Volume 5, Issue 10, October-2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhancing ATM Security Using 3-factor Authentication

Bakpo, F. S., Ezugwu, O.A
Department of Computer Science
University of Nigeria, Nsukka, Nigeria

Abstract: A major problem confronting Automatic Teller Machine (ATM) banking is security. This research work reports on enhancing ATM Security using 3-factor authentication. The first level is the normal ATM 4-digit secret code. At the second level the user is prompted to select a cued click points. Finally, the third level is a 6-digit one time password (OTP) will be sent to the account holder's phone number for further authentication. The 6-digit OTP is only used once and after that, it becomes invalid. Object-Oriented System Analysis and Design methodology (OOSAD) is used in analysis and design, while the system is implemented in C#.Net running on a Windows 7 operating system.

Keywords: Simulator, biometric, Dual-up, Internet service provider, personal identification numbers

I. INTRODUCTION

Security challenge is one of the major problems being faced in the world of technology today. As technology advances so security challenges increase. The issue of security in ATM banking is not new. In [2], the authors proposed the use of biometric as a way of improving security of ATM. They used VB 6.0 to design a simulator that demonstrated how the system works. They equally applied client/server approach in the implementation of the system. According to [3] Biometrics based authentication is a potential candidate to replace password-based authentication. In [4], the use of fingerprint is suggested for the enhancement of ATM security. According to [4], some of the various forms of fraud on ATM include ATM card theft, skimming, pin theft, card reader techniques, pin pad techniques, force withdrawals and lot more. The authors in [5] Worked on Combating Automated Teller Machine Frauds through Biometrics. The researchers in [6] worked on Two- Factor Authentication Using Smartphone Generated One Time Password. In this work they highlighted the importance of one time password in e-shopping and ATM machines. They proposed a system that involves generating and delivering a One Time Password to mobile phone. The authors in [7], proposed a system that combines fingerprint and OTP for security enhancement of the ATM. They noted that ATM systems today use no more than an access card and Personal Identification Number (PIN) for identity verification and that the traditional PIN alone does not provide good transaction security. This paper enhances the security of ATM transaction by introducing a 3-factor authentication platform. 3-factor authentication is a system that makes use of three stages access verification. At the first level the user is prompted to insert the card and the normal ATM 4-digit secret code. After successful verification of a user's 4-digit password, a second verification is further conducted where the user is prompted to select a cued click points. Cued click points design is a pictorial representation of codes which serves as PIN which must be supplied by the user before access is granted. It is a set of color cubes which must have been pre-selected by the users of the system in a particular order during registration. The final and the most reliable verification technique is that the user will be requested by the machine to enter the password sent to him/her via user's phone SMS. The password sent to the account holder is valid for just that transaction session. Any other transaction will equally require another password. This kind of password is called one-time password (OTP). A one-time password is a password that is valid for only one login session or transaction [1]. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The rest of the paper is structured as follows in section 2 ATM system is discussed, in section 3, we looked at ATM security using 3-factor authentication, system analysis and design, in section 4, we did performance evaluation and in section 5 we concluded the work.

II. ATM SYSTEM

An ATM is simply a data terminal with two input and four output devices. Like any other data terminal, the ATM connects to, and communicates through a host processor. The host processor is analogous to an Internet Service Provider (ISP) in that it is the gateway through which all the various ATM networks become available to the cardholder (the person wanting the cash). Most host processors can support either leased-line or dial-up machines. Leased-line machines connect directly to the host processor through a four-wire, point-to-point, and dedicated telephone line. Dial-up ATMs connect to the host processor through a normal phone line using a modem and a toll-free number, or through an Internet service provider using a local access number dialled by modem [8]. ATM architecture is illustrated in figure 1. The ATM architecture consists of three components namely ATM user interface, ATM, and Bank (host processor). The bank is made up of cashier, Account and validation info. The bank validates pin and account. The bank through the cashier also performs such function like openAcct, initialDeposit, authoriseCard, deauthorise and closeAcct.

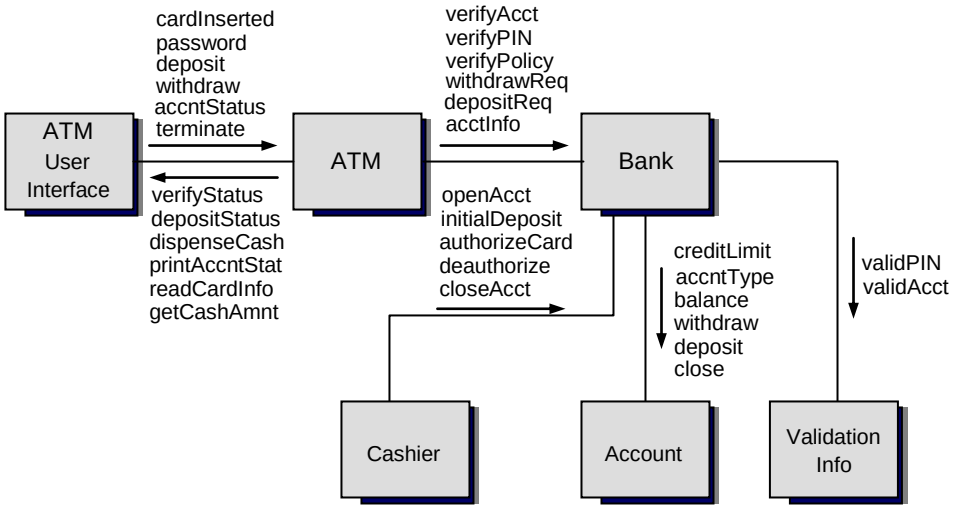

Fig. 1. The ATM Architecture

III. ATM SECURITY USING 3-FACTOR AUTHENTICATION

3-factor authentication is a system that makes use of three stages access verification.

First level: In the first level, the user will be prompted by the machine to enter 4-digit security pin, which must have been registered uniquely for each user of the system.

Second level: Cued Click Points is the second level of user authentication which is specifically designed to graphically authenticate the user using set of colored cubes which must have been pre-selected by each user in a particular order during registration. Cued click points design is a pictorial representation of codes which serves as PIN (Personal identification numbers).

Third level: SMS verification method is the third level of user authentication which uses phone verification as a mean of identifying the users of the system. After a successful authentication through the first and the second levels, the system generates a random 6-digit code which automatically synchronized with the user account. The generated code will be forwarded to the user's registered mobile phone number as a text message which the user is prompted to enter to finally grant him/her access into the system. The password sent to the account holder is valid for just that transaction session. Any other transaction will equally require another password. This kind of password is called one-time password (OTP). 3-factor authentication architecture is shown in fig. 2.

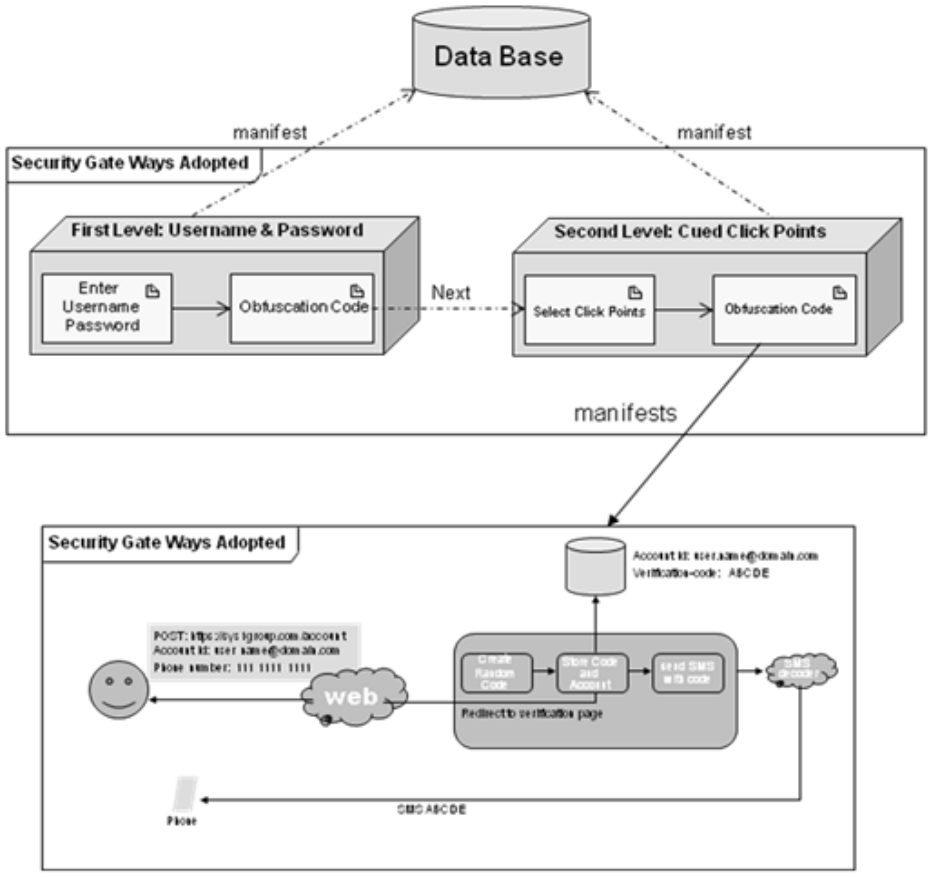

Fig.2. Enhanced 3- factor Authentication System Architecture

A. System Analysis and Design

The system can be described using use case diagram as shown below.

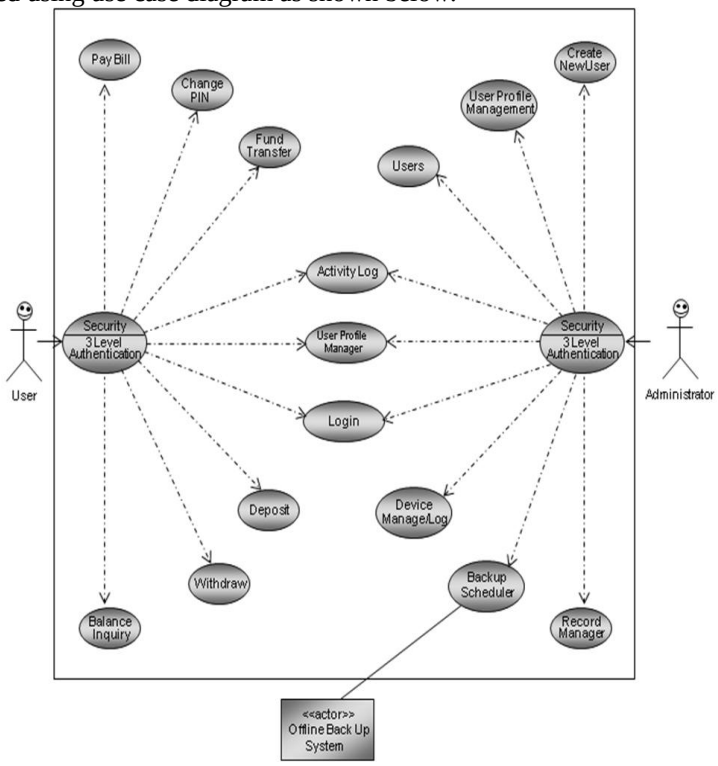

Fig.3. Use Case Diagram for the 3- factor Authentication System

B. System Implementations

The ATM software was implemented with Visual Studio 2010 Integrated Development Environment (IDE) using C# compiler and MS SQL server.

IV. CONCLUSION

ATMs have brought so much relief to the financial world. Various problems were solved with the advent of these machines ranging from keeping the banking hall free of traffic to implementing cashless system. Banks must meet certain standards in order to ensure a safe and secure banking environment for their customers. Security measures at banks can play a critical, contributory role in preventing attacks on customers. This work addressed the security challenges inherent in the ATM banking system. The 3-factor authentication for ATM is a vital achievement of this project work. With the 3-factor authentication put in place, an account holder will no longer fear when he/she misplaces his/her ATM card because no other person other than the legitimate card owner can made transaction with the card.

REFERENCES

[1] One-time password (wikipedia) http://en.wikipedia.org/wiki/One-time_password, retrieved on 26th september 2014.

[2] Ibidapo, O. Akinyemi, Zaccheous O. Omogbadegun, and Olufemi M. Oyelami, Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria EBanking System. International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 10 No: 06 2010

[3] Das, S., Debbarma, J , ,Designing a biometric strategy (fingerprint) measure for enhancing ATM security in India e-Banking system. International Journal of Informationand Communication Technology Research vol 1 no 5 p 197-203.2011

[4] SelinaOko, Jane Oruh,Enhanced ATM Security System using Biometrics. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3, September 2012 ISSN (Online): 1694-0814

[5] OludeleAwodele, AdeniyiAkanni, Combating Automated Teller Machine Frauds through Biometrics. International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012).2012

[6] Sagar Acharya, Apoorva Polawar, P.Y.Pawar, Two Factor Authentication Using Smartphone Generated One Time Password. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 2 (May. - Jun. 2013), PP 85- 90 www.iosrjournals.org.

[7] V.Padmapriya, S.Prakasam,, Enhancing ATM Security using Fingerprint and GSM Technology. International Journal of Computer Applications (0975 – 8887) Volume 80 – No 16, October 2013.

[8] Available at http://www.pg.gda.pl/~mickowal/IE/bankomaty_eng.pdf accessed on 9/12/14

