ISSN No. 0976-5697

Volume 3, No. 5, Sept-Oct 2012

International Journal Of Advanced Research In Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Robust Authentication Model for ATM: a Biometric Strategy Measure for Enhancing E-Banking Security in Nigeria

Moses Okechukwu Onyesolu*
Department of Computer Science
Nnamdi Azikiwe University, Awka
Anambra State, Nigeria.
mo.onyesolu@unizik.edu.ng

McChester Odoh
Department of Computer Science
Nnamdi Azikiwe University, Awka
Anambra State, Nigeria.
oguzuruodo@gmail.com

Allwell Ononiwu Akanwa
Department of Computer Science
Nnamdi Azikiwe University, Awka
Anambra State, Nigeria.
kingallwell@yahoo.com

Victor Chekume Nwasor
Directorate of ICT
Nnamdi Azikiwe University, Awka
Anambra State, Nigeria.
vnwasor@yahoo.com

Abstract: Crimes at automated teller machines (ATMs) are issues that face customers and bank operators. A lot of criminals tamper with ATM terminals and steal customers' card details by illegal means. Security of data from unauthorized access, unauthorized modification and destruction of data most especially in ATM systems has been a challenge. The researchers in this work responded to this challenge by developing and simulating a robust fingerprint authentication model for ATM security. The techniques of the Structured System Analysis and Design Methodology (SSADM), Object Oriented Analysis and Design Methodology (OOADM) and the prototyping methodology were adopted for the systematic study and design of the model. Thereafter, we deployed Microsoft Visual C# and MySQL tools to implement the designed system. The system was interfaced with DigitalPersona, a fingerprint reader. The result is a robust fingerprint authentication model for ATM security.

Keywords- ATM, e-banking, fingerprint, PIN, security

I. INTRODUCTION

Nigeria as a nation is among the growing number of countries where almost every facet of her operations or activities is linked via electronic means. The electronic means of transacting business has therefore given customers the option of transacting business at ease. One area where businesses are transacted electronically is the banking sector; this gave rise to electronic banking (e-banking). Electronic banking (also known as online banking or Internet banking) allows customers of a financial institution to conduct financial transactions on a secure website operated by the institution, which can be a retail or virtual bank, credit union or building society [1].

Security is the protection of data from unauthorized access to prevent data loss, unauthorized modification and destruction. Electronic security is any tool, technique or process that protects a system's information assets from threats to confidentiality, integrity, or availability [2]. The importance of security and the need for its effective and efficient management in Nigerian banks cannot be overemphasized. Securing the business environment poses a lot of concern for both the management and customers of the banks. Considering the fact that modern day banking is virtually online, i.e., electronic banking (e-banking), there must be a need for allaying the fears of the customers.

The paper is arranged as follows. Section II provided the background of ATM security and the need for biometrics. Section III introduced the related works on biometric strategy measure for ATM. Section IV described the materials and methods to develop the robust authentication model. Section V presented the results obtained and the discussions on the results. Section VI concluded the paper.

II. RESEARCH BACKGROUND

Globally, ATMs have been adopted by banks because they offer considerable benefits to both banks and their depositors. ATMs enable depositors to withdraw cash at more convenient time and places than during banking hours at branches. In addition, ATMs reduce the costs of servicing some depositor demands. These potential benefits are multiplied when banks share their ATMs, allowing depositors of other banks to access their accounts through a bank's ATM [3]. Banks have deployed ATMs principally to increase their market share and to reduce cost as ATMs are capable of handling more transactions per unit of time than are tellers [4]. In Nigeria the deployment of ATM by banks and its use by bank customers is just gaining ground and has burgeoned in recent times. This has happened especially after the recent consolidation of banks, which has in all probability, made it possible for more banks to afford to deploy ATMs or at least become part of shared networks [5]. The increased deployment of ATMs in the banking sector has made the issue of technology relevance important. ATM services have a history that is less than twenty years in Nigeria. At first, they were operated as elitist services designed for those desirous of exclusive service. Cards were rare and the process for obtaining them tortuous.

Presently, the use of ATM cards has been widely promoted. Banks no longer appear to want personal contact with their customers. Some banks have resorted to penalizing the customer as it were, for not possessing an

ATM card, by debiting the account of such a customer for withdrawing below a certain amount across the counter. Reference [6] reported that although only a bank had an ATM in 1998, by 2004, fourteen of them had acquired the technology. Reference [6] discovered that the adoption of ICT in banks produced largely positive outcomes such as improved customer services, more accurate records, ensuring convenience in business time, prompt and fair attention, and faster services etc. Also, the banks' image is improved creating a more competent market. Work has also been made easier, and more interesting, the competitive edge of banks, relationship with customer, and the solution of basic operational and planning problems has been improved. Fanawopo [7] stated that Nigeria's debit card transactions rose by 93 percent between January 2005 and March 2006 over previous years owing to aggressive roll out initiatives by Nigerian banks, powered by Interswitch network. The number of ATM transactions through the Interswitch network increased from 1,065,972 in 2004 to 14,448,615 in March 2006. This is a rise of 92.6 percent with respect to the previous years. More than 800 ATMs have been deployed on the network, while about 2 million cards have been issued by 23 banks as at March 2006. ATM cards are fast replacing confounding withdrawal forms as a convenient way of getting money from banks. In a way, they are rewriting the rules of financial transaction.

A smart person no longer needs to carry a wallet-full of paper money, as long as he/she has an ATM card. ATMs were the first well-known machines to provide electronic access to customers. With advent of ATM, banks are able to serve customers outside the banking hall. ATM is designed to perform the most important function of bank. It is operated by plastic card with its special features. The plastic card is replacing cheque, personal attendance of the customer, banking hour's restrictions and paper based verification. ATMs have made hard cash just seconds away all throughout the day at every corner of the globe. ATMs allow you to do a number of banking functions-such as withdrawing cash from one's account, making balance inquires and transferring money from one account to another-using a plastic, magnetic-strip card and personal identification number issued by the financial institution.

Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years [8]. A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects [9]. 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 [10]. Passwords and PINs can be illicitly acquired by direct covert 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 PIN's and passwords- birthdays, phone numbers and social security numbers.

Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. 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 [11]. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity [12]. Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.

III. REVIEW OF RELATED WORK

Selvaraju and Sekar [13] presented an embedded Crypto-Biometric authentication scheme for ATM banking systems where cryptography and biometric techniques were fused together for person authentication to ameliorate the security level. The system works in such a way that at enrollment, the fingerprint template including singular points, frequency of ridges and minutiae is stored at the central banking server. At the time of transaction fingerprint image is acquired at the ATM terminal using high resolution fingerprint scanner. The fingerprint image is enhanced and then encrypted using 128 bit private key algorithm. The encrypted image is transmitted to the central server via secured channel. At the banking terminal the image is decrypted using the same key. Based on the decrypted image, minutiae extraction and matching are performed to verify the presented fingerprint image belongs to the claimed user.

Onyesolu and Ezeani [14] investigated the biometric identifier mostly preferred by customers and staff to be fused with ATM machine for better security. The target population of this study was customers and staff of some commercial banks in South-Eastern Nigeria. The study revealed that the population preferred mostly fingerprint biometric character and strongly believed that the incorporation of fingerprint to the existing ATM card and PIN will provide a better security to the ATM.

Amurthy and Redddy [15] developed an embedded fingerprint system, which was used for ATM security applications. In their system, bankers collect customers' finger prints and mobile numbers while opening accounts, then customer only access ATM machine. The working of the ATM machine is such that when a customer place a finger on the finger print module it automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access. Shaikh and Rabaiotti [16] analyzed the United Kingdom identity card scheme. Their analysis approached the scheme from the perspective of high volume public deployment and described a trade-off triangle model. They found that there

is a trade-off between several characteristics, i.e., accuracy, privacy and scalability in biometric based identity management system, where emphasis on one undermines the other.

Considering the utility derived from using ATMs, Patrı´cio, Fisk, and Cunha [17] undertook a qualitative study of a Portuguese bank regarding customers' use of the ATM and identified that security dimension and technical failures were main causes of dissatisfaction in using the ATM. Moutinho and Brownlie [18] found that waiting in queue to use the ATM was the major cause of dissatisfaction among the users. Howcroft [19] noted that dissatisfaction among customers is associated with frequent interruptions and breakdown of ATMs.

IV. MATERIALS AND METHODS

A hybrid methodology derived from the combination of the Structured System Analysis and Design Methodology (SSADM), Object Oriented Analysis and Design Methodology (OOADM) and the prototyping methodology was adopted in this research work. The investigative phase of the SSADM was deployed as the paradigm for systematic study in order to obtain information on the current trends in the research area of ATM security and satisfaction derived in using ATM. A high-level model (HLM) (Fig. 1) and class model (Fig. 2) were defined from the information obtained. A robust authentication model for ATM using fingerprint biometric strategy was implemented from the combination of Fig. 1 and Fig. 2 using Microsoft Visual C# and MySQL. MySQL is the world most used open source relational database management system (RDBMS). DigitalPersona fingerprint reader was interfaced to the model. It was used to capture the fingerprint data stored in the database and fingerprint data used for matching and authentication. Figure 3 through Figure 8 are the user interfaces of the model. It was designed to be user friendly. The interfaces were required to access information in the database. The GUI was used for interactive querying, data capture, information display, and viewing of objects.

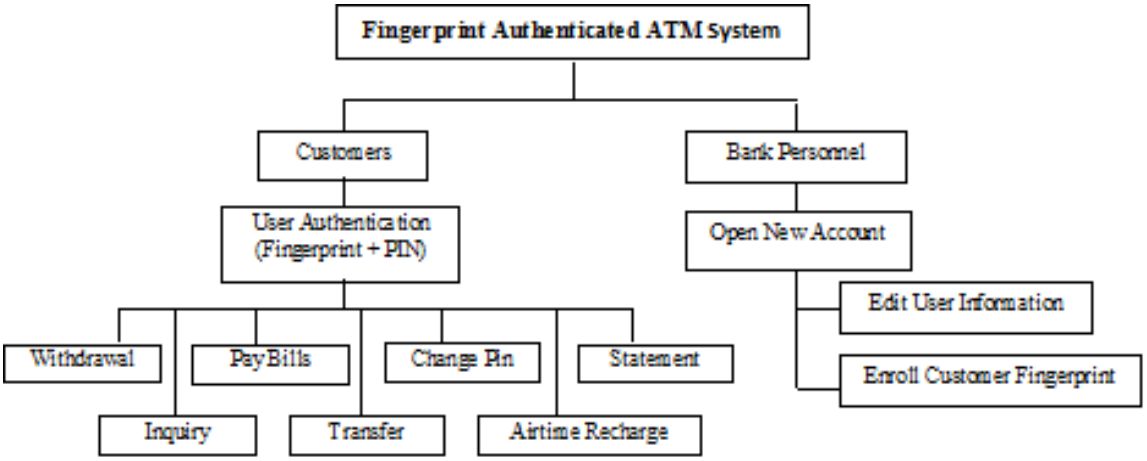


Figure. 1 High Level Model of the ATM System

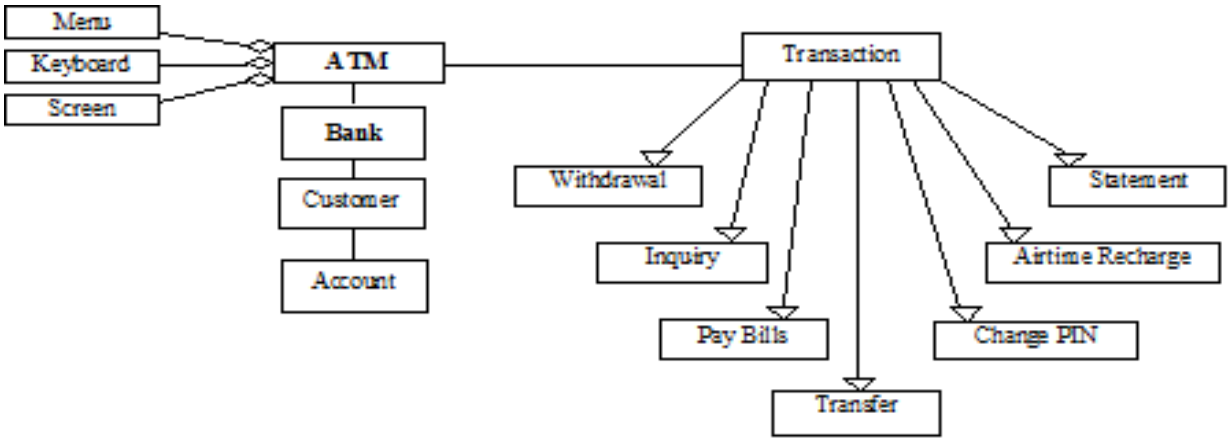


Figure. 2 A Class Model of the ATM System

A. Customer Module:

The components of the customer module of the system include: a page that allows customers enter their account number; a page that allows customers enrolls their fingerprint; a page that accepts customers' 6-digit PIN; a page that allows customers selects the type of transaction they want to perform and pages that foster a customers' successful transaction.

B. Bank Personnel Module:

The components of the bank personnel module (Fig. 3) include: a page that allows the personnel input customer data; a page that enrolls customer fingerprint data and a page that allows the bank personnel to edit customer data.

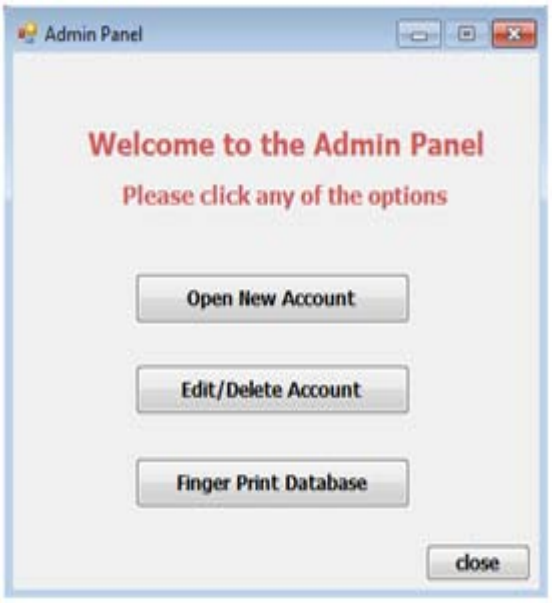


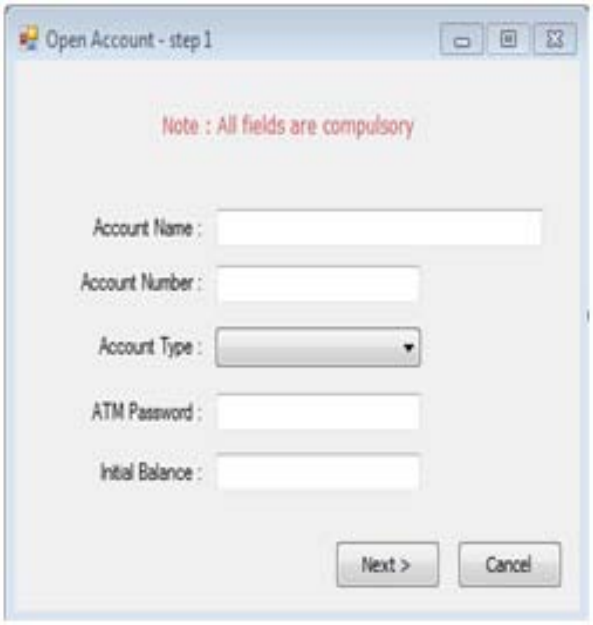
Figure. 3 Bank Personnel Interface

C. *Database* :

The database was designed with MySQL. Entity relationship diagrams (ERDs) were used to derive a set of relational tables that were used to model the application domain. The ERDs were subsequently used to derive the set of relational tables required. Each table in the database had a definite list of fields and their various field definitions. MySQL tables were constructed based on ERDs and were normalized. The table definition involved column names and appropriate data types and width considering the application domain. MySQL Workbench made the work a lot easier.

D. *Customer Profile:*

Customer Profile is a form that accepts the customer's account name, account number (10 - digits), account type (savings, current or credit account), ATM password (6 - digits) and the customer's initial account balance.



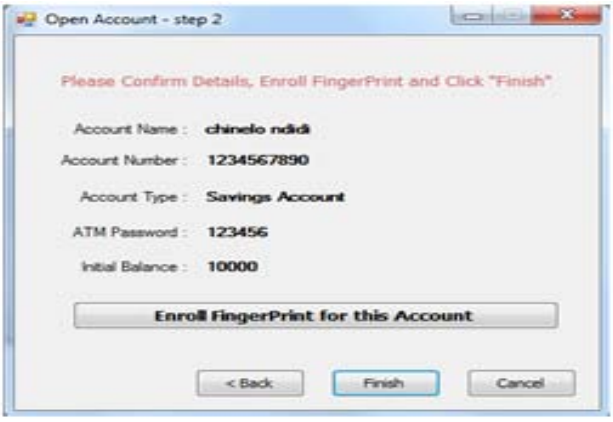


Figure. 4 Customer Opening Account and Enroll Fingerprint Interfaces

E. *Fingerprint Enrollment:*

Fingerprint enrollment (Fig. 5) shows the input received from form one along with a button which when clicked would allow the bank personnel capture the customer's fingerprint.

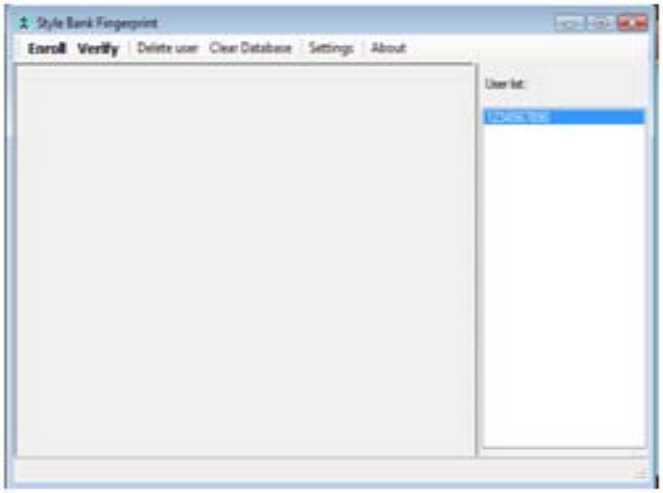


Figure. 5 Fingerprint Enrollment Interface

F. *Output:*

The output is obtained when customers perform transactions on the ATM. The media through which output can be obtained from the system are Visual Display Unit (VDU) and printout from the printer. The system is designed to generate output on the following: cash withdrawal, balance inquiry, fund transfers, airtime recharge, bill payment, account statement and change of secret pin.

Figure 6 The Simulated ATM Interface

V. RESULTS

The results of robust fingerprint authentication model for ATM are presented. These were obtained from the high-level model (HLM) and a class model defined in this work (Fig. 1 and Fig.2). The HLM is a hierarchy of design entities; each entity representing a module. The HLM defined earlier gave rise to a robust fingerprint authentication model for ATM. This model consisted of various modules. The robust fingerprint authentication model for ATM adopted the top-down approach, in which the main program was defined first, followed by the specification of the sub-systems. Here, the program design progressed from the general to the particular, each program unit (module) being progressively refined, designed and listed separately. The modules were integrated together in a way that a program could branch to another module, executes the program there and returns to the main (calling) program after execution.

VI. CONCLUSION

Automatic Teller Machines have become a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, and in particular fingerprint scanning, continues to gain acceptance as a reliable form of securing access through identification and verification processes. Biometrics technology is one area that no segment of the IT industry can afford to ignore. It provides security benefits across the spectrum-from IT vendors to end users, and from security system developers to security system users. Biometric authentication has become more and more popular in the banking and finance sector and it worldwide support and acceptance [20]. The idea of fingerprint is not only for security but also to overcome the lack of customer understanding on ATM concept. Fingerprint authentication is the most popular method among biometric authentication. Fingerprint based identification is one of the most mature and proven techniques. In banking system, biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications. At the time of transaction, customers enroll their fingerprint to a high resolution fingerprint scanner. The fingerprint image is transmitted to the central server via secured channel. At the banking terminal, the minutiae extraction and matching are performed to verify the presented fingerprint image belongs to the claimed user in bank database. The authentication is signed if the minutiae matching are successful. The scheme is fast and more secure.

This paper identifies a high level model for the modification of existing ATM systems using both security protocols as PIN and Biometric fingerprint strategy. We developed a fingerprint mechanism as a biometric measure to enhance the security features of the ATM for effective banking transaction for Nigerian e-banking system. The prototype of the developed application has been found promising on the account of its sensitivity to the recognition of the customers' fingerprint as contained in the database. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines such that only the registered owner of a card can access the bank account.

VII. REFERENCES

[1]. Wikipedia the free encyclopedia (2012). Online Banking. Retrieved July 20, 2012. Source: http://en.wikipedia.org/wiki/online_banking

[2]. Nweke, C.S. and Okoli, N. S. (2012). Simulation of a fingerprint authenticated teller machine. Unpublished Bachelor's Project. Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria.

[3]. McAndrews, J.J. (2003). Automated teller machine network pricing- A review of the literature. Review of Network Economics, Federal Reserve Bank of New York. 2(2) New York, USA.

[4]. Laderman, E.S. (1990). The public policy implications of state laws pertaining to automated teller machines. Federal Reserve Bank of San Francisco Economic Review, 1, pp. 43-58.

[5]. Fasan, R. (2007). Banks, customer relation and use of ATM cards. Business Day Newspapers. Retrieved February 28, 2008. Source: http://www.businessdayonline.com

[6]. Agboola, A. (2006). Information and communication technology (ICT) in banking operations in Nigeria: An evaluation of recent experiences. Retrieved December 25, 2007. Source: http://unpan1.un.org

[7]. Fanawopo, S. (2006). World without cash-Nigeria's payment card grows significantly. Retrieved October 15, 2007. Source: http://www.sunnewsonline.com

[8]. Boateng, R. and Molla, A. (2006). Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons. *Journal of Internet Banking and Commerce*, 11(2), pp. 1-11.

[9]. Amurth, P.K. and Redddy, M.S. (2012). Implementation of ATM Security by Using Fingerprint recognition and GSM, International Journal of Electronics Communication and Computer Engineering, 3(1), pp. 83-86.

[10]. Ratha, N.K, Connell, J.H. and Bolle, R.M. (2001). Enhancing Security and Privacy in Biometrics-based Authentication Systems. IBM Systems Journal, 40(3), pp. 614-634.

[11]. Ratha, N.K., Chikkerur, S., Connell, J.H. and Bolle, R.M. (2007). Generating Cancelable Fingerprint Templates. IEEE Transaction on Pattern Analysis and Machine Intelligence, 29(4).

[12]. Schouten, B. and Jacobs, B. (2009). Biometrics and their use in e-passport. Image and Vision Computing, 27, pp. 305–312.

[13]. Selvaraju, N. and Sekar, G. (2010). A Method to Improve the Security Level of ATM Banking Systems Using AES Algorithm. International Journal of Computer Applications, 3(6), pp. 5-9.

[14]. Onyesolu, M.O. and Ezeani, M.I. (2012). ATM Security Using Fingerprint Biometric Identifier: An Investigative Study. International Journal of Advanced Computer Science and Applications, 3(5), pp. 67-74.

[15]. Amurthy, P.K. and Redddy, M.S. (2012). Implementation of ATM Security by Using Fingerprint recognition and

GSM. International Journal of Electronics Communication and Computer Engineering, 3(1), pp. 83-86.

[16]. Shaikh, S.A. and Rabaiotti, J.R. (2010). Characteristic trade-offs in designing large-scale biometric-based identity management systems, Journal of Network and Computer Applications, 33, pp. 342–351.

[17]. Patrı´cio, L., Fisk, R.P. and Cunha, J.F. (2003). Improving satisfaction with bank service offerings. Managing Service Quality, 13 (6), pp. 471-482.

[18]. Moutinho, L. and Brownlie, D.T. (1989). Customer satisfaction with bank services: A multidimensional space analysis, International Journal of Bank Marketing, 7(5), pp. 23-7.

[19]. Howcroft, J.B. (1991).Customer satisfaction in retail banking. Service Industry Journal, pp. 11-17.

[20]. Kumar, D. and Ryu, Y. (2009). A Brief Introduction of Biometrics and Fingerprint Payment Technology. International Journal of Advanced Science and Technology, 4, pp. 25-37.