Multilevel Authentication for ATM Security

Rini Jones, Sreedevi Krishnan G., Vidhya M. S., UG Students, Dept. of ECE, LMCST
Veena V. U., Asst. Prof., Dept. of ECE, LMCST

Abstract—Biometrics based authentication offers several advantages over other authentication methods. There has been a significant surge in the use of biometrics for user authentication in recent years. In this paper the existing security of the ATM (Automated Teller Machine) system has been improved by integrating the fingerprint of the user into the bank's database as to further authenticate it. During transaction when the user swipes the card, the system requests the fingerprint of the user or the nominee mentioned in the database. When the finger print matches, the main system produces a One Time Password and sends it to the user mobile number registered in the database and thus the user can have a safe and secure transaction.

Index Terms— Authentication, Biometrics, Nominee, Fingerprint, OTP

I. INTRODUCTION

Automated Teller Machines (ATM) have become a part of prestige of the banks all over the world. As the banks compete by opening more and more ATM's every year, research is going on of several aspects of ATM especially security. In real time ATM, user is authenticated only by a four digit Personal Identification Number (PIN) which can be compromised easily. Since this single level is vulnerable to attack, this paper proposes multiple security levels that can minimize the first financial risk to customers. The multiple security levels comprises of an extra user authentication and OTP verification mechanisms [3]. Unlike prior research, this concept is a cost effective way that can be easily integrated into the current ATM functionality.

The pervasive deployment of ATM all over the world itself highlights the importance of ATM in the current society. Even though transactions in ATMs are believed to be secured using PIN only, issues are reported of financial loss of at least one transaction loss to customers when the card is lost [2]. Such a risk can be minimized by adding multiple levels of security for authenticating user and transaction verification based on location information.

II. LITERATURE SURVEY

Automated Teller Machines were first introduced in 1939. At present there are about 3 million units installed all around the world. As the number of ATM units increase, the machines are prone to hacker attacks, fraud, robberies and security breaches. In the past, the ATM machines' main purpose was to deliver cash in the form of bank notes and to debit a corresponding bank account. However, ATM machines are becoming more complicated and they serve numerous functions, thus becoming a high priority target to robbers and hackers [4].

A. Security Measures of ATMs

Modern ATM machines are implemented with high-security protection measures. They work under complex systems and networks to perform transactions. The data processed by ATMs are usually encrypted, but hackers can employ discreet hacking devices to hack accounts and withdraw the account's balance [2]. As an alternative, unskilled robbers threaten bank patrons with a weapon to loot their withdrawn money or account.

Security breaches in Electronic funds transfer systems can be done without delimiting their components. Electronic funds transfer systems have three components; which are communication links, computers, and terminals (ATMs). First, communication links are prone to attacks. Data can be exposed by passive means or direct means where a device is inserted to retrieve the data. The second component is computer security. There are different techniques that can be used to acquire access to a computer such as accessing it via a remote terminal or other peripheral devices such as the card reader. The hacker had gained unauthorized access to the system, so programs or data can be manipulated and altered by the hacker. Terminal security is a significant component in cases where cipher keys reside in terminals. In the absence of physical security, an abuser may probe for a key that substitutes its value.

B. ATM Vulnerabilities

As with any device containing objects of value, cash machines and the systems they depend on to function are the targets of fraud. ATM attacks and fraud continue to make headlines, despite the fact that the technology

running ATM networks is becoming more secure and consumers are perhaps more vigilant than ever. There are six main ATM threats that exist and multilevel authentication of ATM security plays a vital role in reducing these threats.

- Card skimming

Remain as the number one threat globally. Essentially, skimming refers to the stealing of electronic card data, enabling the criminal to counterfeit the card. Consumers experience a normal ATM transaction and are usually unable to notice a problem until their account is defrauded.

- Card trapping

Trapping is the stealing of the physical card itself through a device fixed to the ATM. In a pre- EMV or chip- and- signature environment, the PIN does not need to be compromised. Again contactless capability can help.

- Transaction reversal fraud

TRF involves the creation of an error that makes it appear as though the cash had not been dispensed. The account is re- credited the amount withdrawn but the criminal pockets the money. It could be a physical grab or a corruption of the transaction message.

- Cash trapping

Normally relatively low value, the fraudster will use a device to physically trap the cash that is dispensed and come to collect once the customer has left the ATM location.

- Physical attacks

This category is related to any attempt to rob the ATM of the cash in the safe. Methods of physical attacks include solid and gas explosives, as well as removing the ATM from the site and then using other methods to gain access to the safe.

- Logical attacks

Logical attacks are becoming a major and growing attack vector, and one that has the potential to cause large amounts of losses. In this type of attack, external electronic devices, or malicious software is used in the crime. The tools are used to allow the criminal to take physical control of the ATM dispenser to withdraw money, which is often called “cash- out” or “jackpotting”, as the machine starts spitting out like a casino gaming machine.

The other version of malware attack on ATMs sees criminals using software to intercept the card and PIN data as customers use the machine. They can then use this to clone cards and commit fraud at point of sale terminals, ATMs and in ‘card- not- present’ scenarios.

III. PROPOSED METHOD

ATM cards authentication methods have changed little since their introduction in the 1960’s. Normally, the authentication design involves a trusted hardware device (ATM card or token). The Personal Identification Number (PIN) of the card holder’s is usually the only means to attest the identity of the user; this approach is vulnerable to misplacement, unauthorized access, card swallowing, forgetfulness and others. ATM access is not more secure using 4 digits PIN. So we need a strong authentication and the most promising one is implementing biometrics into it [1].

Biometrics refers to an automatic recognition of a person based on her behavioral and/or physiological characteristics. The main reason for introducing biometric systems is to increase overall security. Biometrics offers greater security and convenience than traditional methods of personal recognition [5]. Biometric tokens are the safest means of preventing ATM frauds. The most widely used biometric tokens are finger prints, irises, faces and palms. The fraudster may match everything but they can never match the biometric peculiarities [3]. 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. Fingerprint-based systems have been proven to be very effective in protecting information and resources in a large area of applications.

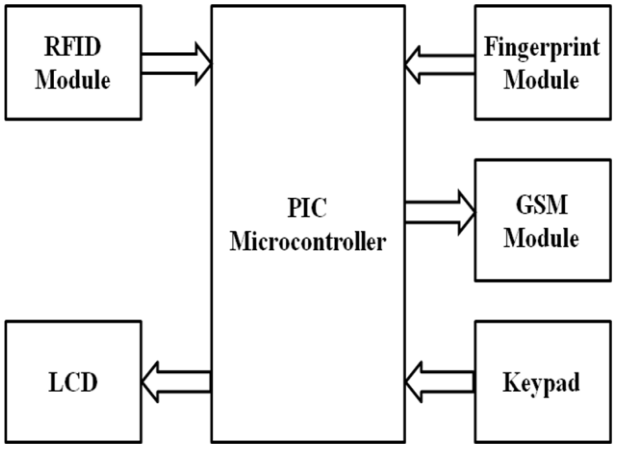

Figure 1: Block diagram

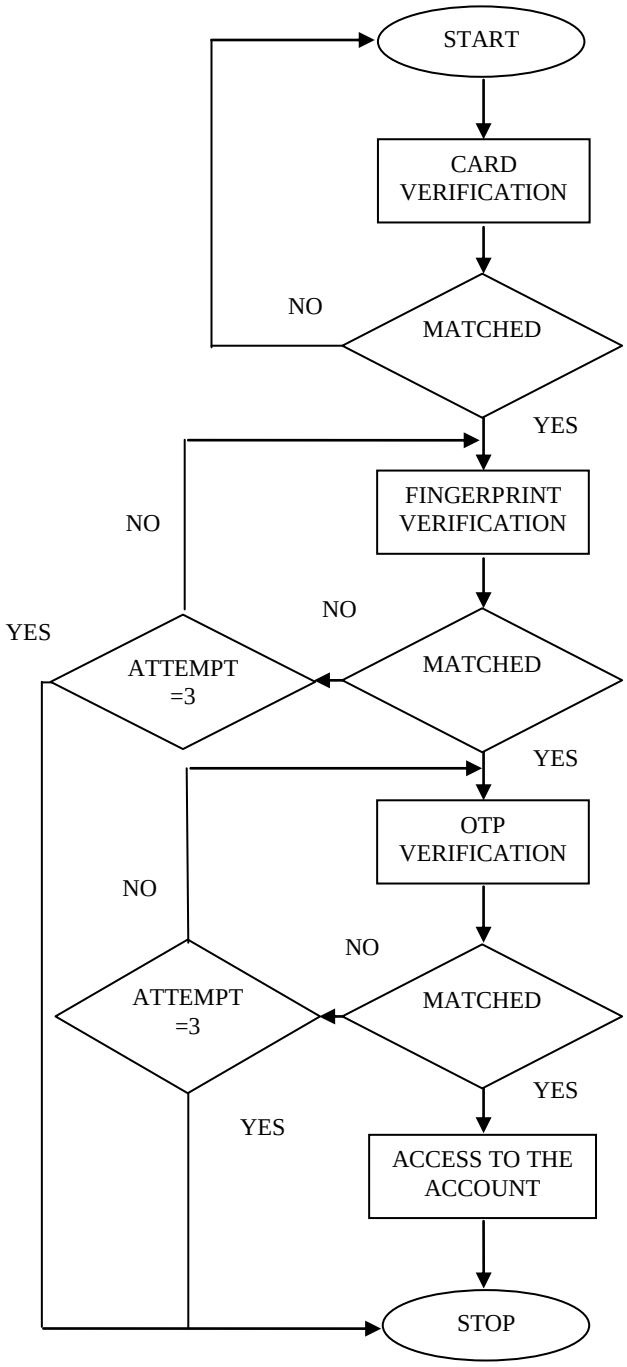

Figure 2: Flow chart of proposed system

The proposed system is a three level authentication structure. The user have ATM card as in the existing system. If the card is an authenticated one then it asks for the fingerprint. After the successful recognition of the fingerprint the system generate an OTP to user's mobile through SMS using a GSM module. Only after these three levels, a user can access the account further. The transaction is denied either if fingerprint and/or OTP mismatch or in case of entered more than three times.

. There are two types of user for an ATM card-a main user and nominee. The security measures for nominees are based on OTP and fingerprint recognition, while the main user has some more additional features. The main user may also need to go through the OTP and fingerprint security methods. If the authentication succeeds, the admin or the main user can change settings or withdraw the cash or check the balance. Change of settings involves an addition of a new nominee or removal of an existing nominee. The nominee has no rights to change the settings, but can withdraw the cash and check the balance.

IV. ADVANTAGES OF PROPOSED SYSTEM

The proposed system is cost-effective and much secured compared with the PIN-base ATM card. It includes basic security to protect the information from unauthorized access and loss. The nominee user can also be included so instead of the main user the nominee can access the account in case of emergency. No need to memorize the countless password or PIN as biometric technology does not require the pin as user's body become the password. Biometric features cannot be easily hacked because of its uniqueness.

V. CONCLUSION

This paper proposed the new approach for existing ATM system for providing more security using biometric features which plays an important role because they are unique and not easily hackable. The proposed system hybridizes feature-based fingerprint and OTP to provide reliable and fool-proof ATM authentication. The biometric-based recognition will have a great influence on the way we conduct our daily business in near future. The massive adoption and implementationof the system proposed here will go a long way insolving our ATM security needs.

REFERENCES

[1] 'Review of Biometric Technologies used for ATM Security', Namit Gupta; International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 2, August 2013

[2] 'Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication', Frimpong Twum; International Journal of Science and Engineering Applications Volume 5, Issue 3, 2016, ISSN-2319-7560 (Online)

[3] *B. Batiz-Lazo and R. J. K. Reid.* "Evidence from the patent record on the development of cash dispensing technology" . History of Telecommunications Conference, 2008. Histelcon 2008. IEEE.

[4] 3 Million ATMs Worldwide By 2015, 8 September 2015 [Number of ATMs worldwide expected to hit 1.5 million in December 2005] www.atmmarketplace.com article.

[5] Jain, L.C. et al. (Eds.). 1999. Intelligent Biometric Techniques in Fingerprint and Face Recognition. Boca Raton, FL: CRC Press.