 (I)))
O = DK1 (EK2 (DK1 (I)))

E/D – DES Encryption/Decryption
K1, K2 – secret keys
I/O – data blocks: input/output

Advanced Encryption Standard

Advanced Encryption Standard (AES)[2] adds support for new encryption standards AES, with Cipher Block Chaining (CBC) mode, to IP Security (IPSec). The National Institute of Standards and Technology (NIST) have created AES. AES is a privacy transform for IPSec and Internet Key Exchange (IKE) and has been developed to replace the Data Encryption Standard (DES). AES offers a larger key size, 128/192/ 256 to decrypt a message is for an intruder to try every possible key.

One Time Password

One Time Password is a password valid for only one login session for particular time only. OTP [3] [4] [5] [6] avoid problems associated with static passwords. Major advantage is potential intruder who manages record an OTP is not valid for longer time.

3. FEATURE WORK

Present ATM banking system are working with ATM cards with PIN/ Biometric systems, in feature we have chance to perform ATM transactions without having any ATM cards by help of One Time Password (OTP) and PIN combination to remove security concern to authenticate user.

4. CONCLUSION

Thus we have reviewed several authentication algorithms like PIN, biometric system to perform the ATM transaction lot of security concerns, increases hardware and software cost. So, with help of One Time Password and PIN combination we can reduce the ATM banking system security problems, reduces hardware and software cost. Using these methods we can perform the ATM transaction while forget ATM cards/ no chance for theft of ATM cards.

REFERENCES

[1]. "Theft Prevention ATM model using Dormant Monitoring for Transactions" Vivek V.Jog IEEE 2013 conference on ICT 2013
[2]. "A Method to improve the security level of ATM Banking System using AES Algorithm" N.Selvaraju, G.Sekar International Journal of Computer Application, 2010
[3]. "One Time Password for Multi-Cloud Environment" Richa Chowdhary, Satyakshma Rawat International Journal of Advanced Research in Computer Science and Software Engineering 2013

[4]. "One time password" http://en.wikipedia.org/wiki/One-time_password
[5]. "Elimination Vulnerable Attacks Using One-Time Password and Pass Text- Analytical Study of Blended Schema" M. Viju Prakash, P.Alwin Infant ,S.Jey Shobana Universal Journal of Computer Science and Engineering Technology
[6]. **"**One-Time Password Access to Any Server without Changing the Server" Dinei Florencio and Cormac Herley.
[7]. "Enhance the security in ATM system with Multimodal Biometrics and Two-Tier Security" kande Aarchana and A.Govardhan Volume 3, Issue 10, October 2013.
[8]. "Different Data Encryption Methods Used in Secure Auto Teller Machine Transaction" Navneet Sharma, Vijay Singh Rathore (IJEAT)
ISSN: 2249 – 8958, Volume-1, Issue-4, April 2012 175
[9]. "A Biometric Authentication Based Secured ATM Banking System" Shouvik Biswas, Anamitra Bardhan Roy, Kishore Ghosh, Nilanjan Dey