A Proposed Framework For ATM Smart Card Security Using Multi-Level Authentication Scheme In Nigeria Banks

Ikudaisi .D.O, Abiodun .O, Agbolade .S, Obabueki .O, Odumabo .A.T, Adekotujo A.S
Department of Computer Science, University of Ibadan, Ibadan, Oyo State, Nigeria
Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria
Lagos State University, Ojo, Lagos State, Nigeria
E-mail: davetoba01@gmail.com,abbeyolu@yahoo.com,sjagbolade@gmail.com,obabueki2@gmail.com,

ABSTRACT

Today card authentication stands out as one of the most crucial areas in information security which has several ways of being applied. In recent time memorial authentication schemes that apply strong text-based passwords have been typically expected to offer some assurance of security for ATM smart card user. But committing to memory such strong passwords can prove to be quite a daunting task thus forcing users to resort to writing them down on pieces of papers or even storing them onto a computer file. The increase in number of customers using ATM has also increased the propensity to fraudulent practices by the ATMs fraud perpetrators. Card jamming, shoulder surfing and Stolen ATM cards constitute 65.2% of ATM frauds in Nigeria. As a means of thwarting such habits, graphical authentication has been proposed as a replacement for text based authentication. This has been spurred by the fact the humans have a natural inclination to remember images more easily than text. Based on research it was discovered that use of text based authentication only is vulnerable to different type of attack which make it not secured enough to be use as a security mechanism. This project proposed the use of both graphic authentication and text based authentication to foster more security in the use of ATM smart card.

Keywords: Authentication, Security, Information security, Vulnerable, Passwords, Smart card, Memory

iSTEAMS Cross-Border Conference Proceedings Paper Citation Format
Ikudaisi .D.O, Abiodun .O, Agbolade .S, Obabueki .O, Odumabo .A.T, Adekotujo A.S (2018): A Proposed Framework For ATM Smart Card Security Using Multi-Level Authentication Scheme In Nigeria Banks. Proceedings of the 13th iSTEAMS Multidisciplinary Conference, University of Ghana, Legon, Accra, Ghana. Pp 77-84.

1. BACKGROUND TO THE STUDY

In recent time information security has been recognized as one of the technical problem area in ATM smart card usage as shown in figure 1.0, especially when dealing with user verification and authentication. User authentication typically in form of a text-based, is a key safety process that either allows or denies access to a system or resource depending on the access code entered. A text-based key comprises of authentication secret data which is used to regulate how user have access to resources. The security of a password lies in it being kept secret from unauthorized users while those wishing to gain access use passwords for the system to be able to determine whether to grant or deny them access accordingly [1].

Today in Nigeria many unauthorized access, threats and theft takes place in ATM machines. In our study it was discovered that most Nigeria banks only adopted the use of only text-based key as a security measure in ATMs. These 4-digit PIN numbers can be hacked easily through specific duplicitous activities and it can be observed by attackers.

Figure 1.0: Typical Image of an ATM Smart Card (Google image)

The usage of smartcard is actively growing over the last decade as they are many usage of them such as telecommunications (GSM), banking services and identity card. One of the most usage smart card today is ATM card. Even it is widely used, ATM card services is not considered secure 100% in order to protect the money in bank account [5]. To protect data during their transmission over insecure channel, adequate network security measures are needed to resist potential attacks from eavesdropping, unauthorized retrieval and intended modification, etc. For every business transaction authentication is required. It is the primary requirement before the user accesses the server over insecure channel as it prevents unauthorized access [8].

2. STATEMENT OF PROBLEM

There is an urgent need for security breaches of smart cards in Nigeria, hacking into the system and creating duplicates of same cards to be rectified. Most model proposed in the past have adopted the use of PIN in smart card authentication (i.e. ATM card, MI fare cards). Despite all this proposed measures, hackers still find numerous ways to hack into the system using brute force attack, pass cloning to have access to ATM smart card information. PIN can easily be accessed or hacked which give way for attackers to access the second layer to clone or use attack software on other security layers which could be a threat to organization. As a solution to this problem, this research propose a framework where a Multi-level security approach using a text-based and graphical password will be adopted in the use of ATM smart card.

3. OBJECTIVE

The main objective of this study is to Proposed a Framework for ATM Smart Card Security using Multi-level Authentication Scheme in Nigeria.

4. METHODOLOGY

The system uses text-based password to access the system first. User are requested to enter a 4-PIN digit to access into the system, user 4-PIN is validated before having access to the system and once after the right validation, user are requested to pick at random the images the correspond to their graphical password. This is done to prevent guessing attacks, eavesdropping attack, skimming attacks and shoulder surfing attacks. For attacker to be able to succeed, the attacker must get the right text-based password and the graphical password.

4.1 The Research Design

As shown in the figure 2.0 below, the design methodology that will be used in designing the new system is the "top down "approach. The top down approach design is a modular technique which breaks the entire system into modules so that they can be tackled easily. This makes documentation and testing simpler since each sub system involves definition of input and output data.

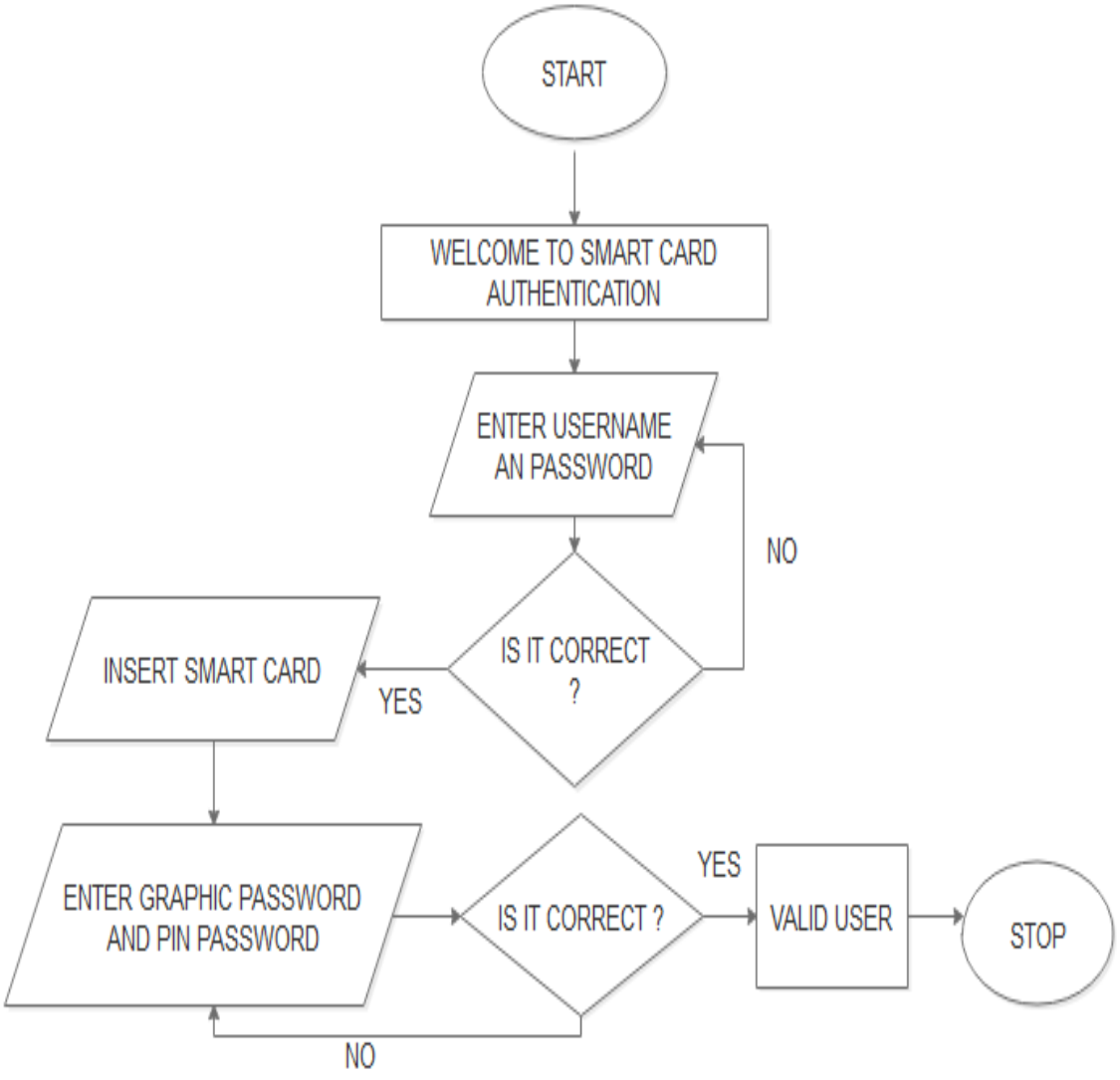

Figure 2.0: Flow Chart Diagram of the Research Methodology

5. INTEGRATION OF TEXT-BASED KEY WITH GRAPHICAL PASSWORD

5.1 Proposed Model

In order to overcome all the prior methods shortcomings, the objective of this paper is to propose a new algorithm based on the Recall-based scheme. The proposed model is to develop a Graphical Authentication System and a Text-based System of ATM Smart Card during Service Delivery. In this algorithm, users need enter their password then later tap their spots in their predetermined image in a sequence to be authenticated as shown in figure 3.0.

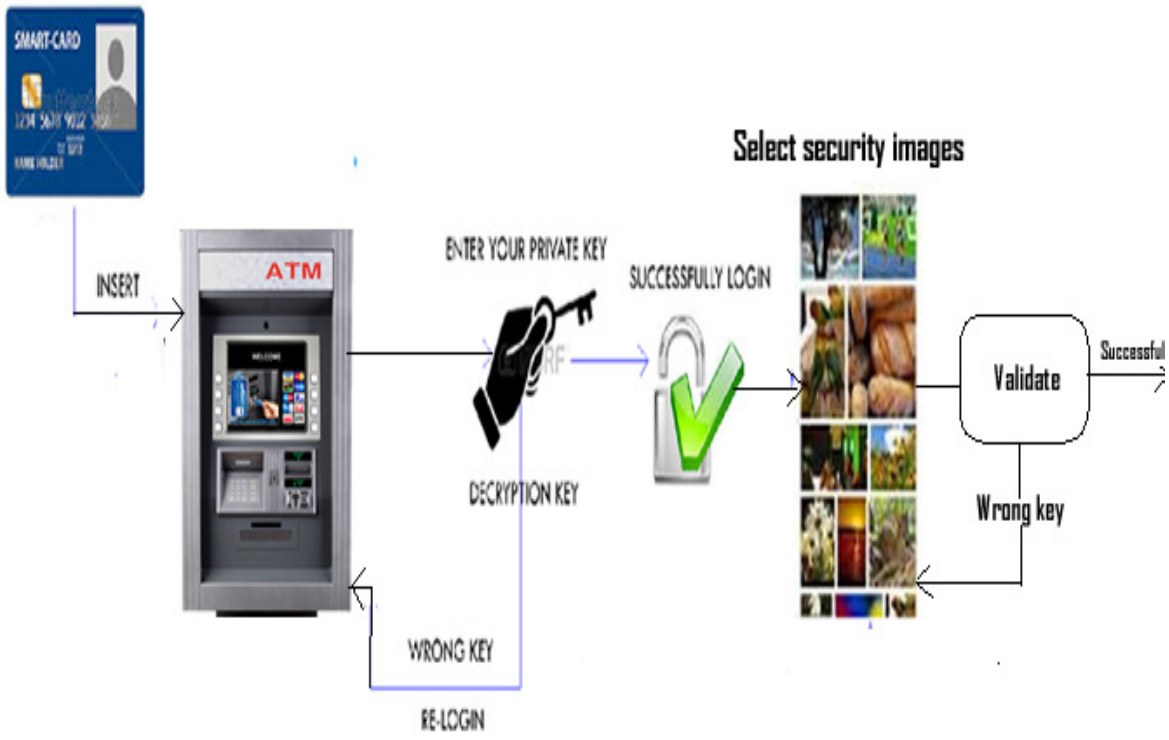

Figure 3.0: Architectural design of the proposed model

5.2 SYSTEM IMPLEMENTATION

i. **Insert Card Form:** As shown in figure 4.0, user proceed by inserting the ATM smart card into the card reader.

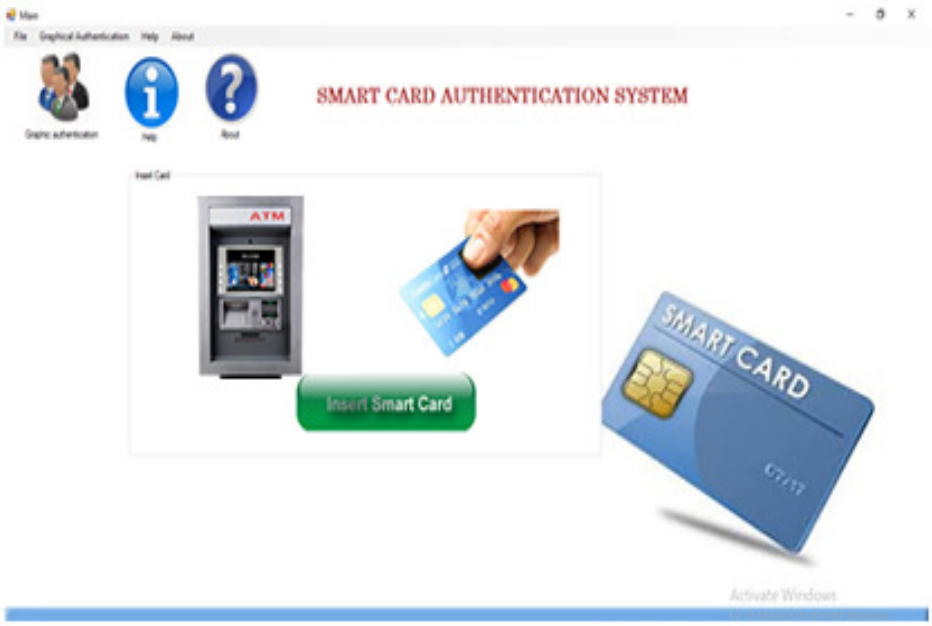

Figure 4.0: ATM smart card insertion process

ii. **Login form:** As shown in figure 5.0, users to have access into the system when valid username and password from the user has been authenticated.

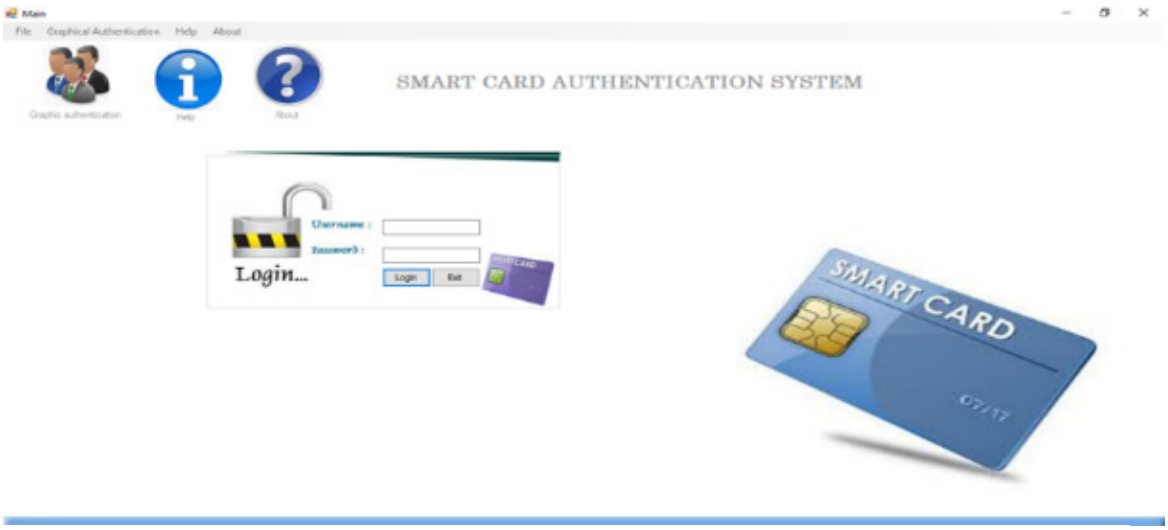

Figure 5.0: Text-based security interface for authentication into the system

iii. **Graphical password**: As shown in figure 6.0, user are to select four images for the next level authentication before having access to the ATM smart card information.

Figure 6.0: Graphical password scheme security interface for authentication into the system

iv. Authentication Validation Message: This interface display a feed back after successful login into the system as shown in figure 7.0.

Figure 7.0: Feedback message after successful authentication

6. DISCUSSION OF FINDINGS

The growth of ATMs in Nigerian banks rose from 83% in 2006 to above 289% in 2018. Almost all banks introduced the ATM in their bank premises in 2007. The increase in number of customers using ATM has also increased the propensity to fraudulent practices by the ATMs fraud perpetrators. A desktop simulation application was developed and tested by different users to allow us to gather users' feedback and execute the attack plan. Response from the user was used to evaluate attack resistance to guessing and shoulder surfing attacks, indicated a system resistance of approximately 90%.

7. CONCLUSION REMARKS

The result of this research, the test and evaluation of base on implementation and simulation demonstrated that the proposed system is more secured when compare with other previous 4-PIN text-based password. Finally, the system have suggested an improved framework which can be use in Automated Teller Machine (ATM) by enhancing the 4-PIN Text-based password security scheme with Graphical Password Authentication Scheme (GPAS). This model will be able to prevent ATM Smart Card from unforeseen attacks such as Guessing, Skimming attack and others. Furthermore, this research will help to improve people confidence in the use of ATM Smart Card.

8. CONTRIBUTIONS TO KNOWLEDGE

Based on our literature review and deep research on various ATM Smart Card with a Text-based password we found out that it is vulnerable to the following attacks; Shoulder Surfing attacks, Skimming attacks, Eavesdropping attacks and Guessing attacks. We hope to have improved on the use of ATM Smart Card in Nigeria banks by providing a framework to improve on security scheme adopted for ATM Smart Card Authentication. This framework will be able to prevent ATM Smart Card from attack such as Skimming attack, Guessing, Eavesdropping attack and others.

REFERENCES

[1]. Arash, H., Abdullah, G., Leila, G. & Samaneh, .F. (2010). A new algorithm on Graphical User Authentication
(GUA) based on multi-line grids, Scientific Research and Essays Vol. 5 (24), pp. 3865-3875
[2]. Eswar, K., Ashok, K. & Srinivasulu, .K. (2013). Smart Card based Robust Security System, International Journal of Engineering Inventions, Vol. 2, Issue 5, pp. 29-35.
[3]. Gulbarga, K. (2015). Smart Card and Its Application , International Journal of Advanced Research in Computer Science and Software Engineering , Vol. 1, No. 4, pp. 199-205.
[4]. Jahan, I., Asif, M., & Rozario, L. J. (2015). Improved RSA cryptosystem based on the study of number theory and public key cryptosystems. American Journal of Engineering Research, 4(1), 143–149.
[5]. Nor, F., Shorayha, E., Nur, Zafirah. & Hassan, .C. (2015). Security Issues in ATM Smart Card Technology, International Journal of Mathematics and Computational Science, Vol. 1, No. 4, 2015, pp. 199-205
[6]. Nivetha, S.,Edna, N., Prasanya, T., & Gohulalakshmi, .D.(2016). Secure Authentication Process in Smart Cards, IEEE International Conference on, Vol.4, No.2, pp.105-110.
[7]. Rao, G. H. (2012). Security Providing using Blowfish, RSA and SHA-512 Algorithms, 8491, 4–6.
[8]. Ravi, S., Jaidhar, C. D., & Shashikala, .T. (2012). Security Issues in Smart Card Authentication Scheme, International Journal of Computer Theory and Engineering Vol. 4, No. 2, pp. 206-211