ENHANCED ATM SECURITY SYSTEM USING BIOMETRICS

Prof. Selina Oko[1] and Jane Oruh[2]

[1]Department of Computer Science,
Ebonyi State University Abakaliki, Nigeria

[2]Department of Computer Science,
Michael Okpara University of Agriculture, Umudike, Nigeria

Abstract

Because biometrics-based authentication offers several advantages over other authentication methods, there has been a significant surge in the use of biometrics for user authentication in recent years. In this paper the existing security of the ATM (Automated Teller Machine) system has been improved by integrating the fingerprint of the user into the bank's database as to further authenticate it. This was achieved by modelling and building an ATM simulator that will mimic a typical ATM system. The end result is an enhanced biometric authenticated ATM system that ensures greater security and increased customer's confidence in the banking sector.

Keyword: Enhancement, Biometric Authentication, ATM system, Security

1. Introduction

Biometrics-based authentication offers several advantages over other authentication. Fingerprint technology in particular, can provide a much more accurate and reliable user authentication method. Biometrics is a rapidly advancing field that is concerned with identifying a person based on his or physiological or behavioural characteristics. As the Automated Teller Machines (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 Automated Teller Machines (ATM) and users and given that the existing security in the ATM system has not been able to address these challenges, there is the need to enhance the ATM security system to overcome these challenges. This study focuses on how to enhance security of transactions in ATM system using fingerprint. The aim of this study therefore is to develop ATM simulator based fingerprint verification operations in order to reduce frauds associated with the use of ATM.

2. Literature review

Madu and Madu (2002) pointed out that the concern of customers about security and privacy, while using this service, is a major cause of their dissatisfaction. Ihejiahi (2009) expressed concern about the lack of cooperation among banks in the fight to stem the incidence of ATM frauds now plaguing the industry. He expressed that the silence among banks on ATM frauds makes it difficult for banks to share vital information that will help curb the menace. 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 customers 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. Omankhanleu (2009) opined that the current upsurge and nefarious activities of Automated Teller Machine (ATM) fraudster is threatening electronic payment system in the nation's banking sector with users threatening massive dumping of the cards if the unwholesome act is not checked. Adeloye (2008) identified security as well as power outage as major challenges facing the ATM users in Nigeria. Brunner et al. (2004) in their study concluded that the location of ATM is a high determinant to fraud or crime carried out at ATM point. From this research over 75% of the respondents affirm that the location of ATM in secluded place contribute to the fraud perpetuated at ATM point. ATM within the banking premises is more secure than ATMs outside the bank premises. Also, it is obvious that the location of ATM in attractive place does not make it prone for fraud. Diebold (2002) in his view states 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. This study elucidates that the common type of fraud perpetuated is

PIN theft which is mostly as a result of congestion at ATM points. Other forms of fraud that were enumerated by respondents were; force withdrawal, card theft, and skimming and congestion method fraud at ATM. Cynthia (2000) states that the 24 hours access to the ATM machine is a double edge sword, it has both advantage and disadvantage. Roli Bansal et al (2011) pointed out that amongst all the fingerprint features, minutia point features with corresponding orientation maps are unique enough to discriminate amongst fingerprints robustly; the minutiae feature representation reduces the complex fingerprint recognition problem to a point pattern matching problem.

3. Analysis and design methodology

3.1Object Oriented Analysis and Design

In this paper, we are adopting Object Oriented Analysis and Design (OOAD) which enable us to make use of Java which is an Object Oriented Language. Object-oriented analysis and design (OOAD) is a software engineering approach that represents a system as a group of interacting objects. Each object represents some entity of interest in the system being modeled, and is characterised by its class, its state (data elements), and its behaviour. Various models can be created to show the static structure, dynamic behaviour, and run-time deployment of these collaborating objects. There are a number of different notations for representing these models, such as the Unified Modeling Language (UML).Object-oriented analysis (OOA) applies object-modeling techniques to analyze the functional requirements for a system. Object-oriented design (OOD) elaborates the analysis models to produce implementation specifications. OOA focuses on *what* the system does, OOD on *how* the system does it.UML

rams, state chart

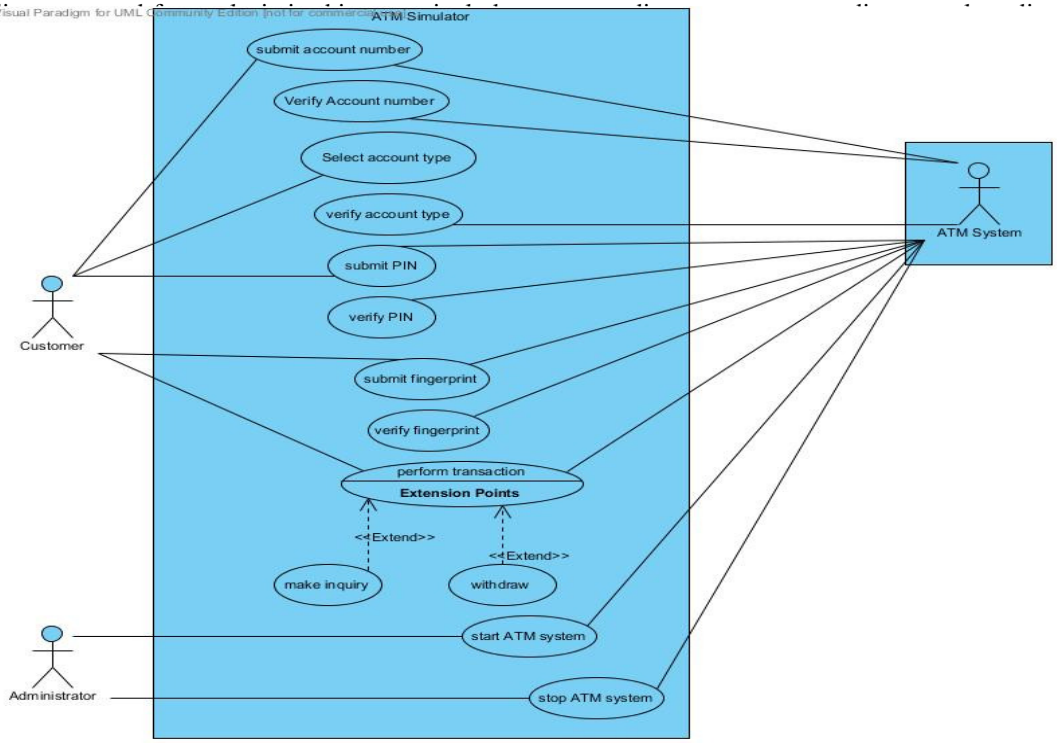


Fig 3.1.1a Use Case Diagram for ATM Simulator.

The diagram above shows the Use Case Diagram for the ATM Simulator. Here the use-cases is triggered by the primary actors; customer and Administrator, and the secondary actor; ATM System.

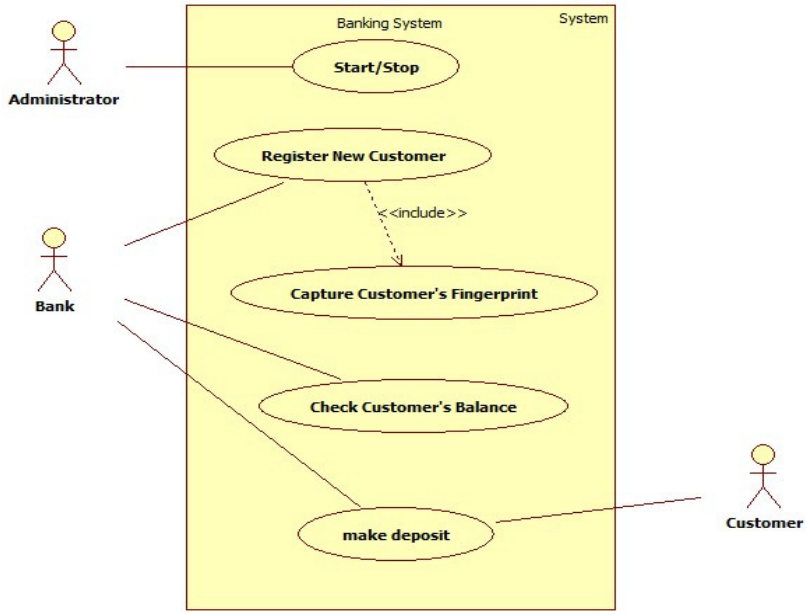


Fig 3.1.1b

The diagram above shows the Use-case diagram for the Banking Application System. The primary actors are Administrator, Bank Staff and Customer.

3.1.2 SEQUENCE DIAGRAM: It tells us the sequences in which the processes happened and in time. It shows the timeline of the processes. The sequence diagram below shows a high level sequence diagram for the ATM Simulator.

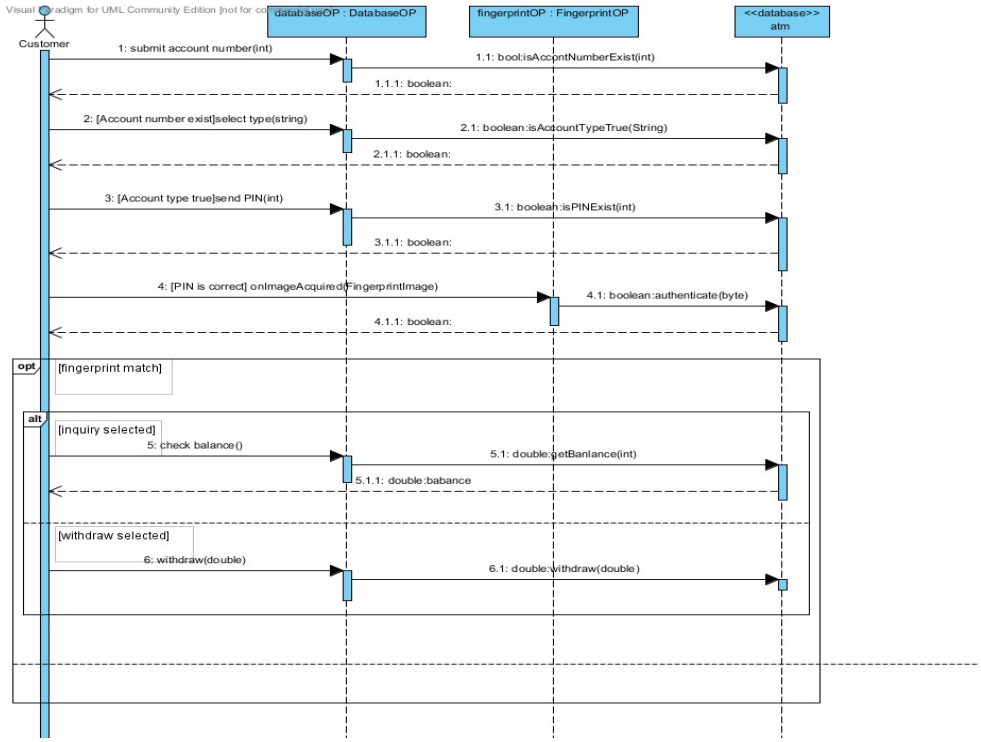


Fig.3.1.2 Sequence Diagram

3.1.3 The class diagram: The diagram below shows the class diagram for the ATM Simulator. Classes, attributes and methods of each class are also shown in the class diagram. This is a detailed class diagram for the ATM simulator.

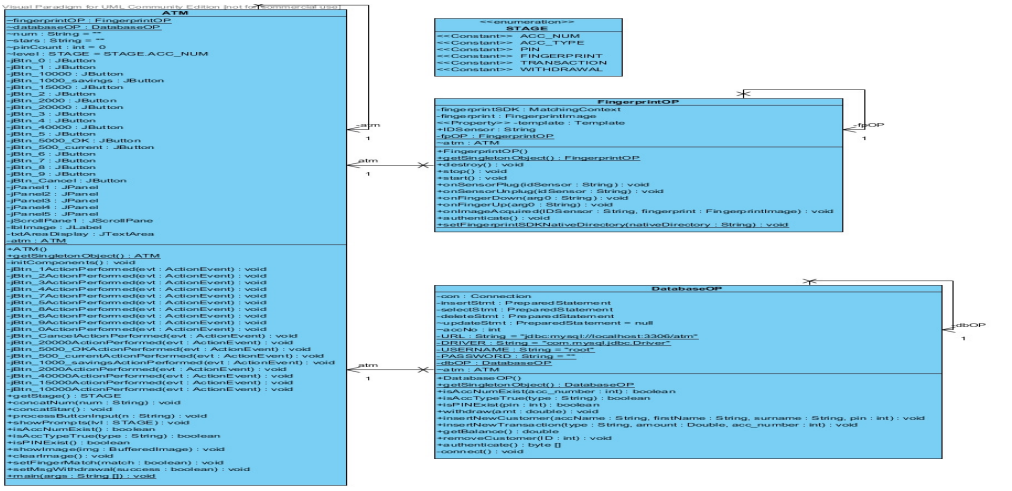


Fig. 3.1.3a Class Diagram for ATM Simulator

From the diagram above we have the classes as the ATM, STAGE, FingerprintOp, DatabaseOp which depicts the object of the class while inside these classes we have attributes with their type; fingerprint:Fingerprintimage.The arrows joining them are showing relationship among the classes.

The diagram below shows the class diagram for the Banking Application software with all the classes and the methods and attributes of each class shown.

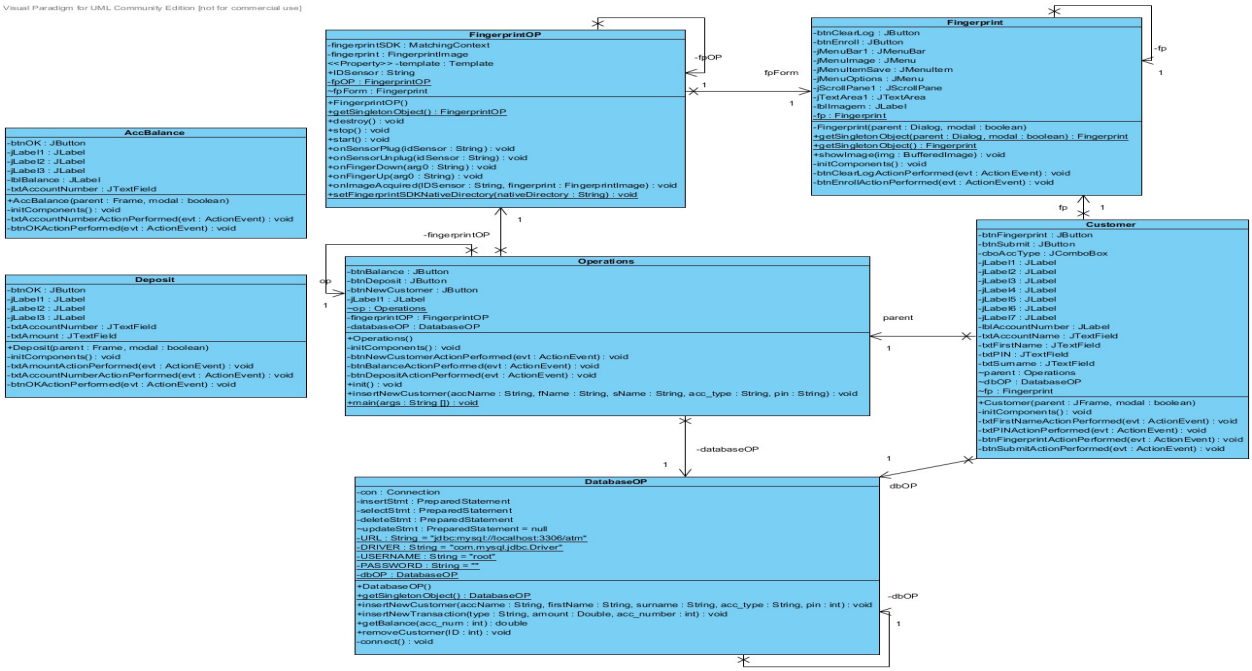
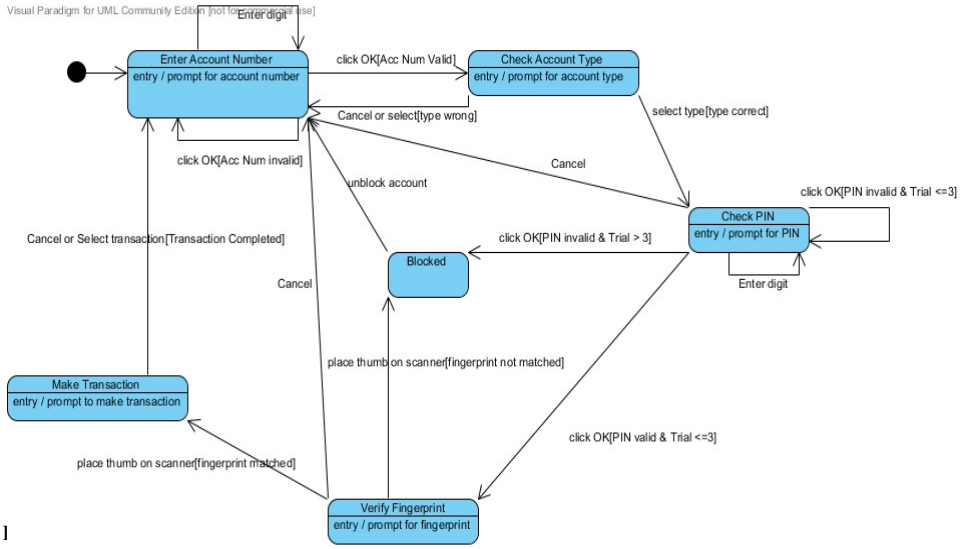


Fig. 3.1.3b Class Diagram for the Banking Application

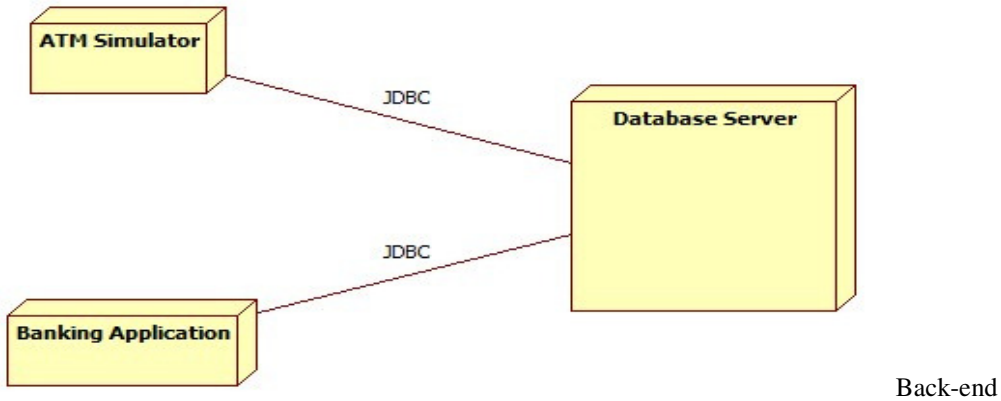
3.1.4 The state chart diagram: It shows the state an object or a system can be at any point in time. It also shows how U can transit from one state to another with the conditions and the arrows that trigger the transition. The diagram below shows the state machine for one ATM session.



4.0 Implementation and testing

4.1 Implementation

4.1.1 Deployment model: Below is a deployment view of the ATM where the ATM simulator and the banking application is connected to the database server across the Java Database Connectivity (JDBC).Hence it can run across a network.



Back-end

Front-end

Fig 4.1.1 Deployment view

4.2 Application programming interfaces (API's) used

- JAVA DEVELOPMENT KIT :This is the core Java Library

- FINGERPRINT SDK JAVA 2009:It is a third party fingerprint Java API from Griaule Biometrics
- JAVA DATABASE CONNECTIVITY (JDBC): The JDBC API provides programmatic access to relational data from the Java programming language.

5.0 Summary, Conclusion and Recommendation

5.1 Summary

From the test carried out we have been able to prove that the biometric ATM is practicable and could be implemented in a real production environment.Biometric tokens are the safest means of preventing ATM frauds. The most widely used biometric tokens are finger prints, irises, faces and palms. The fraudster may match everything but they can never match the biometric peculiarities.

5.2 Conclusion

The main reason for introducing biometric systems is to increase overall security. Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, biometrics can replace or supplement the existing technology. In others, it is the only viable approach. Decision-makers need to understand the level of security guaranteed through the use of biometric systems and the difference that can exist between the perception and the reality of the sense of security provided. The biometric system is only one part of an overall identification or authentication process, and the other parts of that process will play an equal role in determining its effectiveness.

5.3 Recommendation

We recommend the following for future research:

(i) Using a 3-D API for a Graphical User Interface (GUI). Example is openGL in place of Java Swing API.

(ii) The JDBC architecture can be extended to three-tier using application server like APPLET server, JSPservlet on APACHE thumbcard versus database.

(iii) There is need to Develop a fingerprint matching algorithm.

References

[1] Adeloye LA 2008. E-banking as new frontiers for banks. *Sunday Punch*, September 14, P. 25.

[2] 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

[3] Brunner, A., Decressin, J. and Kudela, B. (2004): Germany's Three-Pillar Banking System – Cross Country Perspectives in Europe, Occasional Paper, International Monetary Fund, Washington DC.

[4] Cynthia B. (2000). The measurement of white-collar crime using Uniform Crime Reporting (UCR) Data. S department of Justice, Federal Bureau of Investigation, New York.

[5] Diebold I. (2002). ATM fraud and security: White Paper, New York.

[6] Ihejiahi R 2009. How to fight ATM fraud online. *Nigeria Daily News,* June 21, P. 18.

[7] Madu, C.N., & Madu, A.A. (2002). Dimensions of e-quality. *International Journal of Quality & Reliability Management, 19(3),* 246-58.

[8] Obiano W 2009. How to fight ATM fraud. online Nigeria *Daily News,* June 21, P. 18

[9] Omankhanlen Odidison (2009).ATM fraud rises: Nigerians groan in Nigeria. *Daily News,*Sunday, June 21, pp. 8-10.