International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 05 | May 2018 www.irjet.net p-ISSN: 2395-0072

A Comparative Study of PIN Based and Three-factor Based Authentication Technique for Improved ATM Security

Ojekudo Nathaniel[1], Macarthy Osuo-Genseleke[2]

[1,2] Dept . of Computer Science, Ignatius Ajuru University of Education, Port-Harcourt, Rivers State, Nigeria

---

Abstract - *The rapid increase of technology used in financial institutions has greatly impacted on financial activities and electronic transactions. One of such technologies is the development of Automated Teller Machine (ATM). This technology requires secured, fast and accurate techniques for user identification and authentication which has been a problem. Financial institutions has registered loses because users are being unprotected of their assets and card information. The present ATM security authentication technique is dependent on pin-based verification. Factors such as urgency, memorization of pins, speed of interaction, unintentional pin sharing affects the system diversely. Cards with magnetic chips are easy to clone. This paper presents a comparative study of traditional Pin based authentication technique and a proposed three-factor based authentication technique. The three-factor authentication scheme proposed in this paper integrates biometric fingerprint, PIN and QR-Code technologies to provide improved security for ATM authentication.*

Key Words: **Authentication, Card, Pin Authentication, Biometric Authentication, ATM, Embedded system, Electronic transaction.**

1. INTRODUCTION

The use of ATM (Automated Teller Machine) technologies in financial institutions has greatly impacted on our financial activities. ATM is very popular and most efficient way for transaction of money. ATM also known as cash point, cash machine, etc is a system whose roots originates from the records of a banking institution [1] and [2]. It dispenses cash to customers and could be used to perform other financial transactions without going to the banking hall (Biometrics Overview, 2012). It reduces the work load of banks. Currently, Personal identification number (PIN) is the authentication technique applied on ATM for the security and protection of customers financial details from access by third parties [1].

As Automated Teller Machine (ATM) is becoming common, ATM frauds also are increasing. Crimes at ATM are a nationwide problem that customers and bank operators are faced continuously in recent years [3]. Traditional ATM authentication which is by card and PIN has some lapses [4]. Once account holders card is missing, PIN known, account holder is exposed to fraud. New techniques are being developed to beat security issues of ATM PIN and efficiency is judged based on speed, security, and memory capacity as compared with ancient PIN authentication. Biometric authentication technology may solve this problem since one's biometric data cannot be mimicked and lost, etc. Biometrics authentication ensures identification base on a physiological or behavioral characteristic [5].

In this work, we compare traditional Pin based authentication technique and a proposed three-factor based authentication technique. The three-factor authentication scheme proposed in this paper integrates biometric fingerprint, PIN and QR-Code technologies to provide improved security for ATM authentication.

2. RELATED LITERATURE

2.1 Research Background

Identification is the establishment of identity. Authentication confirms claim by use of identity. PIN authentication technique has many problems. Biometrics is best for authentication today and is realistic [6]. Multifactor authentication technique will enhance banking transactions via ATM. Technique proposed in our work involves three authentications techniques to further enhance ATM usage and operations.

2.2 Related Work

Shuffled ATM keypad method and they develop Bluetooth application to overcome the shortfalls of PIN entry was proposed by [7]. This method shows numbers in the Liquid Crystal Display keypad and communicates the password through the wireless medium.

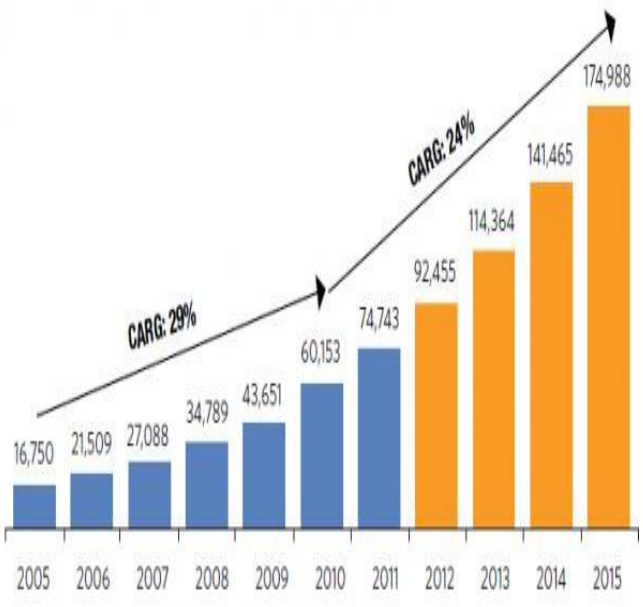

Fig-1: ATM user's growth rate

Source: Edelweiss IB Estimates; Assumed a 24% growth rate for the period 2012-2015

A novel cardholder verification method was proposed by [8]. It gives the user the flexibility to add one or more extra RFID devices like smart watches, smart phones, rings, necklaces, and bracelets and select a suitable security level for use. The Black and White (BW) Method was proposed by [9]. Our popularly known numeric keypad is colored at random, part black and the other white. Only users with correct PIN digit can answer the colors. A keyboard using fake cursor that hides password entry on screen was presented by [10]. In this system, only one cursor is for actual input while others are distraction for third parties.

Forensic Analysis of Skimming Devices for Credit Fraud Detection was proposed by [11]. Magnetic stripe cards are widely used by many different administrations to provide both convenience and security. These types of cards are often trusted on identification and personal authentication. However, they are not designed to withstand attacks that use the sophisticated technologies available today. An object detection method Crime Detection and Avoidance in ATM was proposed by [12]. This method used multiple object detection and event recognition techniques of computer vision.

2.3 Threats to ATM Services

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

2.3.1 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 [10].

2.3.2 Spoofing

Spoofing is impersonation, getting access and taking advantage of someone else's account. [10].

2.3.3 Skimming

This involves the use of card skimmer devices by fraudsters to get card details from the magnetic chip [13]. These devices are usually installed inside or over the top of an ATM card reader.

2.3.4 Card Trapping/Phishing

Card trapping and Phishing attempt to steal card as the customer insert it into the ATM for transaction [14]. 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.

2.3.5 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.

3. ATM SECURITY AUTHENTICATION TECHNIQUES

From the inception of electronic transactions in financial institutions, PIN (4-digit number) is the authentication technique applied on ATM. PIN is employed to verify a client during fund transaction at cash dispenser terminal. In year 2011, First Bank of Nigeria PLC successfully deployed the first Biometric ATM using fingerprint biometric authentication (not in circulation) in addition to the existing PIN authentication technique to enhance security on cards and its terminals. [15].

3.1 Pin Based Authentication

3.1.1 System Architecture

A PIN pad or PIN entry device is important in every debit, credit or sensible card-based dealings to simply accept and cipher the cardholder's Personal Identification Number (PIN). PIN entry technique is usually used for cash dispenser machine, associate integrated purpose of sale devices among that associate electronic till is chargeable for taking the sale quantity and initiating/handling the dealings.

3.1.2 Processing Mode:

The PIN is employed to verify a client (the user of a bank card) at intervals associate degree electronic funds transfer system, and (typically) to authorize the transfer of funds, thus it's necessary to guard it against unauthorized access or misuse. Fashionable banking systems want ability between totally different card issuers, effort banks and retailers as well as transmission of PINs between those entities thus a standard set of rules for handling and securing PINs is required to confirm technical compatibility and a reciprocally in agreement level of security

3.1.3 Technology Used

The private number (PIN) is common authentication technique employed in varied devices like ATM's, mobile devices and electronic door locks. This PIN entry technique is injured to shoulder surfboarding attack (SSA). Once user enters their number in inhabited place, assailant observes the number over their shoulder. This is often referred to as shoulder surfboarding attack.

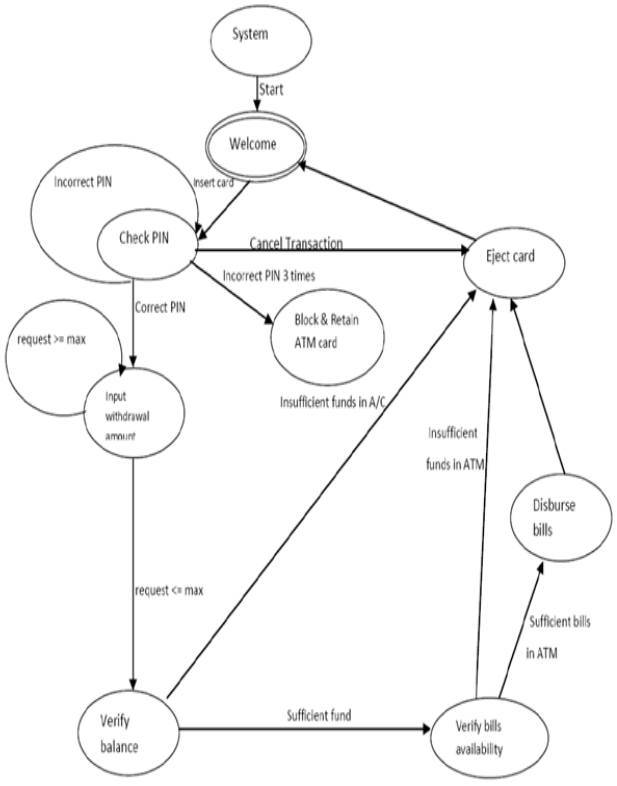

Fig- 2: System Architecture for PIN Based Authentication, Source: Muhammad et al., 2015.

3.1.4 Advantages of PIN Based security technique

i. Provides an easy authentication process for the user.
ii. It saves time as not too many steps are required for authentication.
iii. In the case of missing/stolen ATM cards or forgotten PIN, this can be easily rectified by the bank.

3.1.5 Disadvantages of PIN Based security technique

i. The holder of the card with its PIN becomes the owner of the account at that instance.
ii. High possibility of misuse of missing or stolen card.
iii. It's expensive and time consuming for the bank to generate a new card, if card is stolen /lost.

3.2 Three-Factor Based Authentication

The proposed three-factor based authentication technique integrates Biometric fingerprint and QR-Code technologies with the traditional PIN based authentication technique discussed in section 3.1 above. In this section, biometric fingerprint and QR-Code authentication techniques are discussed.

3.2.1 Biometric Authentication Using Finger Print

a) System Architecture

Biometric is the physical characteristics of the human body. Some of these characteristics are used for authentication hence known as Biometric authentication.

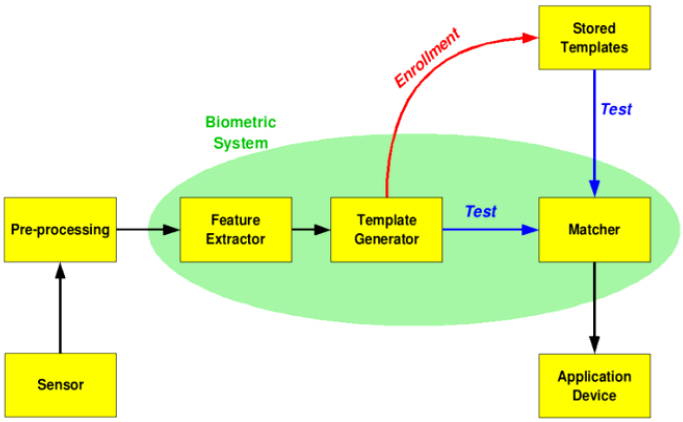

Fig-3: Architecture of Biometric Authentication System (Biometric System Diagram, 2014)

Biometric characteristics identification can be either physiological or behavioral. Once the behavior of a person is used for authentication, its classified as behavioral authentication e.g. signature, etc. while the shape of the body is classified as physiological e.g. finger, etc. Technologies have been developed to recognize these human characteristics for authentication. This authentication technique has great advantage over the traditional method (PIN), it cannot be forged, stolen, etc. as such if combined

with PIN authentication method it will enhance the security of ATMs and its users.

b) Processing Mode

During authentication and processing at the card terminal, the card holder is expected to provide its biometric characteristics; this is to be matched with the already existing sample in the database of his bank. if both features correspond, the card holder is considered to be a valid user. Approximate match can be considered because there are situations where discrepancies might arise due to some certain factors like finger cuts, etc. Situations like this are to be addressed during account opening by creating many samples of a particular type of user biometric features, average taken and stored in the user's database so different situation of users' features can allow the user access to her transaction (Luca et al., 2010). The figure below shows the working process of biometric authentication.

Fig-4. Biometric ATMs (Biometric ATMs, 2010)

c) Technology Used

Creation of account for account holder with biometric feature. Storage of account holders biometric feature in the database. At the ATM stand, the user is expected to provide sample of its biometric feature e.g. finger print, select a bank thereafter, a Virtual Account Identification (V-ID) is generated by the system. This V-ID is sent to the server through the network in an encrypted form (e.g. SSL) while the sample is decrypted and compared with the one stored in the database in the server. If both samples match, the users is authenticated for further transactions else session is terminated.

d) Advantages of Biometric based ATMS

i. Provides strong authentication.
ii. A trusted third parties detail can be used during account opening for authentication.
iii. It reduces bank cost, time and efforts for card processing.
iv. Accounts are assessed as per convenience.
v. Operation of account is solely for account holder.
vi. Its multiple authentications and time consuming but its technology is fast and efficient.

e) Disadvantages with biometric Authentication

i. Installation is expensive.
ii. Biometrics techniques like hand geometry, fingerprint and face recognition (which can be done from a camera across the room) are not quite enveloping, but people have real concerns about peering (hard to watch) into a laser beam or strictly a finger into a slot.
iii. Devices are expensive.
iv. All biometrics readers use sampling and establish a threshold for when a match is close enough to accept. The device has to sample the biometric, measure often hundreds of key point, and compare that set of measurements with a template. There is normal variability.
v. False reading equipment exists although there is improvement.

3.2.2 QR - CODE Using Smartphone with GSM Technology

a) System Architecture

Quick Response codes are two dimensional barcodes that can be used to efficiently store data. They are increasingly used in all life fields, especially with the wide spread of smart phones which are used as QR code scanners.

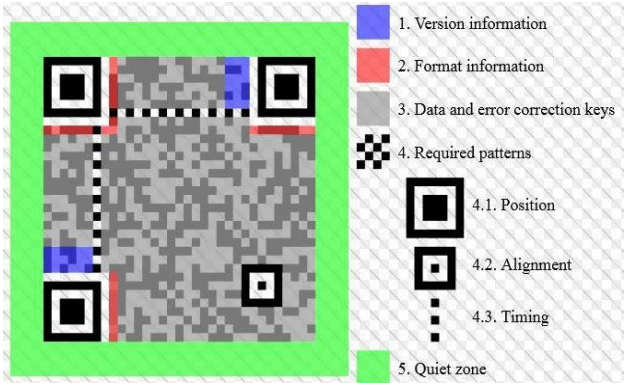

Fig-5: Functioning of a quick response code

b) Processing Mode

Data is presented as square dots with specific pattern. Quick Response scanners read this image and retrieve the stored data based on the pattern of square dots. It has large capacity, it encodes data, its resistant to damage, its reading speed is high, its print out size is small, it reads round the clock and has a structural flexibility of application.

Smart phones with GSM technology are easy to use and versatile. The device has the capacity to stores huge amounts of codes that is scanned with ease and stored onto a mobile phone device.

c) Technology Used

QR Code uses the ISO/IEC 18004:2006 which is an Information technology standard used for data encoding. It is a technique that automatically identifies and captures data. Smart phone devices with GSM technology are used as QR code scanners. The embedded camera in the smart phone captures an image of the QR code, then an application analyses the pattern of square dots to retrieve the encoded data and display it in a useful form make them very popular.

d) Advantages of Proposed System

- It is a more reliable and time saving system
- It is more efficient and faster to use.
- The system is a card less system, so no ATM card is needed and users do not need to memorize PIN.
- It is secure against shoulder surfing attacks, relay, replay attacks, skimming, and partial observation and cloning.

e) Disadvantages of Proposed System

The need of advanced security innovations is an increasing concern for financial institutions in Nigeria due to the constantly increasing threats to data in a networked computer environment. Password implementations based on Text is easy to Hack. Hacking One Time Password (OTP) can be easily done by hacking email account. Another viable option is the image based authentication. This type of authentication also surfer setback as hackers can easily understand image selection and click points by shoulder surfing attack. ATM-MAS authentication system generates unique alphanumeric OTP generation via mobile when QR-code scan is successful. The new users register their mobile number, fingerprint for biometric authentication and other required personal details such as name and address.

4. COMPARISON OF PIN BASED AND PROPOSED THREE FACTOR AUTHENTICATION TECHNIQUES

The comparison is carried out based on factors including system architecture, processing mode and the technology used as shown in Table 1 below;

Table -1: Comparison of Pin based and the proposed three factor based authentication Techniques

SCIENTIFIC FEATURES	PIN BASED	THREE-FACTOR BASED
SYSTEM ARCHITECTURE	Sensible card-based with magnetic chips. Has a PIN pad entry device.	Memory module, Processor, Fingerprint scanner, Display module, Network controller module, Smart phone, Input module, etc
PROCESSING MODE	The card is inserted into the ATM. PIN is entered to verify and authenticate a client	The client places her finger print on the finger print module. A QR code is generated. A Smart phone scans the QR Code to establish co-location and a one-time secret PIN is generated for authentication and processing.
TECHNOLOGY USED	A private number (PIN).	Fingerprint scan, smartphone with GSM Technology, QR-Code, and PIN pad entry device.

4.1 Result and Discussion

Present ATM security authentication process commences as the customer inserts a card into its terminal. These cards are plastic having magnetic chip. The customer's account details are embedded in the magnetic chip. The customer authentication is further ensured using a four-digit PIN that is attached to the ATM card. Authentication is performed when the user inserts the ATM-card in the slot on the ATM machine and provides the unique PIN correctly. There are various threats to this type of authentication. Though First Bank PLC in 2011 lunched fingerprint biometric security authentication in Nigeria, in addition to PIN but not yet in circulation. Card and PIN security authentication system has very serious security challenges and as such we propose Three-Factor based Authentication Scheme that integrates Fingerprint technology, QR-Code Technology and the traditional PIN based authentication scheme for improved ATM security. This technique overcomes most of these security problems. Security experts and researchers have also proposed biometric (irish scan) and PIN identification authentication for the future.

5. CONCLUSIONS

In this paper, we first compared Pin Based Authentication and the techniques integrated in the proposed three factor system including Biometric fingerprint authentication and QR-Code using Smartphone with GSM technology. The comparison was done based on their system architecture, possessing mode, and technology used. ATM authentication using PIN-based entry is highly susceptible to shoulder-surfing or observation attacks. The proposed Three-Factor authentication scheme integrates Biometric fingerprint, PIN

and QR-Code technologies to successfully provide improved security for ATM authentication.

REFERENCES

[1] S.S. Das, and J. Debbarma, "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-banking System," International Journal of Information and Communication Technology Research (IJRCTR), Volume 6, Issue 12, December 2011.

[2] W.W.N. Wan, C.L. Luk, and C.W.C. Chow, "Customers Adoption of Banking Channels in Hong Kong," International Journal of Bank Marketing (IJBM), Volume 41, Issues 5, May 2005.

[3] B. Richard, and M. Alemayehu, "Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons." Journal of Internet Banking and Commerce, Volume 12, Issue 3, March 2006.

[4] P.K. Amurthy, and M.S. Reddy, "Implementation of ATM Security by Using Fingerprint recognition and GSM." International Journal of Electronics Communication and Computer Engineering, Volume 20, Isssue 4, April 2012, pp. 83-86.

[5] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Generating Cancellable Fingerprint Templates." IEEE Transaction on Pattern Analysis and Machine Intelligence, Volume 31, Issue 2, February 2007. pp. 4.

[6] K. Laudon, and C.G Traver, E-Commerce Second Edition, Pearson Education Pvt. Ltd, Singapore, July 2005,237-239.

[7] S. Kumaresan, G.D. Kumar, S. Radhika, "Design of Secured ATM by Wireless Password Transfer and Shuffling Keypad," In IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems, July 2015 pp. 325-329.

[8] A. Abdulrahman, A. Arwa, C. Xiuzhen, and B. Rongfang, A novel verification method for payment card systems, In Springer-Verlag London, May 2015,pp. 1145-1156.

[9] L. Mun-Kyu, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN Entry," In IEEE Transactions on Information Forensics and Security, August 2014,pp. 1556-6013.

[10] A.D. Luca, E.V. Zezschwitz, L. Pichler, and H. Hussmann, H, "Using Fake Cursors to Secure on-screen Password Entry," in Proceedings of CHI, June 2013, pp. 2399–2402.

[11] G. Hong, and J. Bo, "Forensic Analysis of Skimming Devices for Credit Fraud Detection," 2nd IEEE International Conference on Information and Financial Engineering (ICIFE), September 2010, pp. 542 – 546.

[12] B. Sujith, "Crime Detection and Avoidance in ATM: A New Framework," International Journal of Computer Science and Information Technologies, Volume 24, Issue 5, May 2014, pp. 210-222.

[13] T.P. Bhatla, V. Prabhu, and A. Dua, Understanding Credit Card Frauds," Cards Business Review, January 2003.

[14] M. Roland, and J. Langer, "Cloning credit cards: A combined pre-play and downgrade attack on EMV contactless," In Proceedings of the 7th USENIX Workshop on Offensive Technologies, June 2013, pp. 324-348.

[15] First Biometric ATM in Nigeria (2011, April 12). Retrieved April 14, 2018, from Gistmania: http://www.gistmania.com/talk/topic,64655.0.html