WWJMRD 2018; 4(1): 302-305
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Isiaka, Olatunji S.
Computer Science Department
Institute of Information and Communication Technology
Kwara State Polytechnic, Ilorin, Nigeria

Saka, Tajudeen O.
Computer Science Department
Institute of Information and Communication Technology
Kwara State Polytechnic, Ilorin, Nigeria

Bolaji-Adetoro, David F.
Computer Science Department
Institute of Information and Communication Technology
Kwara State Polytechnic, Ilorin, Nigeria

Correspondence:
Isiaka, Olatunji S.
Computer Science Department
Institute of Information and Communication Technology
Kwara State Polytechnic, Ilorin, Nigeria

Secured ATM Operation with Three-Level Authentication System

Isiaka, Olatunji S., Saka, Tajudeen O., Bolaji-Adetoro, David F.

Abstract
The security of automated teller machine (ATM) transactions can be further strengthened using the three-level authentication system where the user is authenticated with what he has (ATM card), what he knows (personal identification number (PIN)) and what he is (fingerprint biometrics). The aim of the paper is to introduce a system where the ATM authenticates and verifies the true identity of the user. The use of fingerprint biometric in conjunction with existing authentication methods will eradicate fraudulent act and improve effective ATM transactions. The fingerprint concept is chosen because of its uniqueness with high level of accuracy, reliable and affordable. The paper, therefore, describes the simulation of an ATM with the capability of the combination of card, PIN and fingerprint biometrics based authentication with a view to provide a more reliable online banking transaction on ATM.

Keywords: Fingerprint Biometrics, PIN, ATM, Three-Level Authentication, Security, Online Banking

Introduction
The security level in the Automated Teller Machine (ATM) would not be hundred percent guaranteed provided there is no special way to identify who is banking at any point in time. One of the most effective ways of identifying and distinguishing between persons through traits is the use of biometrics. Biometrics is a rapidly advancing field that is concerned with identifying a person based on his or her physiological or behavioral characteristics (Rasu et al, 2012). Fingerprint technology in particular, can provide a much more accurate and reliable user authentication method. An important issue when considering biometric technology is to address the distinct classifications formally defined through application and implementation. As the ATM technology is advancing, fraudsters are devising different skills to beat the security of ATM operations.

Various forms of fraud are perpetuated, ranging from: ATM card theft, skimming, pin theft, card reader techniques, pin pad techniques, force withdrawals and lot more. Managing the risk associated with ATM fraud as well as diminishing its impact is an important issue that faces financial institutions as fraud techniques have become more advanced with increased occurrences. Considering the numerous security challenges encountered by ATM users and observing the existing security in the ATM system, there is the need to enhance the ATM security system to overcome these challenges. This study focuses on how to enhance security of transacting with ATM system using fingerprint technologies (Roli et al, 2011).

Current security implementation does not proffer the adequate security necessary to secure electronic transactions, customers' information and funds (Falaye, 2013). It is therefore suggested that future work be done on the technical implementation of a more secured authentication method such as fingerprint technology and facial recognition. The major concerned of Madu and Madu (2002) is about bank users' security and privacy while using the service of the ATM. Obiano (2009) blamed the menace of ATM frauds on indiscriminate issue of ATM card without regard to the customer's literacy level. According to him one of the frequent causes of fraud is when users are careless with their cards and PIN numbers as well as their response to unsolicited e-mail and text messages to provide their card details. Adeloye (2008) identified security as well as power outage as major challenges facing the

ATM users in Nigeria. In his view, Diebold (2002) is of opinion that the major form of ATM fraud is PIN theft which is carried out by various means; skimming, shoulder surfing, camera, key pad recorder etc. Cynthia (2000) views that the 24 hours access to the ATM machine is a double edge sword, it has both advantages and disadvantages.

The use of fingerprints as a biometric is both the oldest mode of computer-aided, personal identification and the most prevalent in use today (Gorman, 1998). In the world today, fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examination, operation of bank accounts among others. They are also used for controlling access to highly secured places like offices, equipment rooms, control centers and so on (Iwasokun et al, 2012). Biometric authentication technologies interface that capture fingerprint for registration and a financial transaction is shown in figure 1.

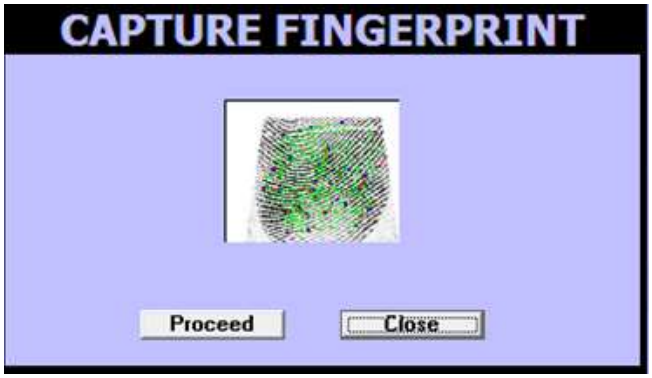

Fig.1: Fingerprint Captured Registration Interface

The fingerprint captured may solve the problem of ATM card theft and guessed PIN since a person's fingerprint is undeniably connected to its owner, it is nontransferable and it is unique for every individual.

System Design and Implementation

In this research we proposed a secured banking operation with the use of fingerprint biometric technologies. The system not only discourages the use of only the traditional 4-digit PIN but also includes the distinct features of biometric technologies (fingerprint authentication) for ATM operations. Fingerprint of customers will be captured at the point of registration and prompted for supply when any banking transaction is to be carried out at the ATM point. This eradicates all forms of security threats and financial misconduct going on in our day to day banking activities. Use case and state chart diagrams are used to describe the design and implementation of this system.

Use Case Diagram

A use case model is instrumental in project development, planning, and documentation of system requirements. It is an interaction between users and a system which captures the goal of the users and the responsibility of the system to its users. It describes the uses of the system and shows the courses of events that can be performed as well as defining what happens in a system (Shan et al, 2011). In the design of the banking ATM application, the actor of the bank system is the bank customer. Figure 2 shows the use case diagram for our system design, where customers can perform transaction by inserting their ATM card and requesting for approval to perform transaction by entering PIN digits and enroll Fingerprint. After the approval, the transaction is then carried out accordingly. At the completion of the transaction, the customer exit application and remove his/her card. Here the use-cases is triggered by the primary actors; customer and Administrator, and the secondary actor; ATM System.

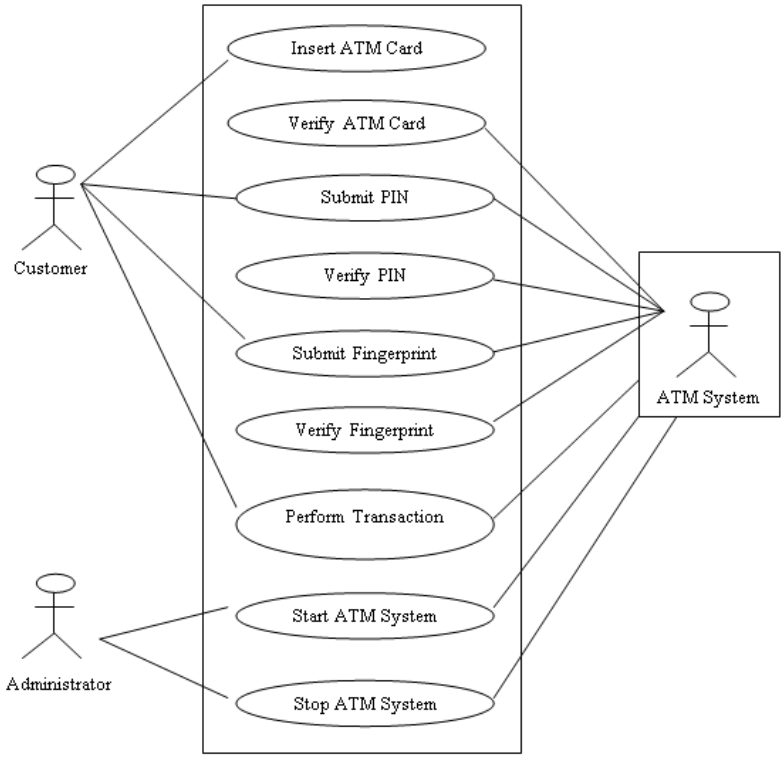

Fig.2: Use Case Diagram for ATM Simulator

State Chart Diagram

This shows the state an object or a system can be at any point in time. It also shows how you can transit from one state to another with the conditions and the arrows that trigger the transition. Figure 3 shows the state machine for one ATM session.

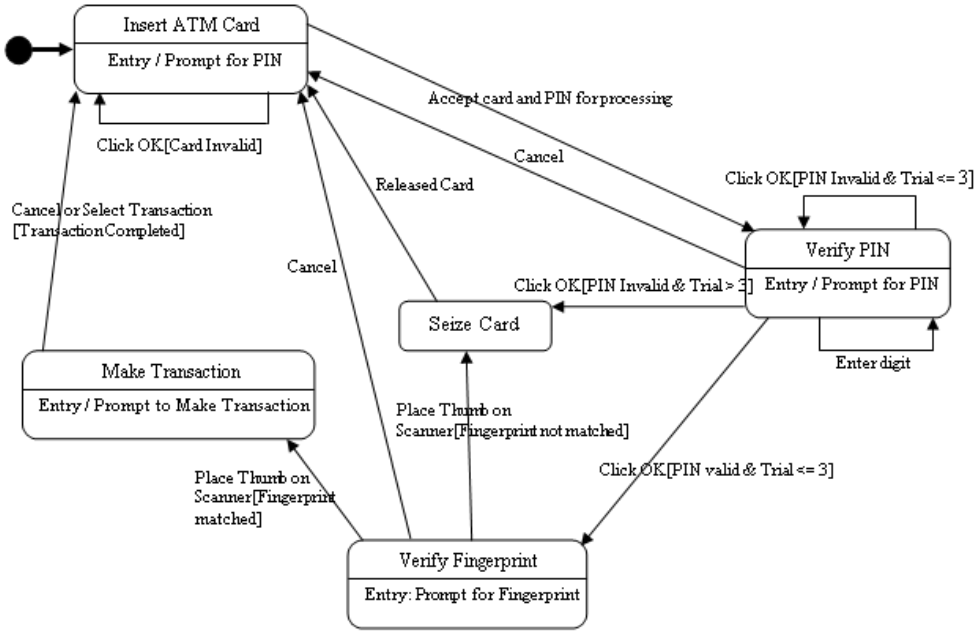

Fig.3: The State Chart Diagram for ATM Session

Discussions

The biometrics authentication of the system was made possible with the use of Griaule Biometrics Software Development Kit (SDK). The design was accomplished with the use of Microsoft Visual C#.net 2012 for the front end while Microsoft Access was used as the back end of the database.

A detail description of the system is expressed in both activity and sequence diagrams. The activity diagram in Figure 4 highlights the operations of ATM through card insertion, PIN validation, Fingerprint validation and transactions.

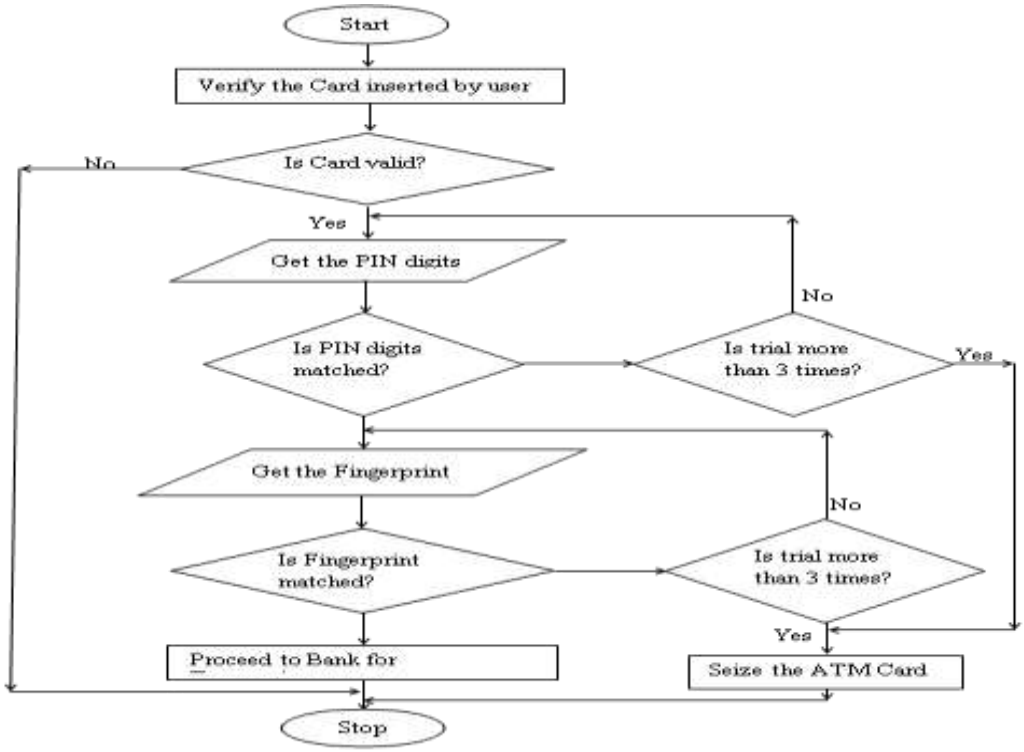

Fig.4: Activity Diagram for Use Case Model

The sequence diagram for use case as shown in Figure 5 is on the following identified classes: Bank user, ATM machine and Account. Sequence diagram tells us the sequences in which the processes happened and shows the timeline of the processes. The sequence diagram below shows a high level sequence diagram for the ATM Simulator.

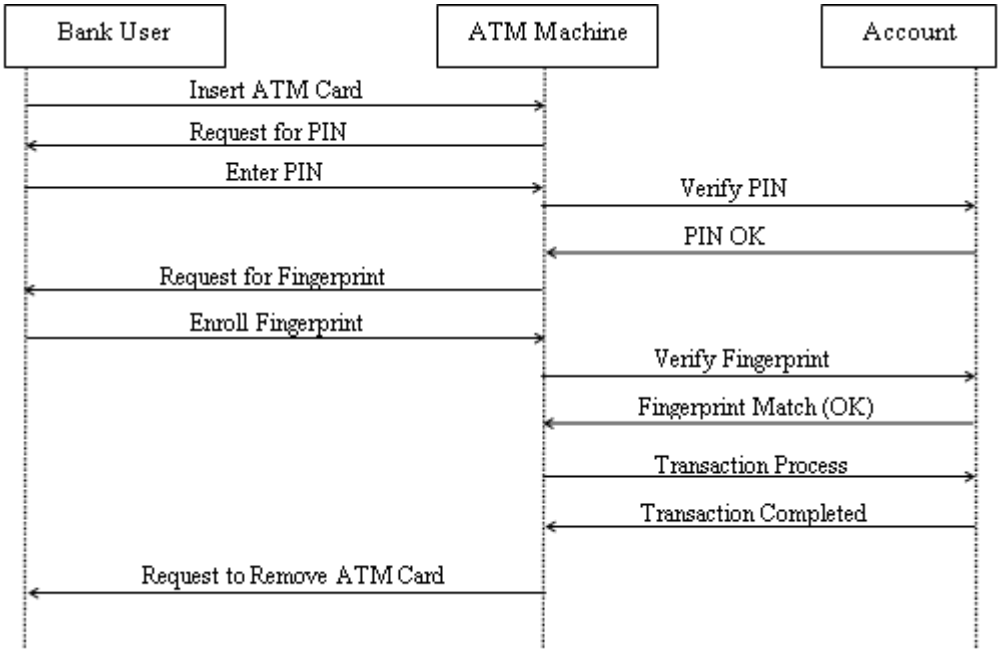

Fig.5: Sequential Diagram for Use Case Model

Conclusion

An enhanced security system if implemented with the use of fingerprint authentication in today's banking services will go a long way to eradicate all forms of financial misconduct trailing our banking sector, since no two persons have the same fingerprint and will help to maintain accurate and a secured banking transaction.

Traditional ATM systems authenticate generally by using the ATM card and the PIN method has some defects. Using ATM card and PIN only cannot verify the user's identity exactly. In recent years, the research on the fingerprint recognition is embedded into the system in order to offer new verification means for us. The original PIN authentication method combined with the biometric identification technology verify the users' identity better and achieve the purpose that use of ATM machines improve the safety effectively.

References

1. Adeloye, L.A (2008). "E-banking as new frontiers for banks". Sunday punch, September 14, P.25.
2. Cynthia B. (2000). "The measurement of white-collar crime using Uniform Crime Reporting". (UCR) Data, Department of Justice, Federal Bureau of Investigation, New York.
3. Falaye, A.A (2013). "A Survey of ATM Security Implementation within the Nigerian Banking Environment".Journal of Internet Banking and Commerce.
4. Gorman L. O. (1998). "Overview of fingerprint verification technologies". Elsevier Information Security Technical Report, vol. 3, no. 1.
5. Iwasokun G. B., Akinyokun O. C., Alese B. K., and Olabode O. (2012). "Fingerprint Image enhancement: Segmentation to thinning". International Journal of Advanced Computer Science and Applications, vol. 3, no. 1, pp. 15-24, 2012.
6. Madu, C.N., & Madu, A.A. (2002). "Dimensions of e-quality". International Journal of Quality & Reliability Management, 19(3), 246-58.
7. Obiano, W. (2009). "How to fight ATM fraud Online". Nigeria Daily News, June 21, P. 18
8. Rasu R., Krishna P. K. and Chandraman M. (2012). "Security for ATM Terminal Using Various Recognition Systems". International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 4, ISSN: 2277-3754 ISO 9001:2008 Certified
9. Roli B., Priti S. and Punam B. (2011). "Minutiae Extraction from Fingerprint Images". International Journal of Computer Science Issues, vol.8, Issue 5, No3. ISSN(online):1694-0814 www.IJCSI.org
10. Shan J. X., Jucheng Y., Dong S. P., Sook Y. and Jinwook S. (2011). "Fingerprint Quality Analysis and Estimation Approach for Fingerprint Matching". State of the art in Biometrics, 2011, ISBN: 978-953-307-489-4