A Fingerprint & Pin Authentication to Enhance Security At The Automatic Teller Machines

Dondo Jacqueline Akinyi Madara, Dr. George Okeyo, Dr. Michael Kimwele

Abstract- The need of money can only be satisfied when you are carrying money with you. That also increases the risk of getting robbed. This research focuses on how to enhance security of transactions in Automatic Teller Machine system using a multi-factor authentication system (PIN and Fingerprint). This research proposed a highly secured Automatic Teller Machine banking system using an optimized Advanced Encryption Standard (AES) algorithm. This research proposes two levels of security. Firstly we consider the security level at the client side by providing biometric authentication scheme along with a password of 4-digit long. Biometric authentication is achieved by considering the fingerprint image of the client. Secondly we ensure a secured communication link between the client machines to the bank server using an optimized energy efficient AES processor. The fingerprint image is the data for encryption process and 4-digit long password is the symmetric key for the encryption process. To get a low power consuming Automatic Teller Machine, an optimized AES algorithm is proposed in this research. In this system biometric and cryptography techniques are used together for personal identity authentication to improve the security level.

Index Terms- AES Algorithm, AES Processor, ATM, Biometric, Cryptography, Encryption, Fingerprint, Multi-factor

1 INTRODUCTION

1.1 Background

Masquerade attacks and other criminal activities at ATMs have become a nationwide issue that faces not only customers, but also bank operators. According to Richard et al (2006) these financial crime cases rises repeatedly in recent years. 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 (Amurthy and Redddy 2012). The prevailing techniques of user authentication, which involves the use of passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations (Ratha et al 2001). 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.

Many people use easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. The increase use of ATMs has seen even the illiterate users most of whom write down their PINs or ask for assistance at the ATMs exposing their PINs. 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 (Oxford English Dictionary) 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 Ratha et al (2007). It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity Schouten and Jacobs (2009). 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,

- *Jaqueline Dondo is currently pursuing masters degree program in Computer Systems in Jomo Kenyatta University of Agriculture & Technology, Kenya, E-mail: jacklinedon@gmail.com*
- *Co-Author Dr. Okeyo & Dr. Kimwele are lecturers in Jomo Kenyatta University of Agriculture & Technology, Kenya*

cannot be copied and cannot be lost. Bioinformatics is an interdisciplinary scientific field that develops methods and software tools for storing, retrieving, organizing and analyzing biological data. As globalization, networking, information and digital era's coming, the demand of high reliability of our identity verification is growing. Among the existing biometric methods, fingerprint biometrics can be an affordable and accurate authentication technology that has been already successfully and widely employed.

This research presents a secured and an energy efficient ATM banking system that is highly secured system compared with the existing one. At present most of the ATM systems use triple data Encryption Standard (3DES). Which has some drawbacks; such as, it is vulnerable to differential attacks and also slow in performance. Ali et. al. (2013) This research presents security in two ways in which both the fingerprint image for the client side security and the AES algorithm for the secured communication in between. This research presents security in two ways in which both the fingerprint image for the client side security and the AES algorithm for the secured communication in between. Based on these perspectives, Advanced Encryption Standard was accepted as a FIPS standard in November 2001, after which AES became the most popular encryption standard all over the world. A lot of researchers are working to improve the speed of AES as well as the other aspects like area, latency, power etc. To make the AES faster and securer, some researchers introduced hardware realizations and s-box optimizations. Today most of the researchers involving the execution of the Advanced Encryption Standard (AES) algorithm are fallen into three areas: ultra-high-speed encryption, very low power consumption, and algorithmic integrity. Fakir et. al. (2013)

1.2 Statement of the Problem

Personal banking information is highly sensitive and users are vulnerable while using ATMs Mohammed (2015). Keypads in particular have been exploited by criminals who have installed small cameras or touch-sensitive overlays, or in some cases have simply observed users as they have keyed in their pins Chris (2009). The physical security of users is also important. ATMs are open late at night but often have limited security. Users may feel anxiety and, in those cases, it is best that they complete their ATM operations as quickly as possible. The frequency at which ATM fraud is increasing and not being detected is creating fear, anxiety and loss of confidence in the banking sector that there is need to improve the existing user authentication process. Around 4,000 pages of data containing Cypriot credit cards were found on a computer belonging to thieves (New Europe 2008) Devices capable of scanning bank and credit cards details were placed on cash machine outside a supermarket in UK (BBC News, 2006)

1.3 Justification

One of the major problems people face is the loss of the password and not remembering it again, these has caused a lot of damage to people and organizations. ATM fraud has been very common in all banks and the problems has created fear in many costumers heart that they prefer going to the bank to collect their money than to use an ATM, also many people are illiterate that they don't know how to use the ATM card.

In the field of computer security, one of the most damaging attacks is masquerading, in which an attacker assumes the identity of a legitimate user in a computer system. Masquerade attacks typically occur when an intruder obtains a legitimate user's password or when a user leaves their workstation unattended without any sort of locking mechanism in place. It is difficult to detect this type of security breach at its initiation because the attacker appears to be a normal user with valid authority and privileges. This difficulty underlines the importance of equipping computer systems with the ability to distinguish masquerading attacker actions from legitimate user activities. Security especially at our banks has been compromised. There are cases of impersonation at the ATM machines and it would be difficult to authenticate someone just with the ATM card and PIN numbers. The current authentication systems are characterized by an increasing interest in biometric techniques. Among these techniques are face, facial thermo gram, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature and voiceprint. All these methods have different degrees of uniqueness, permanence, measurability, performance, user's acceptability and robustness against circumvention Akwaja (2010) finger print is the most preferred.

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 behavioral 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 research focuses on how to enhance security of transactions in ATM system using fingerprint. Present research deals with new innovative model for biometric ATMs which replaces card system by biometric technology for operating ATMs for example In a bid to address issues of safety of customers' funds and avoiding losses through compromise of Personal Identification Numbers (PIN), the apex bank, Central Bank of Nigeria (CBN) is to introduce Biometric authentication of Point of Sale (PoS) and Automated Teller Machines (ATMs) by 2015 according to Leadership New paper (10-07-2013).

1.4 Research Questions

Can the implementation of a multifactor technology such as use of fingerprint and PIN be utilized as a useful identifier in improving security at the ATM machines?

Are there more benefits in using the AES algorithm in a Bank employing a multifactor security system that use PIN and fingerprint for their ATMs?

Will the use of biometric system for ATM authentication be acceptable to the users?

1.5 Objectives

Broad Objective

The purpose of this research is to enhance the security of the existing ATM (Automated Teller Machine) system by integrating the existing PIN (Personal Identification Number) with the fingerprint.

Specific objective

1. To identify different areas that a multifactor security system that use PIN and fingerprint has been utilized.
2. To propose the use of fingerprint and PIN as an authentication system in the Bank's ATM.
3. To propose a low power consuming ATM machine using the AES algorithm.

1.6 Scope of research

The first milestone of my research is learning the biometrics especially the use of thumb/figure recognition. Then we learnt how the PIN verification methods work. Lastly we propose a multifactor authentication model system.

1.7 Limitations of the research

Banks don't not divulge sensitive information about their scale of operation

Budgetary constraints

The research is based on secondary data taken from content analysis and not the bank. This was not accurate.

Security in banking is wide and we have limited our research to one region. This might not represent the nature of all banks.

Bias respondents

2 LITERATURE REVIEW

2.1 Introduction

Since security measures at ATM centers play a significant role in preventing attacks on customers money, several researches have proposed the used of fingerprint in a like manner of this research, to shift from PIN to biometric based security. Fingerprinting has been the most widely used during the 20th century. The maturity of Biometric techniques and generally the dramatic improvement of the captured devices have led to the research of fingerprinting in multiple applications but in the last years, minutiae have been the main type of algorithm used. The minutiae are relatively stable and robust to contrast, image resolution and global distortion as compared to other fingerprint representation Fatai et al. (2014). Jeroen et al. (2011) provided a better understanding of the benefits and limitation of integration of biometrics in a PIN-base payment authentication system. Based on their review they proposed a biometric that can be integrated in a PIN-based authentication infrastructure by binding a fixed binary, renewable string to a noisy biometric sample.

2.2 Related studies

The South African Social Security Agency (SASSA) has introduced a new SASSA Payment Card that has a fingerprint authenticated features. The card is a SASSA branded smart payment MasterCard, which has an embedded chip containing personal details, fingerprint and secret PIN, with the card the customers can easily withdraw and make payment at point-of-sale (POS) center, purchase airtime, pay water and electricity bill from the accounts, or open accounts. (SAAS, 2013).

Wang Y. et al (2007) proposed a fingerprint orientation model based on 2D Fourier expansions (FOMFE) in the phase plane. Though FOMFE does not require prior knowledge of singular points, it is able to describe the overall ridge topology seamlessly. Fengling et al (2005) proposed a smartcard based encryption/authentication scheme for ATM banking system. The first layer of the scheme is used to perform authentication based on available information on the smartcard. Fingerprint based authentication via feature and minutiae matching then followed on the second layer. Das and Jhunu (2011) focused on vulnerabilities and the increasing wave of criminal activities occurring at ATMs and presented a prototype fingerprint authentication for enhancing security. The systems adopt the same measure as the current work by formulating modules for fingerprint enrolment, enhancement, feature extraction and database and matching. Santhi and Kumar (2012) proposed an ATM security enhancing method with secured Personal Identification Image (PII) process. A detailed research on various existing biometric systems is also presented stating the strengths and limitations. Bhosale and Sawant (2012) and Ibiyemi et al (2012) present groundbreaking models for biometric ATMs which replaces card system with biometric technology. The proposed systems hybridize feature-based fingerprint, iris and PIN to provide reliable and fool-proof ATM authentication.

Customers must be convinced that the technologies provide more benefit than the card-and-PIN system, which works well, said John Hall, spokesman for the American Bankers Association. The cards also serve functions beyond the ATMs, as debit cards and as advertising for the banks. "Getting that wallet space is important," said Bill Spence, a biometric expert with Campbell, Calif.-based Recognition Systems Inc. The growers wouldn't need to carry ATM cards, which can be a lure for thieves. "Biometrics is certainly the most secure form of authentication," said Avivah Litan, an analyst with Gartner Inc., a Stamford, Conn.-based technology analysis firm. "It's the hardest to imitate and duplicate." Jain, A.et. al. (2000)

However, companies that make automated teller machines have found budding markets for the fingerprint technology in South America, where citizens already are accustomed to the use of fingerprints for general identification, such as ID cards they carry. Diebold Inc. of North Canton, Ohio, has supplied fingerprint-capable ATMs to a bank in Chile that is using them in a pilot project. Last year Dayton, Ohio-based NCR Corp. installed 400 of them in Colombia. BanCafe, Colombia's fifth largest bank, bought the ATMs at the end of 2002 for added security for coffee growers and to get them to open accounts.

Mali et al (2012) provided a network security framework for real time ATM application using a combination of PIN, thumb scanning and face recognition to foster security. The proposed framework is expected to register thumb and face features to be stored at a server side in encrypted format. Authentication is done by decrypting patterns from database, and matching with input pattern before access is granted for ATM operations. The integrated system uses Principal Component Analysis (PCA) and Eigen algorithm for face recognition, LSB algorithm for stegnogaphy and AES algorithm for cryptography. Though the framework looks promising, its practicality is not supported by detailed implementation and evaluation. Abayomi et al (2012) proposed an enhanced e-banking system where customer can access multiple accounts over different banks institutions with a single ATM card with fingerprint authentication. A match-on-card technique was used that relies on a one-to-one matching where the data from the ATM fingerprint sensor is compared only to the template stored on the user's ATM card. This will help in privacy concern of users; the system will also help the users to have access to multiple accounts with a single ATM card. It is secured and help in reducing ATM fraud. This research presents security in two ways. This design considers the fingerprint image for the client side security and also considers the AES algorithm for the secured communication in between the client and server. A lot of researchers are working to improve the speed of AES as well as the other aspects like area, latency, power etc. To make the AES faster and securer some researchers introduced hardware realizations and s-box optimizations. Today most of the researchers involving the execution of the Advanced Encryption Standard (AES) algorithm are fallen into three areas: ultra-high-speed encryption, very low power consumption, and algorithmic integrity. Many research works have been done by different hardware realizations using ASIC and FPGA technology. Some References present the fastest FPGA realization of the AES algorithm. Fingerprint based authentication is more secure, reliable and standard than the password based authentication. Finger-scan biometric is based on the distinctive characteristics of the human fingerprint. Our existing ATM system is password based. The limitation of this system is that it fails to identify the person rather it only identify the card and password as well as the communication link is not secured. , which have access to be hacked. The proposed ATM system is able to overcome this type

of limitations because proposed ATM system is fingerprint based.

2.3 Identified Gap

AT present most of the ATM systems use triple-data Encryption Standard (DES) Nawaz et. al.(2013) but the triple-DES has some drawbacks. It is vulnerable to differential attacks and also slow in performance. DES (Data Encryption Standard) has been used as a de facto standard cipher for more than 20 years. In 2001, NIST (National Institute of Standards and Technology) made Rijndael the new standard cipher AES Daemen and Rijmen (2001), NIST (2001). Personal banking information is highly sensitive and users are vulnerable while using ATMs Mohammed (2015). Keypads in particular have been exploited by criminals

2.4 A conventional ATM system

ATM is the abbreviation of "Automated Teller Machine". This machine allows the account holder to have transactions with their own accounts without allowing them to access the entire bank's database. The idea of self-service in retail banking was developed through independent and simultaneous efforts in Japan, Sweden, the United Kingdom and the United States. In the USA, Luther George Simjian has been credited with developing and building the first cash dispenser machine. The first cash dispensing device was used in Tokyo in 1966.

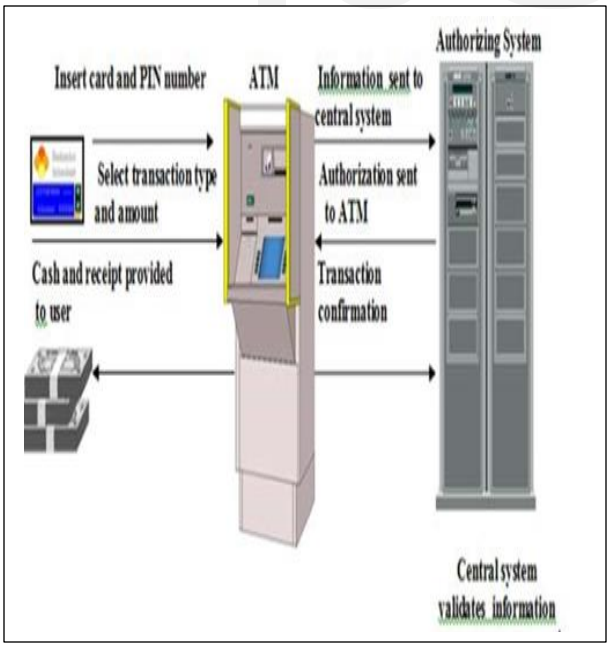

Figure 1 A Conventional ATM System

ATM first came into use in December 1972 in the UK. IBM 2984 was designed for request of Lloyds Bank. ATM is typically connected directly to their hosts or ATM Controller via either ADSL or dial-up modem over a telephone line or directly via a leased line. For transaction security all communication traffic between ATM and transaction process is encrypted by cryptography. Nowadays, most of ATM uses a Microsoft OS primarily Windows XP Professional or Windows XP Embedded or Linux.

2.5 Fingerprint

Fingerprint is a characteristic which is unique for each person. Every fingerprint contain unique identifiable piece of information. The uniqueness in each fingerprint is due to the peculiar genetic code of DNA in each person. Ridges and valleys are the parts of fingerprint that provide friction for the skin. The direction and location of ridges make the identification. A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human. There are three types of fingerprint patterns.

2.6 AES Algorithm

The Rijndael algorithm referred to as the AES Algorithm, is a symmetric key block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Figure 2 shows that AES has four stages which are required for every round except that the last round excludes the mix column phase and the first round has only key addition.

The four stages of Rijndael algorithm (AES algorithm) are:

- Substitute bytes: This function uses an S-box to perform a byte-by-byte substitution of the block. For encryption and decryption, this function is indicated by SubBytes () and InvSubBytes () respectively.
- Shiftrows: This is a simple permutation. For encryption and decryption, this function is indicated by ShiftRows () and InvShiftRows () respectively.
- Mix Columns: This is a substitution that makes use of arithmetic over GF (28), with the irreducible polynomial “m(x) = x8 + x4 + x3 + x +1”. For encryption and decryption, this function is indicated by MixColumns () and InvMixColumns () respectively.

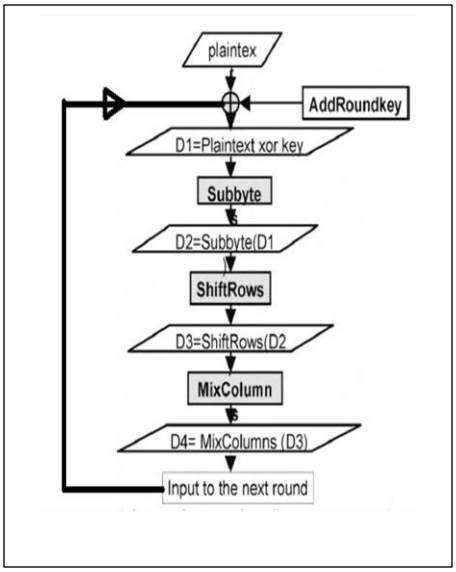

Figure 2 Proposed ATM System

- Add round key: This function does a bitwise XOR operation of the current block with a portion of the expanded key. For both encryption and decryption this function is indicated by AddRoundKey (). For the AddRoundKey () stage, the inverse is achieved by XORing the same round key to the block, using the result: A ⊕A⊕ B = B.

3 RESEARCH METHODOLOGY

3.1 Introduction

The methodology proposed by Webster and Watson (2002) was followed. In the subsequent pages of this chapter, the steps taken to identify relevant literature is presented, along with the results of this procedure. The purpose of this research is to present a secured and an energy efficient ATM banking system that is highly secured. At present most of the ATM systems use triple-data Encryption Standard (DES) but the triple-DES has some drawbacks. It is vulnerable to differential attacks and also slow in performance. Nawaz (2013). This research presents security in two ways, a design that considers the fingerprint image for the client side security and also consider the AES algorithm for the secured communication in between the client and server. Reducing the power consumption of AES (Advanced Encryption Standard) circuits is a critical problem when the circuits are used in embedded systems. Many circuit architectures for AES have been proposed recently and their performances have been evaluated by using ASIC libraries Kuo et al. (2001), However, most of them are simple implementations according to the AES specification, and there is no report of low-power AES implementations, as far as the authors know. In this research, we investigated a design methodology for a low-power AES. Although many power reduction techniques for IP cores are known for various design abstraction levels from the algorithm level to the transistor level Chandrakasan and Brodersen (2007)[2], we focused on the logic level (gate level), because the power optimization techniques at this level can be applied in many applications. The optimizations at the other levels cannot be adopted as often, because the AES circuit is usually used as an IP core in a system, and changing the algorithm, operator scheduling, data-path architecture, and/or arrangements of transistors of the AES is difficult under given requirements for throughput, clock speed, and technology library Morioka and Akashi (2014). Security has become a great issue in every part of life. Passing of information faces massive problems due to various types of attacks into the communication link. The biometric authentication process adds a new dimension of security for any person sensitive to authentication. In this chapter we describe the research methodology of this research, explain the sample selection, describe the procedure used in designing the instrument and collecting the data, and provide an explanation of the statistical procedures used to analyze the data.

3.2 Research design

A descriptive research methodology is used for this research because it portrays accurately that most ATM users have no confidence in the use of PIN as the only means of identity at the ATM machines, by conducting a survey and fact finding. We used some survey methods like comparative and correlation approach conducting survey on users and also existing literature. This research has some aspects of qualitative methods where the users opinions and attitude is used to come up with the conclusions about the use of PIN and biometric at the ATM. Gravetter and Forzano (2011) explain that descriptive research design involves the measurement of a variable or a set of variables as they naturally exist. The research is aimed at collecting information from respondents in determining e-learning security issues. Chandran (2004) notes that descriptive research designs are used in studies that answers the “who”, “what”, “when”, “where” and “how” questions. This design describe what is prevalent in security challenges in ATM systems. The use of descriptive research design enabled the description of the identification

of security issues affecting ATM system in banking sector in Kenya. A survey is administered to a selected sample from Machakos. The term 'survey' is commonly applied to a research methodology designed to collect data from a specific population, or a sample from that population, and typically utilizes a questionnaire or an interview as the survey instrument (Robson, 1993)

3.3 Research population

The total population of the research is banks that are in Machakos County. Machakos County has an estimated population of 1,098,584 people machakos county profile (2015) which includes five towns; Athi River, Machakos, Kangundo-Tala, Kathiani and Masii. The target population is the ATM users which the researcher is interested in describing and making statistical inferences about. It refers to the entire group of individual or objects to which researchers are interested in generalizing the conclusion.

3.4 Sample and sampling techniques

For this research, my sampling unit is geographical where Machakos town is sampled. The methodology for this research is a stratified random sample of bank users across the town. Gay (1987) reports: Random sampling is the best single way to obtain a representative sample.

3.5 Data collection instruments

This research had two sets of data, the primary data and the secondary data. The primary data was collected using questionnaires and personal interviews directly from the ATM users and a central-site intercept survey in which potential audience members were approached in a public area and asked to respond to a quick questionnaire. The research was conducted on an existing group, numerical data is collected Data for this research is obtained through the following: Questionnaire: this is administered on the customers and staff of the selected banks. This involves close-response questions with only 'yes' or 'no" answers to assist in carrying out the research. Personal Interview: for all the technical questions the secondary data is collected mainly from Library research or content analysis. This aids in consulting relevant literature already written on the subject

3.6 Data analysis

Data analysis involved editing, coding, classification and tabulating of the data collected. The editing is done by me scrutinizing questionnaires to detect errors and omissions then translate or rewrite the responses especially because some handwritings might not be clear, this was achieved by conducting a field editing where clarity is made as the data is being collected. Centralized editing after the data is collected. The analysis is done by SPSS and there was need of assigning numerical values to the answers given during data collection for the sake of coding and classification using tables to tabulate the findings to summarize the survey.

Acknowledgments

I thank God almighty for giving me patience, knowledge and understanding and most importantly for giving me life. I thank Dr. Kimwele and Dr. Okeyo, Lecturers at Jomo Kenyatta University of agriculture and Technology for guiding me through my research, to my mother Foska Dondo for her encouragement.

REFERENCES

[1] (AES)", FIPS Publication 197, http://csrc.nist.gov/encryption/ aes/index.html, Nov. 2001.
[2] A.P. Chandrakasan and R.W. Brodersen (eds.), Low Power Digital CMOS Design, Kluwer Academic Publishers, 2005.
[3] Abayomi-Alli A., Omidiora E.O., Olabiyisi E.O., and Ojo J.A., Enhanced E-Banking System with Match-On-Card Fingerprint Authentication and MultiAccount ATM Card. The Journal of Computer Science and Its Aplication, An International Journal of the Computer Society of Nigeria (NCS), V0l. 19, No.2 December, 2012
[4] Akwaja Chima, Nigeria Connects 99 million Subscribers, Fin. Standard., 2010, 10: 15-512.
[5] ATM scam targets hundreds of credit cards', New Europe, issue: 793, 4 August 2008, From http://www.neurope.eu/articles/89221.php (last visited on 20 April 2009).
[6] B, Schouten and B. Jacobs, Biometrics and their use in e-passport, Image and Vision Computing vol. 27, pp. 305–312. 2009,
[7] B. Richard and M. Alemayehu, Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons. Journal of Internet Banking and Commerce, vol. 11, no. 2, 2006. Downloaded March 15, 2012 from http://www.arraydev.com/commerce/jibc/
[8] Bhosale ST, and Sawant BS, Security in eBanking via Card-less Biometric ATMS. International Journal of Advanced Technology & Engineering Research, 2012, 2: 9-12.
[9] Chris. Christian Science Monitor. 'Guard your card: ATM fraud grows more sophisticated'. July 23, 2003.From http://www.csmonitor.com/2003/0721/p15s01-

wmcn.html
[10] Das SS, and Jhunu D, Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System. International Journal of Information and Communication Technology Research, 2011, 197-203.
[11] Fatai, O.W., Awotunde, J.B. and Matluko, O.E, A Novel System of Fingerprint Recognition Approach for Immigration Control, IOSR Journal of Computer Engineering (IOSR-JCE) 2278-8727Volume 16, Issue 3, Ver. III (May-Jun. 2014), PP 39-42.
[12] Fengling H, Jiankun H, Xinhuo Y, Yong F, and Jie Z, A novel Hybrid Crypto- Biometric Authentication Scheme for ATM Based Banking Applications. Lect Notes Comput Sci, 2005, 3832: 675-681.
[13] H. Kuo et al., "Architectural Optimization for a 1.82 Gbits/sec VLSI Implementation of the AES Rijndael Algorithm," Proc. CHES2001, LNCS Vol. 2162, pp. 53–67, 2001
[14] http://leadership.ng/news/100713/cashless-policy-cbnintroduce-biometrics-atms-pos-2015#sthash .I0I5wd2G.dpuf Leadership New paper, 10-07-2013.
[15] Ibiyemi T. S, Obaje S. E, and Badejo J Development of Iris and Fingerprint Biometric Authenticated Smart ATM Device & Card. 24th National Conference of the Nigeria Computer Society (NCS), 2012.
[16] J. Daemen and V. Rijmen, “AES Proposal: Rijndael,” http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf.
[17] Jain, A., Hong, L., & Pankanti, S. (2000). Biometric Identification, Communications of the ACM, 43(2), p. 91-98.
[18] Jeroen B., Ileana B., Koen G., and Emile K., Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment infrastructure, 2011.
[19] Kuykendall, Lavonne and W. A. Lee, Intermediary Risk? Card Hack Puts OSOs in the Hot Seat, American Banker, February 21 2003.
[20] M. Theofanos, B. Stanton, and C. A. Wolfson, Usability & Biometrics: Ensuring Successful Biometric Systems. National Institute of Standards and Technology (NIST), 2008.
[21] Machakos county profile, from http://www.machakosgovernment.com/MachakosProfile.aspx last visited on 10 October 8, 2015
[22] Mali P, Salunke S, Mane R, and Khatavkar P., Multilevel ATM Security Based On Two Factor Biometrics, 2012, IJERT 1: 8.
[23] N.K. Ratha, J.H. Connell, and R.M. Bolle, Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.
[24] N.K. Ratha, S. Chikkerur, J.H. Connell and R.M. Bolle. Generating Cancelable Fingerprint Templates”, IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, 2007.
[25] National Institute of Standards and Technology (NIST), “Advanced Encryption Standard
[26] P.K. Amurthy and M.S. Redddy, Implementation of ATM Security by Using Fingerprint recognition and GSM, International Journal of Electronics Communication and Computer Engineering vol.3, no. 1, pp. 83-86, 2012.
[27] Santhi B, and Kumar RK, Novel Hybrid Technology in ATM Security Using Biometrics. Journal of Theoretical and Applied Information Technology, 2012, 37: 217-223.
[28] Shoppers are targeted in ATM scam‘, BBC News, 11 March 2006, available at http://news.bbc.co.uk/2/hi/uk_news/england/tees/4796002.stm (last visited on 20 April 2009).
[29] Swann, J., Teaching Ethics: It's the Right Thing to Do. OR/MS Today, 2004, 31:10.
[30] The South African Social Security Agency (SASSA), A leader in the delivery of social security services. Re-register to get yours: SASSA HOUSE 501 Prodinsa Building Cnr Steve Biko and Pretorius Street Pretoria, 2013.
[31] Travel Guide for Your Finances. ‘Card Fishing ATM Scam’. Card Fishing ATM Scam. December 27, 2006. From http://www.travelfinances.com/blog/index.php/2006/12/27/card-fishing-atm-scam/
[32] U. Uludag, Secure biometric systems, Ph.D. dissertation, Michigan State University, 2006.
[33] Wang Y, Hu J, and Phillips D, A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing. IEEE Trans Pattern Anal Mach Intell, 2007, 29: 573-585.
[34] Webster, J. & Watson, R.T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly, 26(2), pp. xiii-xxiii. West, D.M. (2004).