Journal of Experimental Sciences 2020, 11: 22-27
doi: 10.25081/jes.2020.v11.6201
http://updatepublishing.com/journal/index.php/jes

Research Article

ISSN: 2218-1768

ATM Shield: Analysis of Multitier Security Issues of ATM in the Context of Bangladesh

Md. Raqibul Hasan Rumman[1], Atish Sarker[1], Md. Majharul Islam[2]*, Md. Imdadul Hoque[3], Robin Kuri[3], Md. Babar Ali Bhuyan[2], Nayeem Al-Tamzid Bhuiyan[4]

[1]Department of Computer Science and Engineering, Military Institute of Science and Technology, Bangladesh, [2]Department of Information and Communication Engineering, Noakhali Science and Technology University, Bangladesh, [3]Department of Computer Science and Telecommunication Engineering, Noakhali Science and Technology University, Bangladesh, [4]Department of Electrical and Computer Engineering, North South University, Bangladesh

Received: February 09, 2020
Accepted: May 03, 2020
Published: May 16, 2020

***Corresponding Author:**
Md. Majharul Islam
Email: majharulislam.ice@gmail.com

ABSTRACT

Over the last decade, consumers have been largely dependent on and trust the Automatic Teller Machine (ATM) to conveniently meet their banking needs. However, despite the numerous advantages of ATM system, ATM fraud has recently become more widespread. In this paper, we provide an overview of the possible fraudulent activities that may be perpetrated against ATMs and investigates recommended approaches to prevent these types of frauds. In particular, we develop a prototype model for the utilization of three tier security equipped ATM to provide security solutions against must of the well-known breaches. In this research article, the tools and techniques of ATM fraud are contemplated. A secure three layer electronic transaction mechanism of ATM is developed to prevent ATM frauds. In this three layer authentication systems the users can improve ATM security against frauds and crimes.

KEYWORDS: ATM fraud, biometrics, fingerprint verification

INTRODUCTION

Technology is always improving. In recent years, it has risen at an exponential rate. Technology makes everything easier and simpler. In the banking system, we noticed technol-ogy sweeping in and taking over making it easier to deposit and retrieve money. With the advancement of technology, frauds, and exploits in the banking system has increased as well. The need for security and safety of the banks and the retrieval of money has become of utmost importance. Automatic Teller Machines (ATMs) are a self-service banking machine that allows customers to access their bank account without the aid of a bank teller or bank clerk. They are useed for financial transactions, they operate 24 hours a day helping customers to withdraw cash, deposit cash, transfer funds, check account balance, and print statement of account. They are placed in convenient locations such as retail outlets, banking premises, grocery stores, shopping malls, and gas stations [1]. They make banking transactions easier, by helping banks to meet the demands of their customers; customers do not need to go to the banking hall, or even in some cases they do not need to queue in banks just to make basic banking transactions. Some ATM machines allow customers of different banks to perform basic banking transactions without going to their bank or their bank's ATM machine [2]. Despite all these advantages, it has been reported in [3] that customers and banks are faced with a lot of ATM fraud and other ATM security related problems. Therefore, there is a need to provide a means of securing ATM transactions against frauds and crimes. Bangladesh being a developing country needs to look into the security measures as technology takes over every sector including the banks before thieves and hackers can exploit the people more than they already have. We have accounts of ATM threats constantly rising and in recent times it is only increasing. In Bangladesh, there are accounts of fraudulent methods already persistent. In the vision to Digital Bangladesh this is an alarming issue and therefore we have proposed an idea which, although sophisticated may very well making ATM transactions easier and much more secure than the present scenario. This study suggests a multifactor authentication security technique to improve the security and safety of ATM and its users for Financial Institutions in Bangladesh that can help make ATMs more secured. The pro-posed technology includes tri-factor Authentication Scheme. It demonstrates a three tier Authentication structure that offers a simple and secure authentication scheme that takes place at the ATM machine.

MOTIVATION

While we were thinking of the banking system as a whole, we discussed how it is now that we have a lot of banks, and how technology has shaped it. Now a day there is a lot of credit cards and debit cards and other membership cards that it is a hassle to maintain them. Adding to this we also thought of the security perspective of the system and realized that in a developing and populous country like Bangladesh it is necessary to maintain security because there is a growing threat to the people and banks. In recent times there were a lot of attacks and theft of money through ATM scamming and it is on the rise. In Bangladesh alone, there were multiple accounts of theft of the ATMs. This is a matter of personal and also national security. We care about the security of money of every person and so we have thought of improving this. Here lays our motivation to form a system that will be infallible and impenetrable. Then we also thought about how we could make the system easier to handle. In a world of technology, an easy and secure transaction is of sheer importance. We planned to provide just that using simple everyday used mobile phones and put forward a way to easily transact with the banks and make it safe and secure.

LITERATURE REVIEW

Hossain [6] focused on the basic structure and operating system of Automated Teller Machine in Bangladesh. Salam et al [4], (2014) propose multilevel security of ATM transactions gives an insight into how ATM works and how to enhance the security in ATM. In this concept, the author discusses by creating an Android app and the user is supposed to login to the app with a password. Then the card should be swiped and the PIN is entered. The PIN and the password of the app are stored in the database and they are checked for symmetry. After verification, the users should enter the transaction id in the mobile application and all the process is carried out in the mobile phone itself. Only the cash is withdrawn in the ATM. There occurs a problem if both the PIN and password of the App is leaked, then it can be hacked easily. This method improves the alert to the customers to use ATM cash transactions. A Murthy and Reddy [5] developed an embedded fingerprint system, which is used for ATM security applications. In their system, bankers collect customer's fingerprints and mobile numbers while opening accounts, and then customers only access the ATM. The ATM works in such a way that every time a customer places his/her finger on the printing module, the ATM automatically generates a different 4-digit code as a message to the mobile phone of the authorized customer through a GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering the received code, the ATM checks whether the code is valid or not before allowing the customer further access and usage. Since security measures at ATM centers play a significant role in preventing attacks on customers, money, several researches have proposed the use of fingerprint in a like manner of this research, to shift from PIN to three tier based security.

THREATS TO ATM SERVICES

There many threats related to ATM security as the popularity and usage increases incessantly. New ATMs are being installed in different locations daily and the users are also increasing. Some of the threats are discussed below.

Shoulder Surfing: Shoulder surfing is a way of looking over someone's shoulder, to get information. In a crowded environment, it is very easy and effective to stand beside a fellow and watch how PIN numbers are entered at cards terminal [7].

Spoofing: Spoofing is impersonation, getting access and taking advantage of someone else's account [7].

Skimming: This involves the use of card skimmer devices by fraudsters to get card details from the magnetic chip [8]. These devices are usually installed inside or over the top of an ATM card reader.

Card Trapping/Phishing: Card trapping and Phishing attempt to steal card as the customer insert it into the ATM for transaction [9]. A device is placed over or inside the card slot to capture the consumer's card. These devices are designed to prevent the card from being returned to the consumer after transaction.

PIN Cracking: ATM PIN is the primary security against ATM fraud. For cracking the PIN, the program is written in such a way that tries the PIN for particular account and this require average of 5000 transactions to discover each PIN. Also hackers have only three guesses to match against 10,000 PINS.

Reply Attacks: Here, attackers spy the conversation between the sender and receiver and takes important information e.g. sharing key and then contact to the receiver with that key. In Replay attack the attacker gives the proof of his identity and authenticity.

ATM Hacking: Attackers use sophisticated programming techniques to break into websites which reside on a financial institution's network. Using this access, they can access the bank's systems to locate the ATM database and hence collect card information which can be used later to create a clone card. Hacking is also commonly used to describe attacks against card processors and other components of the transaction processing network. Most of the ATM hackings are due to the use of non-secure ATM software.

Physical Attack: ATM physical attacks are attempted on the safe inside the ATM, through mechanical or thermal means with the intention of breaking the safe to collect the cash inside. Some of the most common methods include ram raids, explosive attacks and cutting. Robbery can also occur when ATMs are being replenished or serviced. Staffs are either held up as they are carrying money to or from an ATM, or when the ATM safe is open and cash cassettes replaced. There are a variety of mechanical and physical factors that can inhibit attacks to the safe.

Current Alert: The stolen money was not slashed from any customer's account as the fraudsters disconnected the machines from the main server first.

SYSTEM ANALYSIS

A. How ATM Works

ATMs have a small display and either touch screen or input devices for entering inputs. To access their bank account, customers insert a plastic card into the magnetic stride reader. The plastic cards are issued by the holder's bank. The magnetic stride card contains an identification code that is transmitted to the banks central computer through a host computer. This identification code identifies the holder of the ATM card. The ATM asks for a PIN which is use to authenticate the user. If the user is authenticated, the ATM permits the transaction with the banking computer [6]. The basic ATM working relation is given in Fig. 1.

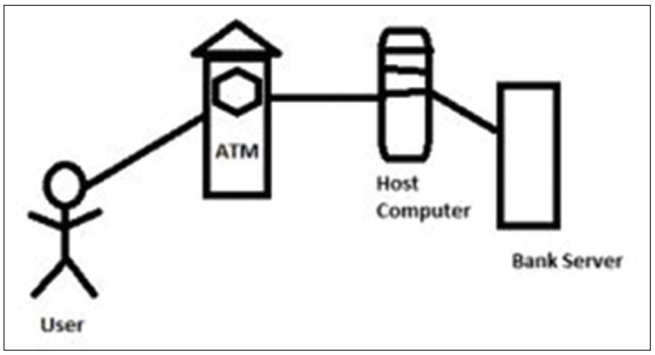

Figure 1: Basic ATM working relation

B. Existing ATM Security Technology

With the growing security threats on banks, banking industries have been adopting new technologies to secure banking transactions. One of the recent technologies adopted by banks is the two factor authentication which often combines the use of PIN and One Time Password (OTP) for user's authentica-tion. In two factor authentication method, first the customer enters the PIN, if the PIN is validated; the bank computer generates and sends an OTP to the customer's mobile phone via SMS. The customer enters the received OTP. If the OTP entered by the customer corresponds to the OTP generated by the bank computer, the customer is authenticated and the transaction is permitted. This OTP password is only valid for one log on after which it is discarded. The two factor authentication method is illustrated in Fig. 2.

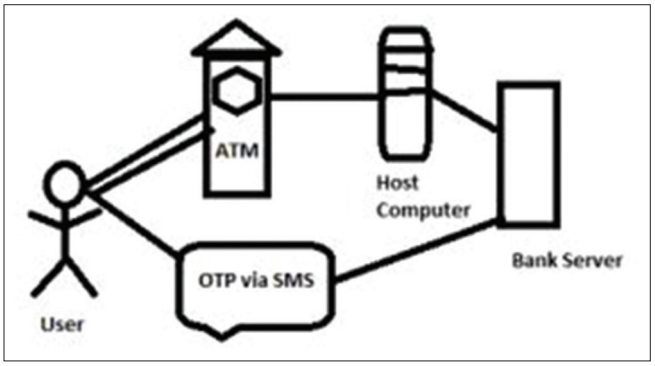

Figure 2: Two factor authentication in ATM

C. Our Objective

Credit card fraud is a major problem in today's world. Financial institutions has registered field loses currently due to users being unprotected of their assets and card informa-tion. The present system of authentication of ATM is mostly dependent on pin-based verification. Factors such as urgency, memorization of pins, speed of interaction, unintentional pin sharing affect diversely for the current system. There are many threats regarding ATM like shoulder-surfing or observation attacks, including card skimming and video recording with hidden cameras while users perform PIN-based authentication at ATM terminals is one of the common threats for common users. Cards with magnetic strips are easy to clone. Card-less transaction are getting popular, where users can use mobiles phones to perform the financial transaction. Researchers have struggled to come up with secure solutions for secure PIN authentication. So our target is to:

- Finding the major vulnerabilities
- Detect the unsecure security portion
- Provide an authenticated tri way security system via QR code and biometric and PIN which is more compatible with the vulnerabilities

We want to ensure that networks are secure, so if one ATM is hacked, fraudsters can't infect the entire ATM network.

METHODOLOGY

In this work, we suggest a multifactor authentication security technique to improve the security and safety of ATM and its users for Financial Institutions in Bangladesh. This technique is called ATM tri-factor Authentication Scheme. It demonstrates a three tier Authentication structure that offers a simple and secure authentication scheme. The first tier is the biometric authentication using fingerprint. The second tier is the QR code authentication using GSM smart phones as scanners. The third tier is PIN authentication. The proposed scheme improves on the existing authentication scheme to make the ATM authentication more secured against fraud. Also we determine the performance evaluation of proposed scheme by comparing the security performance of existing authentication schemes. Our proposal is not replacing the existing security technology, rather it serves as an additional layer of security that protects the existing authentication system from frauds and crimes. Card and PIN security authentication system has very serious security challenges and as such we propose Three-Factor based Authentication Scheme offers a simple and secure authentication scheme.

i. The first tier is the biometric authentication using fingerprint.
ii. The second tier is the QR code authentication using GSM smartphones as scanners.
iii. The third tier is PIN authentication.

A. Biometric Authentication Using Fingerprint

We choose The Minutiae-based processing due to its popularity and it's a well-known method for fingerprint verification. It's

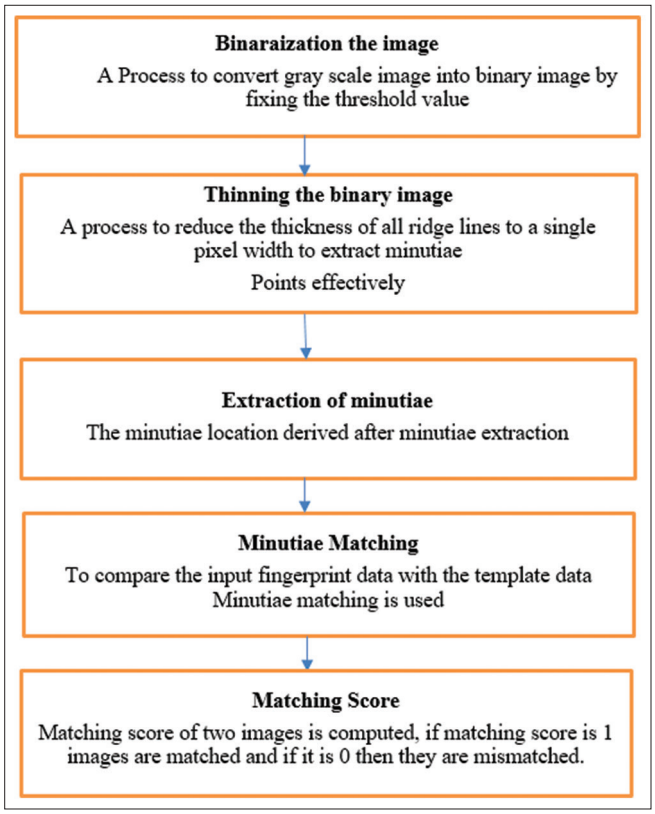

Figure 3: Block diagram for fingerprint authentication

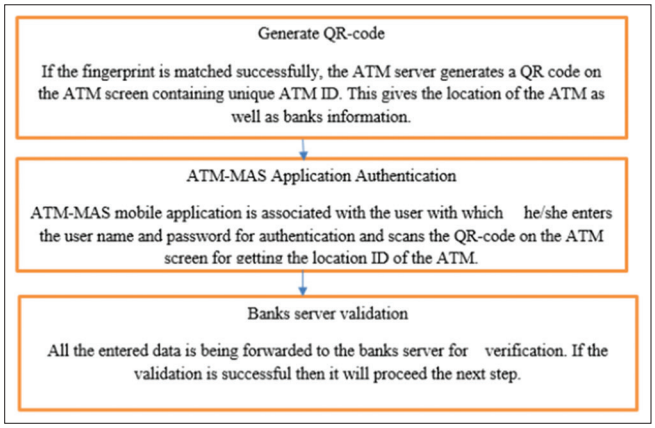

Figure 4: Block diagram of the QR-code authentication using GSM

the foremost popular ones being included in most existing fingerprint identification and verification systems. Minutiae are small points of interest within the fingerprint image. The minutiae- based method recognition in two stages (Fig. 3) (i.e. minutiae extraction and minutiae matching).

Algorithm
Input: User's fingerprint image (Grey-scale)
Output: Verified fingerprint image with matching score

1. First we convert the grey-scale image to binary image (Binarized).
2. Thinning the images to remove selected foreground pixels from binary images.

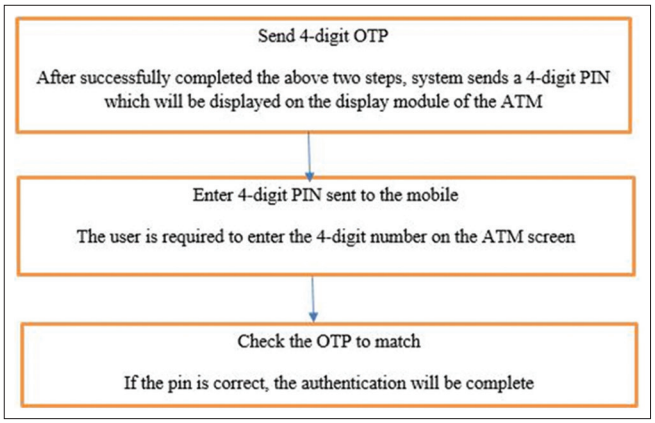

Figure 5: Block diagram for PIN authentication

3. The next step is extraction of minutiae points.
4. To generate the data matrix for getting the orientation, position and type of minutiae.
5. Minutiae Matching - To compare the input fingerprint data with the template data.
6. Matching Score - It is used to calculate the matching score between the input and template data

Advantages of Biometric Fingerprint Authentication:
i. Biometric security system is very convenient and versatile for both the using and managing.
ii. It provides the more accurate identification.
iii. Biometric security systems are designed with ease of use in mind and give you accurate results with minimal effort thus it is efficient

B. QR Code Authentication Using GSM Smartphones

After successfully fingerprint validation the next step will be the validation of QR code using GSM smartphones (Fig. 4). Smart phones with GSM technology are easy to use and versatile. They are increasingly utilized in all life fields, especially with the wide spread of smart phones which are used as QR code scanners. The process is depicted in the following flow diagram:

Algorithm
1. Generate QR-code.
2. ATM-MAS Application Authentication.
3. Banks server validation.

Advantages of QR Code authentication:
i. It is easy to access.
ii. Cost Effective.
iii. Ease to assessment and repair

C. PIN Authentication

After successfully validation of fingerprint authentication and QR-code validation, our next step is PIN number authentication (Fig. 5). This makes the whole system more authentic and increase the security level. The process is depicted in the following flow diagram:

Figure 6: Overall system flow diagram

Algorithm
Input: 4 digit PINS
Output: Matching the OTP

1. Generates 4 digits pin
2. Input the PINS for matching
3. Validate or Matching the PIN

SYSTEM DESIGN

Our design requires minimal overhead computation on the personal devices with most operations sent to the server and does not impose any hardware-oriented requirements on the terminals. The major benefit for our model is that it is more reliable and time saving as well as faster. Also it is a card less system that means customer don't need to carry any card thus provides the flexibility. It is secure against shoulder surfing attacks, reply attacks, skimming and partial observation. So the overall flow diagram looks like (Fig. 6):

ADVANTAGES OF PROPOSED SYSTEM

1) Multilevel security at client side using cryptography algorithm and user's biometric features.
2) Biometric features cannot be easily hack because of its unique identification
3) QR code generation via mobile phone
4) At server side steganography algorithm is used for hiding the encrypted information.

CONCLUSION

The network needs security against attackers and hackers. Network Security includes basic securities to protect the information from unauthorized access and loss. ATM access is not more secure using 4 digits PIN. The Proposed idea will confuse the Password guessing and password thieving in future from unauthorized person. Therefore this kind of additional technique preventing pin theft in future. ATM authentication using PIN-based entry is highly susceptible to shoulder-surfing or observation attacks. Credit/Debit cards are also not resilient to relay and other skimming and cloning attacks. In this paper, we propose the ATM custodian for ATM, a unique biometric and QR code based authentication service for ATMs using personal mobile. We have focused the security design for this system is based on visual privacy of users for QR code scanning and address the security vulnerabilities in PIN-based authentication. This paper proposed the new approach for existing ATM system for providing more security using three shield tire features which plays an important role because these are unique and not easily hackable.

CONFLICT OF INTERESTS

The authors declare that they have no competing interests.

SOURCES OF FINANCIAL SUPPORT

There is no funding to be disclosed.

REFERENCES

1. Qadrei A, Habib S. Allocation of heterogeneous banks' automated teller machines. In2009 First International Conference on Intensive Applications and Services 2009 Apr 20 (pp. 16-21). IEEE.
2. ATM of Banks: Fair Pricing and Enhanced Access - Draft Approach Paper, Reserve bank of India, Technical report, 2007.
3. ATM crime: Overview of the European situation and golden rules on how to avoid it, European Network and Information Security Agency, Aug. 2009, Technical Report.
4. Salam A, Ali A. Multi-Level Security for ATM Transaction. International Journal of Computer Applications.;975:8887.
5. Krishnamurthy P, Redddy MM. Implementation of ATM Security by Using Fingerprint recognition and GSM. International Journal of Electronics Communication and Computer Engineering. 2012;3(1):1-4.

6. Hossain M, Bari R. *Unerstanding of ATM (Automated Teller Machine) in Bangladesh* (Doctoral dissertation, BRAC university).
7. De Luca A, Von Zezschwitz E, Pichler L, Hussmann H. Using fake cursors to secure on-screen password entry. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2013 Apr 27 (pp. 2399-2402).
8. Bhatla TP, Prabhu V, Dua A. Understanding credit card frauds. Cards business review. 2003 Jun;1(6):1-5.
9. Roland M, Langer J. Cloning Credit Cards: A Combined Pre-play and Downgrade Attack on {EMV} Contactless. In Presented as part of the 7th {USENIX} Workshop on Offensive Technologies 2013.