Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X
Vol.2 Issue 2 (2016) 48-51. Submitted 28/03/2016. Published 05/04/2016

ENHANCED ATM SECURITY AND THEFT IDENTIFICATION USING BIO METRICS

[1]R.Purushothaman, [2]M.Rajasekar, [3]S.Iyyappan, [4]M.Sudhakaran,
[1,2]Dept of EEE, GTEC, Vellore, India
[3]Asst. Prof, Dept of EEE, GTEC, Vellore, India
[4]Associate Prof, Dept of EEE, GTEC, Vellore, India

Abstract:

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 project the existing security of the ATM (Automated Teller Machine) system has been improved by integrating the palm print of the user into the bank's database as to further authenticate it. This was achieved by modeling 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.

Index Terms—palm-print recognition, modularization, biometric authentication, security.

1. INTRODUCTION

This project proposes a system which takes the user biometric palm print compares it with the image stored in database on a server and provides more secure financial transaction. Nowadays various electronic devices use biometrics for fast identification and authentication. Computer systems in offices, banks uses different pins for transaction for secured reasons. General methods of identification using ID cards and pin is not reliable. An embedded palm print biometric authentication scheme for automated teller machine (ATM) banking systems is proposed in this project. In this scheme, a palm print biometric technique is fused with the ATM for person authentication to improve the security level. Nowadays A lot of criminals activities occur in banking services. Criminals interfere with the ATM terminal and steal customers card details by illegal means .Once user bank card is lost and the password is stolen, the user account is vulnerable to attack .Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a pass word or PIN. This PIN has some defects. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct secret observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PINs and passwords - birthdays, phone numbers and social security numbers. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card. Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is automated methods of recognizing a person based on a physiological or behavioral characteristic.

2. LITERATURE SURVEY

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

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.

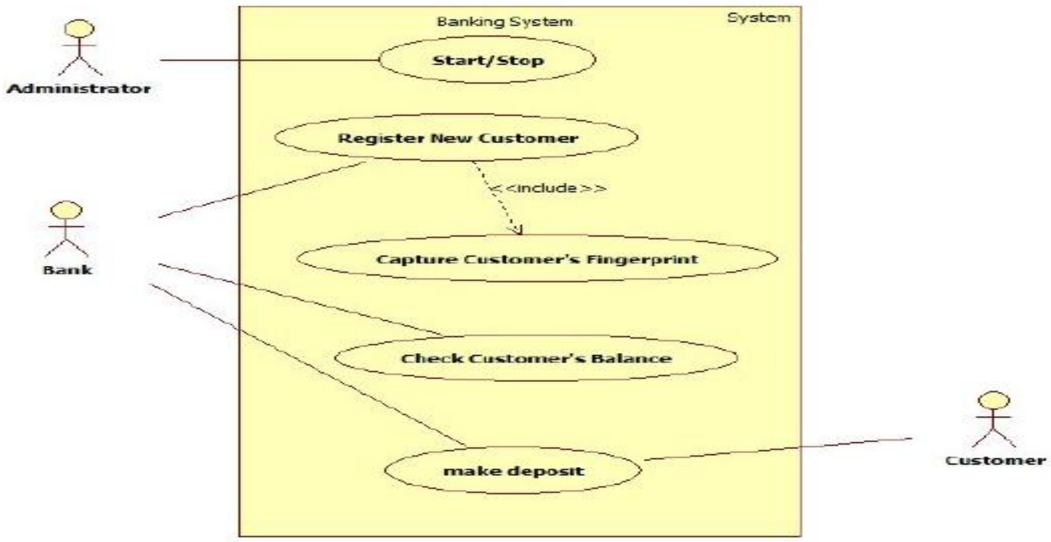

Fig.1.Analysis

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.

4. RESULT ANALYSIS

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. 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.

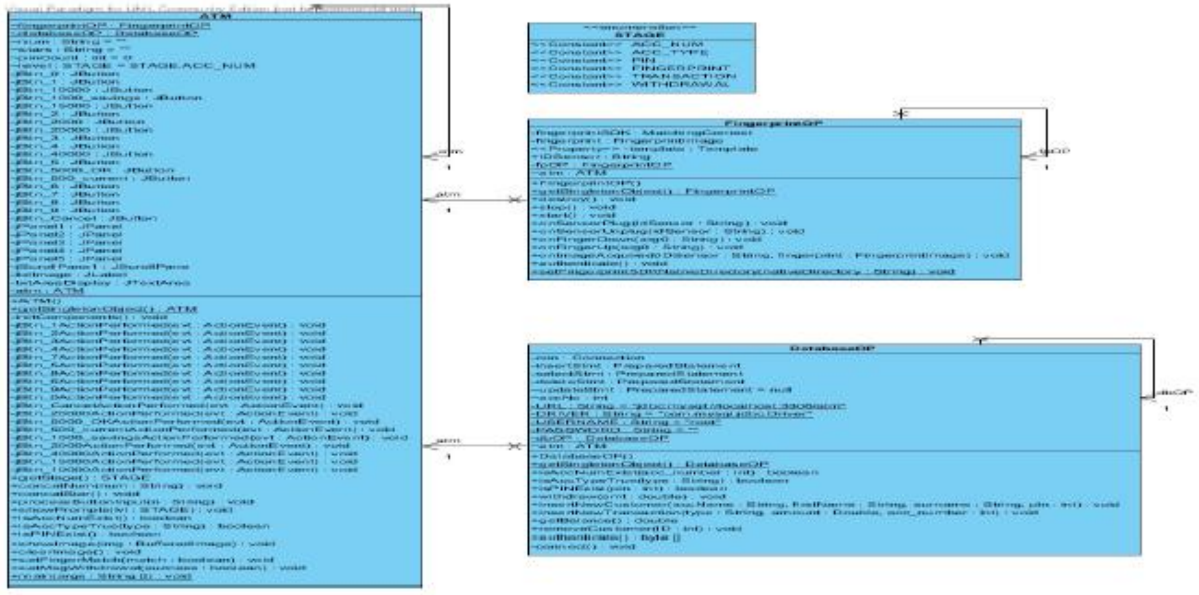

Fig.2.ATM Simulator

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. 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. 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.

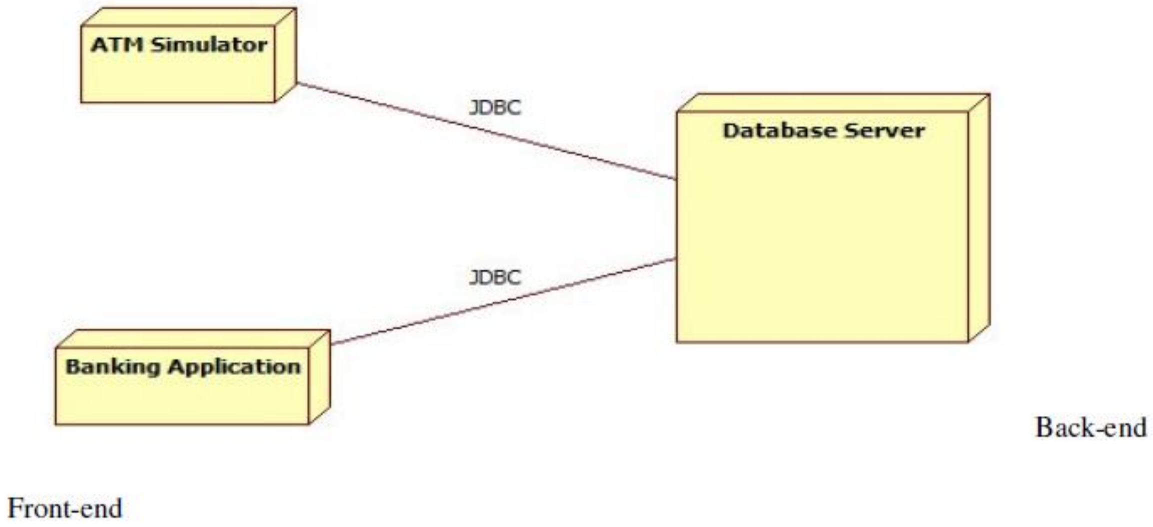

Fig.3.Result analysis

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.

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.

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.