Implementation of Multifactor based Authentication Scheme for Enhanced ATM Security

Macarthy O-Genseleke
Dept. of Computer Science
Ignatius Ajuru University of Education, Port-Harcourt, Nigeria

Osuigbo Ebenezer N.
Dept. of Computer Science
Kenule Beeson Saro-Wiwa Polytechnic, Bori, River State, Nigeria

Chioma Chigozie-Okwum
Dept. of Computer Science
Federal College of Land Resources Technology, Owerri, Nigeria

ABSTRACT

The main objective of this work is to develop an authentication scheme that will enhance ATM security using multifactor based authentication scheme, which combines Biometric Fingerprint, PIN and QR-Code authentication. In these system, Bankers will collect the customers finger print and mobile number while opening the accounts then customer only accesses ATM machine. The working of this ATM machine is when customer places finger on the finger print module when its access automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer should be entered by pressing the keys on the screen. After entering it checks whether it is a valid one or not and allows the customer further access.

General Terms

Authentication, Card, Pin Authentication, Biometric Authentication, Automated Teller Machine (ATM), Embedded system, Electronic transaction.

Keywords

ATM-MAS, QR-Code, Fingerprint,

1. INTRODUCTION

The use of ATM (Automated Teller Machine) technologies in financial institutions of Nigeria 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 (Das and Debbarma, 2011) and (Wan et al., 2005). 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 (Das and Debbarma, 2011).

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 (Richard and Alemayehu, 2006). Traditional ATM authentication is by card which can be credit, debit, or smart and PIN (Amurthy and Reddy, 2012). Once account holders card is missing, PIN known, account holder is exposed to fraud. The existing authentication schemes used in ATMs has brought about frustration to users as a result of transaction frauds and crime associated with the use of ATMs in recent times. Current ATM authentication is based on card and PIN, some security challenges such as Shoulder Surfing, Spoofing, Skimming, Card Trapping/Fishing, Reply Attacks are eminent, hence, the need of a more secured and efficient authentication technique for ATM. New authentication techniques are being developed to beat security issues of ATM PIN. The efficiency of these techniques 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 (Ratha et al., 2007). Biometrics features include fingerprint, hand or palm geometry, retina, iris and face while behavioral features are signature and voice.

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 Nigeria. This technique is called ATM Multifactor Authentication Scheme (ATM-MAS). 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.

2. METHODOLOGY

The proposed system, Automated Teller Machine-Multifactor Authentication Scheme (ATM-MAS), gives us the opportunity to perform ATM transactions without having any ATM card and by help of One Time Password (OTP) and PIN combination to remove security concern to authenticate user (Ojekudo Nathaniel and Macarthy Osuo-Genseleke, 2018).

The System was designed in a way that the user gains access to the ATM using fingerprint biometric authentication. The user accesses an ATM terminal and place finger on the fingerprint scanner module for authentication. If the fingerprint matches the user details in the bank's server, the server generates a QR-code on the ATM screen which contains the unique ATM ID. The Unique ATM ID gives information about the ATM such as its location and the bank that owns the ATM terminal. In this, ATM-MAS mobile application is associated with the user with which he/she enters the user name and password for authentication and scans the QR-code on the ATM screen for getting the location ID of the ATM. All the entered data is being forwarded to the banks server for verification purpose. If is successful, the system sends an 8-digit PIN in which only 4-digits will be displayed on the display module of the ATM. The remaining

4-digits is then sent to the user via the smartphone. The user is required to enter the 4-digit number on the ATM screen. Thus the authentication will be complete. The user can proceed to complete transaction process by entering the required transaction details. Upon receiving all the details, the bank server creates a corresponding QR-code which is sent to the ATM screen. The user uses the smart phone to scan the QR code for verifying the account transaction. Finally, the system checks if both the QR code sent to the ATM screen and that which has been received by the server are same. If they match each other the transaction becomes successful. The QR code which is sent to the ATM screen contains the machine location ID and is continuously changing to ensure a better security for the system.

The protocol used in this system is immune to shoulder-surfing attackers, and ensures resistance against relay and replay attacks by authenticating co-location with the ATM terminal to the bank's server. 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.

3. SYSTEM DESIGN

The general architecture of the proposed system is shown in Figure 5. The detailed system design consists of two major parts which includes both the hardware and the software.

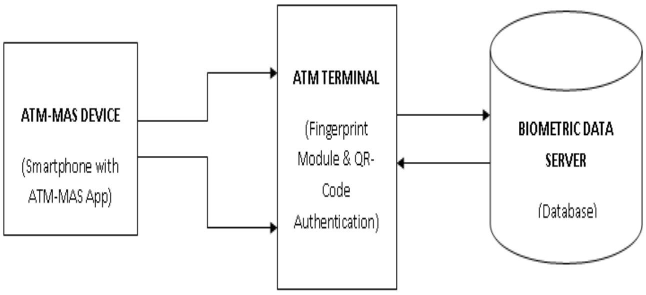
ATM-MAS DEVICE
(Smartphone with ATM-MAS App)
ATM TERMINAL
(Fingerprint Module & QR-Code Authentication)
BIOMETRIC DATA SERVER
(Database)

Fig 1: General Architecture of the System

The hardware design specifications implement embedded system design principles while the software design consists of three parts. The details of the hardware and software design are discussed as follows:

3.1 Hardware Design

The core of the system is the hardware technology implemented of the fingerprint recognition scanner. The embedded system chip used is S3C2440. The use of this chip also offers advantages of high speed communication rate across the network. Some other hardware modules that are included in the design are ATM display unit (LCD), keyboard, and alarm, all of which are connected to the main chip (S3C2440). The memory module used is SRAM. The memory module and FLASH are also embedded as part of the system architecture.

Detailed specification is as follows:

i. ***Display Module:*** The display module is implemented using OMAP5910 as a LCD controller. This display module supports 1024*1024 images of 15 gray-scale or 3375 colours.

ii. ***Memory Module:*** The memory module used is the 32-bit HY57V561620CT-6 of SRAM chip. It stores the application code, the fingerprint data and the algorithm implemented.

iii. ***FLASH Chip:*** The FLASH chip used is the 16-bit 29LV160BB- 70REC and are connected with the main chip. It complements the functionality of the memory module.

iv. ***Keyboard module:*** It is used for entering user information such as the OTP.

v. ***Biometric Scanner module:*** Atmel Company's be used as The Biometric scanner module implements the fingerprint recognition. AT77CI04B is used as the fingerprint scanner. It has a 500dpi resolution, anti-press, anti-static, anticorrosion.

vi. ***Network Controller Module:*** RTL8308B Ethernet switch controller`` is used to provide eight 10/100 Mbps RMII Ethernet ports and can connect networks of security agents like the police and remote biometric data server.

For the user to access the system, the biometric scanner module will be connected to the remote biometric data server to match the captured fingerprint image data with the stored fingerprint details on the server. If the result isn't correct, the system sends a pre-recorded voice notification message to the security agents via the network (See Figure 2).

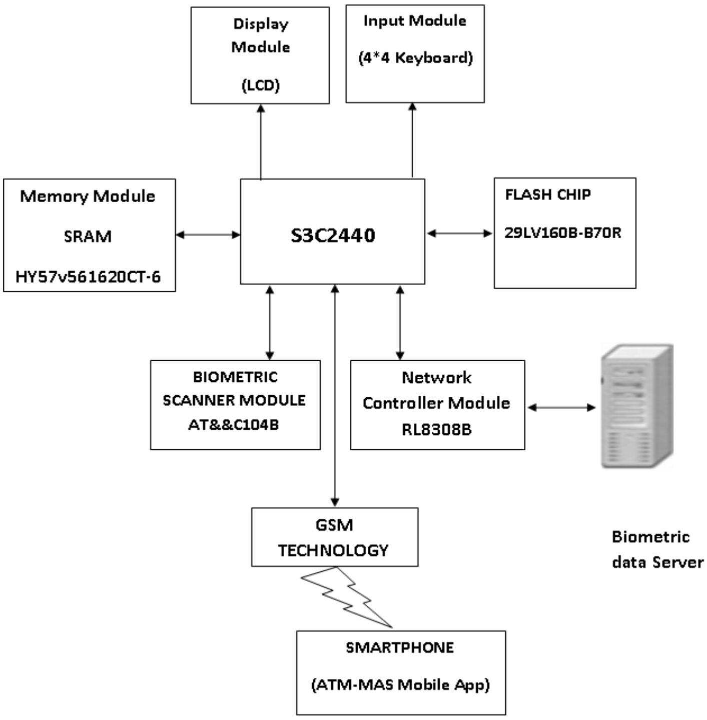
Display Module (LCD)
Input Module (4*4 Keyboard)
Memory Module SRAM HY57v561620CT-6
S3C2440
FLASH CHIP 29LV160B-B70R
BIOMETRIC SCANNER MODULE AT&&C104B
Network Controller Module RL8308B
Biometric data Server
GSM TECHNOLOGY
SMARTPHONE (ATM-MAS Mobile App)

Fig 2: ATM-MAS Hardware Design

3.2 Software Design

The system software design is composed of three distinct parts including flowchart for the main program, the initialization, and fingerprint recognition. ATM-MAS application is implemented through the following steps:

i. Firstly, ATM-MAS load the Linux kernel and the File system into the main chip.

ii. Secondly, initialization is implemented for specific tasks system checking, Mobile communication technology etc.

iii. Finally, each module is reset to enable commands. The entire process starts with the authentication of the user's fingerprint.

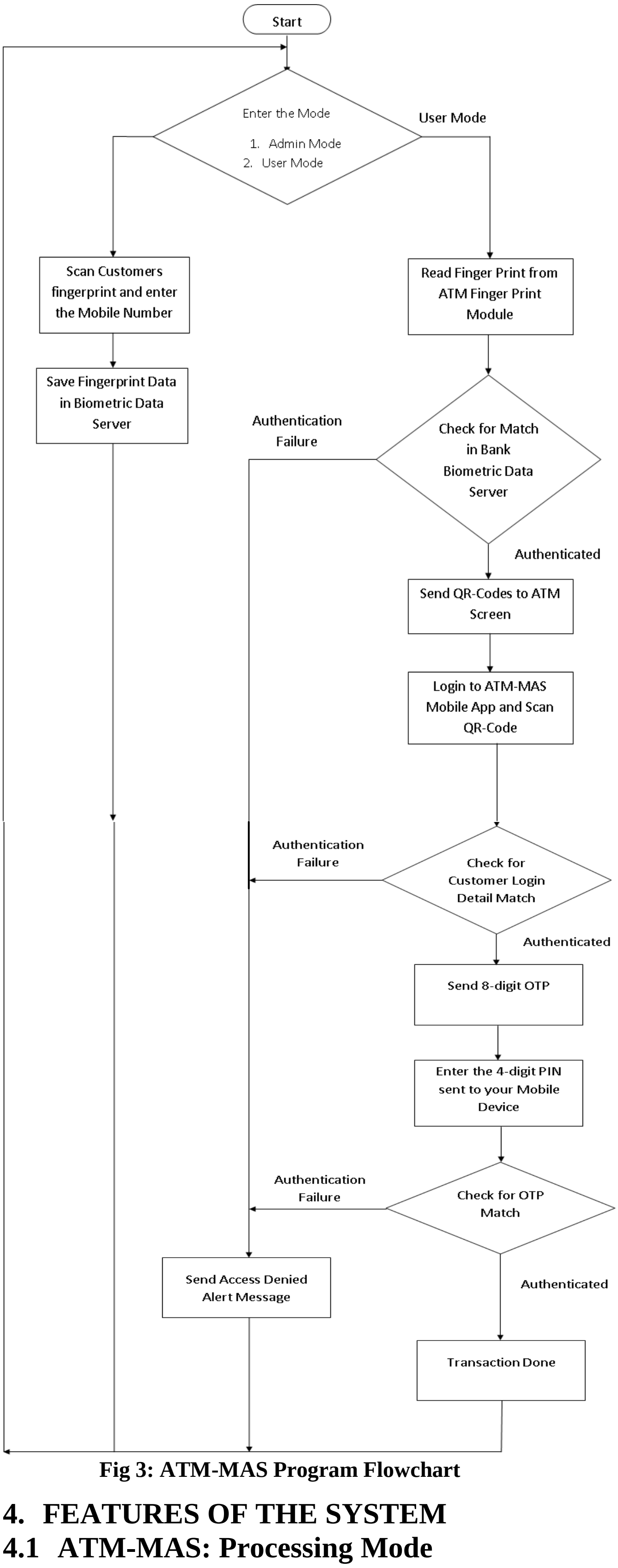
Start
Enter the Mode
1. Admin Mode
2. User Mode
User Mode
Scan Customers fingerprint and enter the Mobile Number
Save Fingerprint Data in Biometric Data Server
Read Finger Print from ATM Finger Print Module
Check for Match in Bank Biometric Data Server
Authentication Failure
Authenticated
Send QR-Codes to ATM Screen
Login to ATM-MAS Mobile App and Scan QR-Code
Check for Customer Login Detail Match
Authentication Failure
Authenticated
Send 8-digit OTP
Enter the 4-digit PIN sent to your Mobile Device
Check for OTP Match
Authentication Failure
Authenticated
Send Access Denied Alert Message
Transaction Done

Fig 3: ATM-MAS Program Flowchart

4. FEATURES OF THE SYSTEM

4.1 ATM-MAS: Processing Mode

The process starts with the system requiring the fingerprint of the user. If biometric input is correct, the system would send 8- digits PIN. 4digit out of the 8-digit pin will be displayed on the ATM display module while the remaining 4-digits will be sent to the user using the mobile number of the phone used to scan the QR-Code. The user then enters the 4-digit pin on the ATM using the input module. If authentication is not successful, the system sends a notification message to the mobile number and the bank (See Figure 3).

4.2 ATM- MAS: Technology Used

4.2.1 Fingerprint Technology

The entire process starts with the biometric fingerprint authentication. The user sweeps his/her finger over the sensing area on the ATM. The sensor used in our system for capturing the fingerprint image is an AT77C104B linear sensor. The linear sensor is an embedded system with 8-way navigation based hardware and clicking functionality. The captured image is stored temporarily SRAM module. This is then uploaded through bank network to a remote to biometric data server to be compared with registered fingerprints. S3C2440 is the chip used in controlling the output of the process. The design of algorithm based on fingerprint recognition is so vital for the whole system. Our approach is based on two steps for fingerprint image processing: The fingerprint recognition process and the fingerprint image enhancement design.

4.2.2 QR-Code using Smartphone

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. 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. 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.

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.

4.3 Advantages

i. It is a more reliable and time saving system

ii. It is more efficient and faster to use.

iii. The system is a card less system, so no ATM card is needed and users do not need to memorize PIN.

iv. It is secure against shoulder surfing attacks, relay, replay attacks, skimming, and partial observation and cloning.

4.4 Disadvantages

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.

5. CONCLUSION

A secured ATM authentication using multifactor based authentication offers an enhanced ATM security. ATM-MAS implements a cardless and an enhanced security authentication for ATM based on the stable and reliable characteristics of Fingerprint Biometric, QR-Code with smart phone technology and PIN characteristics. Access is only granted based on authenticity of the security features for owner's recognition. This study recognizes a proposed model for the enhancement of current security schemes used in ATM systems by QR code system and mobile application. The Proposed idea will confuse the Password guessing and password thieving in future from unauthorized person. Therefore, this kind of additional technique is good for preventing pin theft in future. ATM authentication using PIN-based entry is highly susceptible to shoulder-surfing or observation attacks.

6. 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, pp. 83-86, April 2012.

[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, pp. 4, February 2007.

[6] Ojekudo Nathaniel and Macarthy Osuo-Genseleke "A Comparative Study of PIN Based and Three-factor Based Authentication Technique for Improved ATM Security." International Research Journal of Engineering and Technology. Volume 5, Issue 5, pp. 3749-3754, May 2018.