Secured Automatic Teller Machine (ATM) and Cash Deposit Machine (CDM)

Shailesh N. Sisat[1]
Dept. of Electronics & Telecommunication
G. H. Raisoni C. O. E. & M., Amravati
Maharashtra – India

Vishwajit K. Barbudhe[2]
Dept. of Electronics & Telecommunication
Jagdambha C.O.E.T, Yawatmal
Maharashtra – India

Prajkta S. Bhopale[3]
Dept. of Electronics & Telecommunication
G. H. Raisoni C. O. E. & M., Amravati
Maharashtra – India

Abstract: Authentication is an important part of any secrete operation and concept is applicable for trustworthy Automatic Teller Machine which ensures that, only individuals with corroborated identities can log on to the system or access system resources. In this paper, I survey the literature to describe the ways that ATMs have influenced these aspects of security, and conclude with suggestions for further research.

Keywords: Automated Teller Machines, ATM, Cash deposit machine, CDM, biometric ATM.

I. INTRODUCTION

ATM system follows four digit PIN authentication process for user validation. Many researchers suggest the additional authentication process such as biometric, thumb and face validation. Now a days we are aware of the ATM which make the task of money withdraw more flexible. In addition to this banks are introducing Cash deposit machine (CDM) that makes easy to deposit cash to user account. As day by day this process is becoming easier, hackers started their job to disturb the ATM process. This paper describes basic ATM attacks.

II. EXISTING ATM MACHINE ALGORITHM AND FLOWCHART

The given existing ATM algorithm and flow chart describes the operation of ATM during withdraw of notes from the ATM machine. However the machine doesn't know that the note is fake or original notes.

Step 1. User accesses his account using Debit card through ATM machine with help of PIN.

Step 2. ATM machine reads this card and check it with Bank server.

Step 3. And now ATM waits to enter the transactions request.

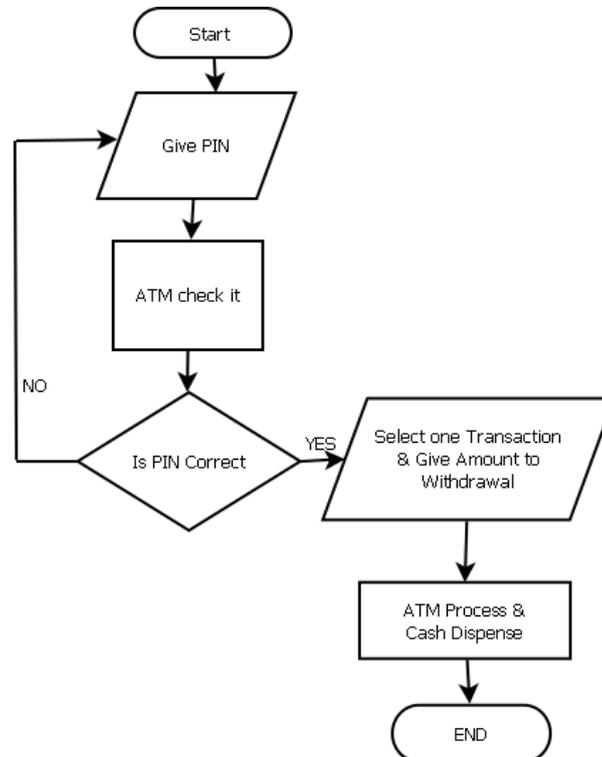**Step 4.** User may use ATM now and transact.

Fig1. Existing ATM Flow chart using PIN

III. ATTACKS IN AUTOMATED TELLER MACHINE

ATM threats can be segmented into three types of attacks: card and currency fraud, logical attacks and physical attacks [1].

Card and currency Fraud: Card and currency fraud involves both direct attacks to steal cash from the ATM and indirect attacks to steal a consumer's identity (in the form of consumer card data and PIN theft). The intent of indirect attacks is to fraudulently use the consumer data to create counterfeit cards and obtain money from the consumer's account through fraudulent redemption [1].

Skimming Attack: skimming attack is the most known attack related to ATMs. It involves small portable card reader used to capture the authenticated data available on the ATM magnetic strip.

Card Trapping and Fishing: Card trapping is conducted by placing a device over or inside the card reader slot to capture the consumer's card. These can be devices such as plates over the card reader, thin metallic strips covered in a plastic transparent film, wires, probes and hooks. These devices are designed to prevent the card from being returned to the consumer at the end of a transaction [1].

Logical/data Attacks: It includes attack on ATM's software, operating system and communication network and systems. Main target is to introduce viruses intended to exploit an ATM's operating system mostly job of hackers who install malware to violate the confidentiality, integrity or authenticity of transaction-related data.

Physical Attacks: It includes getting cash by physically damaging the ATM. It involves any component or part of the ATM.

IV. LITERATURE SURVEY ON SECURITY IN AUTOMATED TELLER MACHINE

Dhiraj Vasant Kapare , Sadashiv Lokhande, Sayaji Kale propose the project designed to provide fully automatic cash deposit machine. It is combination of Embedded, DIP & Automation. In Mat lab every data image of note is compared with ideal stored image of every appropriate type of note. Every note is passed through UV light to detect the originality of note which consequently results in acceptance and rejection of faulty notes [2].

Shouvik Biswas, Anamitra Bardhan Roy, Kishore Ghosh, Nilanjan Dey prapose a Bio-metric system for encrypting the user password is proposed for secure remote ATM transaction. A retinal image is acquired at transaction terminal and Bio feature points are extracted from the blood vessel tree. User password is encrypted using some selective feature points. After transmission to the central server, encrypted password is decrypted using stored Bio-key to extract the password and check with the stored password? The success of the transaction is based on the stored database. The proposed scheme is self manipulative, simple, fast and yet much more secure. The efficacy of this computer simulation of bio-metric authentication system claims a secure online transaction [3].

Pooja Mali Shruti Salunke Rajashri Mane Pooja Khatavkar proposes a unique authentication and encryption technique using two factor biometric pattern of a person. At the time of registration to the network, a person's face is scanned and phase features of the image are generated. Therefore a local binary code of sixty four byte is extracted of this matrix and is transmitted to the server. Server stores this key as user's identity or password. Then the user thumb is scanned and its features are extracted and stored in server database [4].

Essien Eyo E, proposed algorithm for automated teller machine and concluded that The ATM network has to provide software interfaces to the software used by different banks and different network software. Also there should be no restriction of the ATM network to a specific network protocol as long as the performance requirements are satisfied [5].

Anurag Anand Duvey, Dinesh Goyal, Dr. Naveen Hemrajani introduced new authentication system which is secure and highly usable, based on multifactor authentication approach. It uses a novel approach to create an authentication system based on DynaPass and SMS to enforce an extra security level over the traditional login in an ATM machine. The DynaPass is most sensitive data for any financial transactions, so we are storing DynaPass in encrypted format on user's cell phone. The Bank or Financial institutions are responsible for DynaPass generation and distribution to their customers [6].

Akash choubey, Amarjot Singh, Srikrishna Karanam, Devinder Kumar, and Ketan Bacchuwar, introduces a novel system, a combination of behavioral traits as well as traditional methods for identity recognition. The system uses signature verification as the behavioral trait along with a unique identity number (referred as UIN in rest of paper) for the recognition. Signature verification is an important domain for confirming a person's identity. The system is applied of an ATM (Automatic Teller Machine) to decrease the risk of theft from an individual's account. It can be effectively employed to reduce the risk of forgery by releasing the trouble of carrying ATM cards by the users, by employing a signature verification system fused with a unique identity number [7].

K. Satish, Y.K.Viswanadham, I Leela Priya praposed simulation model to deposit money to an account in ATM itself [8].

V. OBJECTIVE OF THE STUDY

Many researchers provide security solutions to protect the AUTOMATED TELLER MACHINES. However the suggested security algorithms only deal with the user authentications. Sometime customers are getting fake notes from ATM. Fake and duplicate currency note is a major issue. Note security and reliability must be taken in to consideration while designing the security algorithm for ATM.

VI. CONCLUSION AND FUTURE WORK

This paper gives an idea about the basic Automated Teller Machine and its major security issues and basic requirements. However ATMs deals with the currency notes, focus should be on note security while designing the ATM. The future work for this research area will include the design of algorithm by considering security and reliability of currency notes through ATMs. It will include modification in the existing ATM algorithm while depositing money in the ATM by the bank authority and modification in the CDM while depositing money in the CDM by the customer.

References

1.   "ATM FRAUD AND SECURITY" ©Diebold, Incorporated, 2012, File number 98-192

2.   Dhiraj Vasant Kapare , Sadashiv Lokhande, Sayaji Kale "Automatic Cash Deposite Machine With Currency Detection Using Fluorescent And UV Light" International Journal Of Computational Engineering Research (ijceronline.com) Vol. 3 Issue. 3

3.   Shouvik Biswas, Anamitra Bardhan Roy, Kishore Ghosh, Nilanjan Dey, "A Biometric Authentication Based Secured ATM Banking System", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 4, April 2012.

4.   Pooja Mali Shruti Salunke Rajashri Mane Pooja Khatavkar, "Multilevel ATM Security Based On Two Factor Biometrics", International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 8, October – 2012 ISSN: 2278-0181

5.   Essien Eyo E, "Proposed algorithm for automated teller machine", Elixir Adoc Network 36 (2011) 3164-3167

6.   Anurag Anand Duvey, Dinesh Goyal, Dr. Naveen Hemrajani, "A Reliable ATM Protocol and Comparative Analysis on Various Parameters with Other ATM Protocols", International Journal of Communication and Computer Technologies Volume 01 – No.56 Issue: 06 Aug 2013, ISSN NUMBER : 2278-9723.

7.   Akash choubey, Amarjot Singh, Srikrishna Karanam, Devinder Kumar, and Ketan Bacchuwar , "A Novel Signature Verification Based Automatic Teller Machine", international Journal of Information and Electronics Engineering, Vol. 2, No. 4, July 2012

8.   K. Satish, Y.K.Viswanadham, I Leela Priya, "Money to ATM – Fake Currency Detection", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5) , 2012,5046-5050.

9.   Richa Tuli, Abhijeet Khatri, Anita Yadav, "A comparative study of customer attitude towards ATM of SBI and ICICI bank", International Journal of Marketing and Technology, Volume 2, Issue 8

10. Muhammad Asif Khan, "An Empirical Study of Automated Teller Machine Service Quality and Customer Satisfaction in Pakistani Banks", European Journal of Social Sciences – Volume 13, Number 3 (2010)

11. Yingxu Wang, Yanan Zhang, "The Formal Design Model of an Automatic Teller Machine (ATM)" International Journal of Software Science and Computational Intelligence, 2(1), 102-131, January-March 2010