Volume 13 | Number 2 | April-June 2018

Journal of Applied Security Research

An International Journal of Police Security Operations & Practices

John Kostanoski, Editor

Routledge Taylor & Francis Group

Article

Global Civil Society: Challenges of Security and Policing □

Brian F. Kingshott & Jan B. Kingshott

Pages: 385-401

Published online: 08 Sep 2016

Abstract | Full Text | References |
PDF (405 KB)

191
Views
0
CrossRef citations
0
Altmetric

Article

The Dilemma of Terrorist Retaliations Against Schools in Sectarian Conflict Regions: The Case of Lebanon □

Hoda Baytiyeh

Pages: 402-421

Published online: 08 Sep 2016

Abstract | Full Text | References |
PDF (438 KB)

89
Views
1
CrossRef citations
0
Altmetric

Article

Visible School Security Measures across Diverse Middle and High School Settings: Typologies and Predictors □

Katarzyna T. Steinka-Fry, Benjamin W. Fisher & Emily E. Tanner-Smith

Pages: 422-436

Published online: 08 Sep 2016

Abstract | Full Text | References |
PDF (405 KB)

Technology

Authentication System □

Ameh Innocent Ameh, Olayemi Mikail Olanyi & Olumide Sunday Adewale

Pages: 469-488

Published online: 08 Sep 2016

Abstract | Full Text | References |
PDF (980 KB)

79
Views
0
CrossRef citations
0
Altmetric

Article

OMAMIDS: Ontology Based Multi-Agent Model Intrusion Detection System for Detecting Web Service Attacks □

K. Anusha & E. Sathiyamoorthy

Pages: 489-508

Published online: 08 Sep 2016

Abstract | Full Text | References |
PDF (1200 KB)

64
Views
1
CrossRef citations
0
Altmetric

Student Papers

Article

Securing Cyberspace: Man versus Machine □

Christine Vega

Pages: 509-516

Published online: 08 Sep 2016

Abstract | Full Text | References |
PDF (299 KB)

152
Views

0
CrossRef citations
0
Altmetric

Article

OPM Hack: The Most Dangerous Threat to the Federal Government Today

Stephanie Gootman

Pages: 517-525

Published online: 08 Sep 2016

Abstract | Full Text | References |
PDF (260 KB)

796
Views
0
CrossRef citations
3
Altmetric

Article

Criminal Liability of Insolvent People Using Credit Cards

Puttipong Huntopap

Pages: 526-538

Published online: 08 Sep 2016

Abstract | Full Text | References |
PDF (328 KB)

44
Views
0
CrossRef citations
0
Altmetric

Retractions

Retraction

Retraction

Page: 539

Published online: 21 Apr 2016

Citation | Full Text |

Registered in England & Wales No. 3099067
5 Howick Place | London | SW1P 1WG

Taylor & Francis Group
an **informa** business

Routledge
Taylor & Francis Group

Journal of Applied Security Research

ISSN: 1936-1610 (Print) 1936-1629 (Online) Journal homepage: http://www.tandfonline.com/loi/wasr20

Securing Cardless Automated Teller Machine Transactions Using Bimodal Authentication System

Ameh Innocent Ameh, Olayemi Mikail Olanyi & Olumide Sunday Adewale

To cite this article: Ameh Innocent Ameh, Olayemi Mikail Olanyi & Olumide Sunday Adewale (2016) Securing Cardless Automated Teller Machine Transactions Using Bimodal Authentication System, Journal of Applied Security Research, 11:4, 469-488

To link to this article: http://dx.doi.org/10.1080/19361610.2016.1211846

Published online: 08 Sep 2016.

JOURNAL OF APPLIED SECURITY RESEARCH
2016, VOL. 11, NO. 4, 469–488
http://dx.doi.org/10.1080/19361610.2016.1211846

Routledge
Taylor & Francis Group

TECHNOLOGY

Securing Cardless Automated Teller Machine Transactions Using Bimodal Authentication System

Ameh Innocent Ameh[a], Olayemi Mikail Olanyi[a], and Olumide Sunday Adewale[b]

[a]Department of Computer Engineering, Federal University of Technology, Minna Nigeria; [b]Department of Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria

ABSTRACT
In today's corporate environment, it is important to ensure that only authorized customers have access to offered services. With the availability of ready-to-use sniffers and access code hacking tools, the standard card and Personal Identification Number combination may no longer be sufficient to withstand the test of secure authentication. Additionally, the huge and recurrent card possession and repossession cost incurred by banks' customers, occasioned by card expiry, loss, theft, and damage is, agreeably, undesirable. In this article, we present the development of a bimodal customer authentication system for a cardless Automated Teller Machine (ATM). The system employs the principle of eigenvectors and Euclidean distance for fingerprint verification. The Personal Identification Number (PIN), which serves as the second factor of authentication, is determined on account opening and hashed using the truncated SHA 512/256 Secure Hashing Algorithm. Analysis of the system performance shows genuine acceptance rates (1-FRR) from 98% and upwards, and equal error rates of 0.0065. A low standard deviation of 0.01 of the Average Matching Times (AMT) shows the consistency of the algorithm in processing the fingerprints. Therefore, the performance evaluation of the system using these metrics portrays the adequacy and suitability of the developed system for ATM user authentication.

KEYWORDS
Cardless; fingerprint; customer; authentication; security; ATM

Introduction

An Automated Teller Machine (ATM) is a computerized telecommunication device which provides clients of banks access to financial services at places not limited to the premises of a bank without the human intervention of a bank teller (Adelowo & Mohammed, 2010). On most modern ATMs, customers are identified by the insertion of plastic cards with magnetic stripe or chip that contains a unique number and other security information like date of expiration, and card verification value. Authentication is achieved by the input of a valid Personal Identification

CONTACT Ameh Innocent Ameh ✉ ameh247@gmail.com 🖃 Department of Computer Engineering, Federal University of Technology, Minna, Nigeria.

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/wasr.

Number (PIN) by the customer. Through the ATM, access is granted customers to perform such transactions as cash deposits and withdrawals, cash advances through credit cards, account balance inquiries, as well as purchase prepaid cell phone credit (Khalifa & Kamarudin, 2013).

With the rising incidences of crimes around the ATM according to the Nigerian Deposit Insurance Corporation (NDIC), the need for a more robust user authentication system cannot be overemphasized (Ameh, 2015). This is occasioned, in part, by the activities of fraudsters, and the carelessness of ATM users, who vary in their levels of sophistication and literacy respectively. Password compromise and discovery have contributed immensely to the absence of secure authentication on ATMs. Many customers use guessable combinations, compromise their PIN, make infrequent changes, and often make notes of their PINs and passwords in discoverable places. It is fast becoming acceptable that the card and PIN authentication may no longer be adequate to serve the growing high-risk e-business marketplace from a security point of view. Authentication, however, cannot exist on its own, but must be part of a security system design framework. The purpose of system design is to create a technical solution that satisfies the functional requirements for the security system. The functional specification produced during system requirements analysis is transformed into a physical architecture through system modelling and database design (Olaniyi Arulogun, Omidiora, & Adeoye, 2013a). The four security control objectives that address an adequate security framework in the context of ATM are (Brent, 2004):

1. Authentication–This control objective is responsible for proving the identity of the ATM service requester prior to granting access to the available services. With a weak process of authentication, the safety and security of banks' customers' money stands highly jeopardized, with imaginable financial loss to both the banks and her customers, and irrecoverable reputational damage to the banks.
2. Data integrity–This security control objective ensures that data has the same value, irrespective of the direction, or perspective from which it is being accessed. It ensures that credential and financial data were modified by the authorized people, and that no unauthorized changes have been made.
3. Confidentiality–This security objective restricts data access only to the people authorized to see it. In ATM banking, the confidentiality of access codes is not guaranteed under the traditional method of card and PIN due to the availability of sniffers, skimmers, key loggers, PIN guess ability, and hackers.
4. Nonrepudiation–This security control objective ensures that a user may not deny financial transactions. When the confidentiality of a card PIN is compromised, the actual beneficiary of a transaction is brought to doubt. With biometric authentication, the issue of nonrepudiation ceases to bedevil ATM transactions significantly.

This research was motivated by the following factors:

- The proven vulnerabilities of the existing ATM system,

- The startling fraud figures chiefly aided by the complementary usage of the card and PIN in Nigeria (NDIC, 2012), and
- The extortionate cost of card holding.

The proposed technique would be profitable to both banks and customers in the areas of security, and eradication of the recurrent cost of card acquisition and maintenance; hence the provision of a secure e-business model for improved customer service, retention, and by extension, revenue generation.

The problem of ATM fraud is global in nature and its consequences on bank patronage should be of concern to the stakeholders in banks, information technology, and computer security practitioners. Card theft, PIN theft and cracking, all contribute to fraud schemes. According to an NDIC report in 2015, deposit money banks reported 10,612 fraud cases involving the sum of $80.43m (₦25.61bn) with expected/contingent loss of about $19.44m (₦6.19bn) in 2014. The expected/contingent loss had increased by $1.37m (₦436m) (7.57%) over $18.1m (₦5.76bn) reported in 2013. NDIC traced the increase in fraud cases partly to a rise in the usage of ATMs for financial transactions (NDIC, 2015). In the first quarter of 2011 alone, of the 842 cases of reported frauds among 24 Nigerian banks, 523 cases were ATM related, representing a 62.11% rise against the previous quarter of October to December 2010. This involved a whopping $350,310.18 (₦111,549,270.88), a 6.79% increase against the previous quarter (Ameh, 2015).

In addition to the incidences of frauds due to the insecurity of the card and PIN combination, the huge and recurrent card possession and repossession costs incurred by banks' customers, occasioned by card expiry, loss, theft, and damage, is agreeably undesirable. These startling figures in NDIC 2015 annual report, partly resulting from the ATM and its usage is a huge indictment on the formidability of the system's security. Additionally, the extortionate cost of card holding as well as the possibility of card duplication and cloning, have made the complete replacement of the card system ATM transactions imperative. The existing ATM authentication system has the following drawbacks: The unauthorized possession of an ATM card and its PIN automatically transfers account ownership to the fraudster/impostor to a very large extent, who may proceed with card usage without further verification. This gives room for severe security issues.

In this work, a secure fingerprint authentication model for a cardless ATM using Principal Component Analysis (PCA), with a PIN as a second factor of authentication was developed, and a prototype for the model was implemented. The performance of the developed model was also evaluated using such performance metrics as False Rejection Rate (FRR), False Acceptance Rate (FAR), and Average Matching Time (AMT).

Related works

Since security measures at ATM centers play a critical and contributory role in preventing attacks on customers, several authors have used biometrics in a similar research context to shift from PIN to biometric based security. In Jain, Prabhakar, and Chen (1999), the logistic transform was used to integrate the output scores from Hough transform, String distance, and dynamic programming based matching algorithms. Both algorithms are minutia-based and make use of dynamic programming to deal with elastic distortion. The integration of the three algorithms involved solving a minimization problem with more number of parameters but resulted in performance issues, like high FRR resulting from distorted fingerprints.

A smartcard based encryption/authentication scheme for ATM banking system was proposed by Fengling, Jiankun, Xinhuo, Yong, and Jie (2005). The first layer of the scheme was 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. The major shortfall of this work was that it failed to address the issue of smartcard's susceptibility to theft, cloning, and retraction. Das and Jhunu (2011) and Yun and Jia (2010) proposition focused on vulnerabilities and the increasing wave of criminal activities occurring at ATMs. A prototype fingerprint authentication for enhancing ATM security was presented. The system adopted the same measure as this current work by formulating modules for fingerprint enrollment, feature extraction, database and matching. A major difference is that the direct gray scale method of feature extraction, known for higher accuracy, was adopted in this work because the direct gray scale methods mitigates the loss of minutiae information.

A network security framework for real time ATM application using a combination of PIN, thumb scanning, and face recognition to foster security was proposed by Mali, Salunke, Mane, and Khatavkar (2012). 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 patterns before access is granted for ATM operations. The integrated system uses PCA and Eigen algorithm for face recognition, Least Significant Bit algorithm for steganography, and Advanced Encryption Standard algorithm for cryptography. Though the framework looks promising, its practicality is not supported by detailed implementation and evaluation. Additionally, the three modes of authentication, two of which are biometric, make the system expensive. The system also gave rise to too many parameters to handle.

In Awotunde, Jimoh, and Matiluko (2015), a convenient cost effective bimodal system using fingerprint and a short-code message to authenticate account holders transaction was proposed. The system relied on the erratic nature of short messaging platforms. Besides not being a reliable means of real-time communication, short messaging service may not be available to every possible user of the proposed system. This work used the truncated SHA 512/256 hash algorithm to retrieve PINs in the bimodal authentication system as a second factor of authentication. In furtherance to Awotunde and colleagues' (2015) recommendation for the development of a dual biometrics authentication system, and the complete eradication of the PIN and Card combination, this work developed a cardless ATM system. However, the dual biometrics system was not employed for reasons of cost, convenience, as well as acceptability, being a new introduction and integration into the existing ATM banking ecosystem in sub-Sahara Africa.

Alebiosu, Yekini, Adebari, and Oloyede (2015) designed a cardless electronic ATM with biometric authentication. Although the work addressed the problem of card theft, cloning, loss, single factor authentication, and employed fingerprint biometric authentication technique, the work lacks lucid design and detailed development consideration for possible adoption, hence the performance of the proposed system could not be evaluated. Additionally, not all transactions on the ATM are bimodally authenticated, and the PIN, though alphanumeric, was not secured by any known or nouvelle cryptographic algorithm to mitigate the incidences of fraud. Also, authors in Alebiosu and colleagues (2015) do not provide any mathematical proof of concept to substantiate the design, and the period per biometric authentication of a single user is undoubtedly very high as three out of five different fingerprints would have to pass verification.

In this article, improvements were made on these baselines related works by developing a secure fingerprint and PIN-based bimodal authentication. PINs were secured using the truncated SHA 512/256 hash algorithm, which provided encryption as well as allowed for fast retrieval of the PINs from their secure hash table abodes. Minutiae features were extracted using Principal Component Analysis with negligible or no loss of minutiae information. Fingerprint module for obtaining live scans of fingerprint was developed and integrated with existing ATM system using affordable and easily available materials. Evaluation of system performance was also carried out to authenticate the sufficiency of the employed algorithms and embedded system design methodology to replace the existing and proposed methods in the works of previous authors.

Materials & methods

Determination of fingerprints Eigenvectors and Eigenvalues

Suppose a fingerprint image consists of N pixels, so it can be represented by a vector Γ of dimension N. Let $\{\Gamma_i | i = 1, \ldots, M\}$ be the training set of fingerprint images. The average fingerprint of these M images is given by

$$\Psi = \frac{1}{\mathrm{M}} \sum_{i=1}^{\mathrm{M}} \Gamma \mathrm{i} \tag{1}$$

Then each fingerprint Γ_{i} differs from the average fingerprint Ψ by Φ_{i}:

$$\Phi_{\mathrm{i}} = \Gamma_{\mathrm{i}} - \Psi; \mathrm{i} = 1, \ldots, \mathrm{M} \tag{2}$$

A covariance matrix of the training images can be constructed as follows:

$$C = AA^T \tag{3}$$

Where $A = [\Phi_1, \ldots, \Phi_M]$. The basis vectors of the fingerprint space, that is, the Eigen fingerprints, are then the orthogonal Eigenvectors of the covariance matrix C.

Finding the Eigenvectors of the N by N matrix C is an intractable task for typical image sizes, hence, a simplified way of calculation is adopted. Since the number of training images is usually less than the number of pixels in an image, there will be only M−1, instead of N, meaningful Eigenvectors (Nikola, Slobodan, & Benjamin, 2007). Therefore, the Eigen fingerprints are computed by first finding the eigenvectors, v_l $(l = 1, M)$, of the M × M matrix L:

$$L = A^T A \tag{4}$$

The Eigenvectors, u_l $(l = 1, \ldots, M)$, of the matrix C are then expressed by a linear combination of the different fingerprint images, Φ_i $(i = 1, \ldots, M)$, weighted by

$$v_l\ (l = 1, \ldots, M) : U = [u_1, , u_M] = [\Phi_i, \ldots, \Phi_M]\,[v_i, , v_M] = A.V \tag{5}$$

In practice, a smaller set of M' (M' < M) Eigen fingerprints is sufficient for fingerprint matching. Hence, only M' significant Eigenvectors of L, corresponding to the largest M' Eigenvalue, are selected for the Eigen fingerprint computation, thus resulting in a further data compression. M' is determined by a threshold, θ_λ, of the ratio of the Eigenvalue summation (Turk & Pentland, 1999).

$$M\prime = \min_r \left\{ r \middle| \frac{\sum_{I=1}^{r} \lambda_I}{\sum_{I=1}^{M} \lambda_I} > \theta_\lambda \right\}. \tag{6}$$

Fingerprint matching using Eigen fingerprints

The Eigen fingerprint-based fingerprint matching procedure is composed of two stages: a training stage and a matching stage.

In the training stage, the fingerprint of each known individual, Γ_k, is projected into the fingerprint space and an M'-dimensional vector, Ω_k, is obtained:

$$\Omega_k = U^T (\Gamma_k - \Psi)\,; k = 1, \ldots, N_c, \tag{7}$$

Where N_c is the number of fingerprint classes.

A distance threshold, θ_c, that defines the maximum allowable distance from a fingerprint class as well as from the fingerprint space, is set up by computing half the largest distance between any two fingerprint classes:

$$\theta_c = \frac{1}{2}\max_{j,k}\left\{\left\|\Omega_j - \Omega_k\right\|;j,k = 1,\ \ldots N_c\right\} \tag{8}$$

In the matching stage, a new image, Γ, is projected into the fingerprint space to obtain a vector, Ω:

$$\Omega = U^T\Gamma - \Psi \tag{9}$$

The distance of Ω to each fingerprint class is defined by

$$\varepsilon_k^2 = \left\|\Omega - \Omega_{\mathrm{k}}{}^2\right\|;k = \mathit{1},\ \ \ldots,\ \ N_c \tag{10}$$

When the fingerprint image to be matched (known or unknown), is projected on this fingerprint space, the weights associated with the Eigen fingerprints, that linearly approximate the fingerprint or can be used to reconstruct the fingerprint obtained. Now these weights are compared with the weights of the known fingerprint images so that it can be recognized as a known fingerprint used in the training set. In simpler words, the Euclidean distance between the image projection and known projections is calculated; the fingerprint image is then classified as one of the fingerprints with minimum Euclidean distance.

For the purpose of discriminating between fingerprint images and nonfingerprint-like images, the distance, ε, between the original image, Γ, and its reconstructed image from the Eigen fingerprint space, Γ_f, is also computed:

$$\varepsilon^2 = \|\Gamma - \Gamma_{\mathrm{f}}\|^2, \tag{11}$$

Where:

$$\Gamma_f = U.\Omega + \Psi \tag{12}$$

These distances are compared with the threshold given in equation (6) and the input image is classified by the following rules (Turk & Pentland, 1999):

$$\mathrm{IF}\,\varepsilon \geq \theta_{\mathrm{c}},\quad \mathrm{THEN}$$

Input image is not a fingerprint image;

$$\mathrm{IF}\,\varepsilon < \theta_{\mathrm{c}}\,\mathrm{AND}\ \ \varepsilon_{k^*} \geq \theta_c\quad \mathrm{THEN}$$

Input image contains an unknown fingerprint;

$$\mathrm{IF}\,\varepsilon < \theta_{\mathrm{c}}\ \mathrm{AND}\ \ \varepsilon_{k^*} = \min_k\{\varepsilon_k\} < \theta_c\,\mathrm{THEN}$$

Input image contains the fingerprint of the customer k^*.

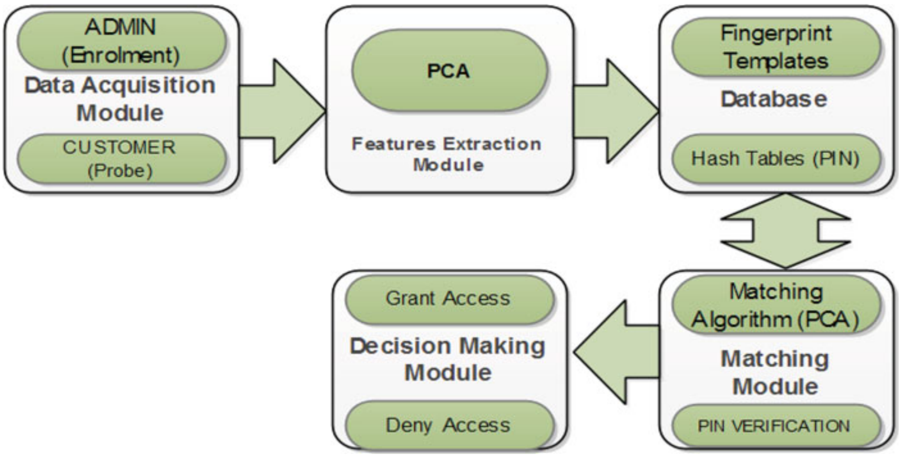

Figure 1. System architecture of the bimodal authentication system (PCA = Principal component analysis; PIN = Personal identification number).

The research design

The bimodal authentication for a cardless ATM System consists of five basic modules: the data acquisition module, the features extraction module, the database, the matching module, and the decision-making module. The architecture of the system is shown in Figure 1.

User enrollment at the bank takes place during account opening, and fingerprint image acquisition both occur in the data acquisition module. The minutiae features are extracted in the feature extraction module by the feature extraction algorithm before storage in the fingerprint database. The predetermined PIN at account opening is also hashed and stored in a separate database. The fingerprint matching algorithm and the PIN verification algorithm both make up the matching module, while the decision-making module grants or denies access to ATM transactions. These modules are described as follows:

The data acquisition module

As shown in Figure 1, the data acquisition module consists of two (2) subunits: The enrollment (Bank Administrator) subunit, and the probe (customer) subunit.

Enrollment (bank administrator) subunit

At enrollment (during account opening), the fingerprints constituting the training set were obtained via the fingerprint sensor under similar lighting conditions. They were also resampled to the same pixel resolution. Using the theory of PCA algorithms:

1. Select a fingerprint image of N pixels from a training set of M images represented by a vector Γ of dimension N.

2. Resample all fingerprints to the same resolution.
3. Calculate the average fingerprint of these M images.
4. Calculate the difference, $\Phi_{i,}$ of each fingerprint Γ_i from the average fingerprint Ψ.
5. Construct a covariance matrix C of the training images.
6. Compute the Eigenvectors.
7. Express the Eigenvectors of the matrix *C* as a linear combination of the different fingerprint images.
8. Compute a set of Eigen fingerprints.

Customer authentication subunit

This begins when a customer approaches the ATM to make a transaction. The customer places the thumb on the sensor, which captures a probe and compares it with the templates in the database.

The database module

This module contains all the biometric and nonbiometric data obtained from the customer at account opening. It is subdivided into two parts:

The fingerprint database

This contains the biometric templates, (I_k, v_k) where I_k is the customer's name—and v_k is the fingerprint signature associated with I_k of known people who are enrolled into the system. The database is centralized for more efficiency and for the avoidance of counterfeiting and duplication. The templates were classified so as to reduce the computational overhead of pattern matching. For example, for a male customer, his probe is not checked against female's templates.

Hash functions for PINs

During account opening, a PIN is registered, and it forms the basis for the second level of authentication. These numerical values are stored in hash tables, where a hash function is implemented, to map keys to the integers (PINs) to obtain an even distribution on a smaller set of values. The hashing scheme considered for this design was the truncation of SHA-512 operation with 256 bit in SHA-512/256. This is meant to balance the cost of providing the necessary additional security/storage against the performance cost of calculating the hash. The hybridized combination of SHA-512/256 (truncation) to the SHA portfolio avails the implementation with performance and cost advantages.

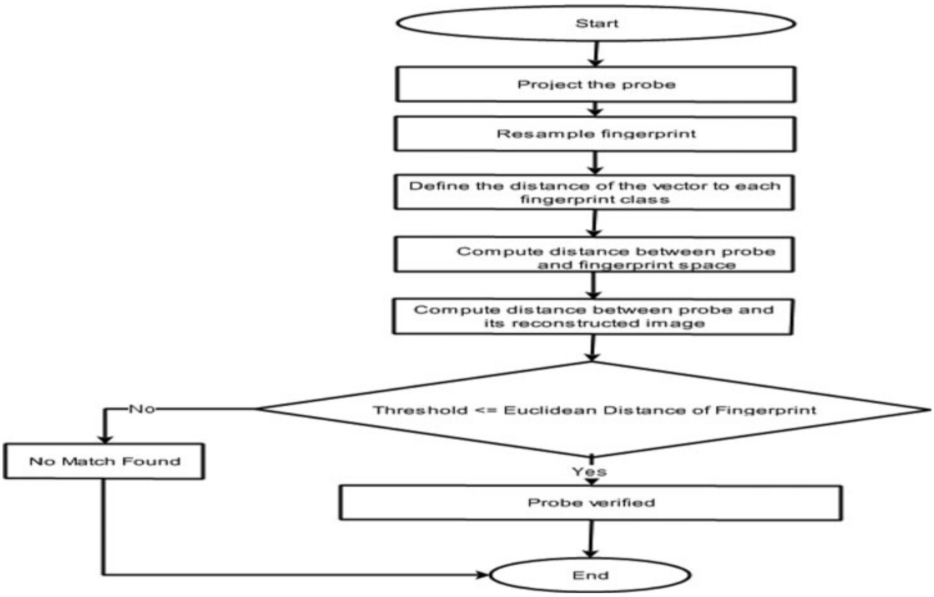
Start
Project the probe
Resample fingerprint
Define the distance of the vector to each fingerprint class
Compute distance between probe and fingerprint space
Compute distance between probe and its reconstructed image
Threshold <= Euclidean Distance of Fingerprint
No
No Match Found
Yes
Probe verified
End

Figure 2. Flowchart for fingerprint authentication.

The fingerprint matching algorithm

Fingerprint matching was achieved through the use of the following algorithm to match the probe with the template (using Euclidean distance defined in section 4.2). The algorithm is as follows:

1. Project a new image, $\mathbf{\Gamma}$, into the fingerprint space to obtain a vector, $\mathbf{\Omega}$.
2. Resample resolution.
3. Define the distance of the vector $\mathbf{\Omega}$ to each fingerprint class.
4. Compute the Euclidean distance, $\boldsymbol{\varepsilon}$, between the probe, $\mathbf{\Gamma}$, and the fingerprint space.
5. Compute distance, $\boldsymbol{\varepsilon}$, between Γ and its reconstructed image $\mathbf{\Gamma}_f$ from the Eigen image space.
6. Compare $\boldsymbol{\varepsilon}$ with the threshold given in equation (8) and classify image as known, unknown, or not a fingerprint.

Figure 2 is the flowchart for the fingerprint authentication process.

System hardware and software development considerations

The system hardware and software prototype comprises of fingerprint sensor, Arduino Uno development board and the banking application software. The fingerprint biometric integration was used as a means of heightening the security in ATM banking. The fingerprint sensor captures an image of the customer's fingerprint and sends a signal to the ATmega328 microcontroller chip on the Arduino board. The digitized image is compared with stored templates in the database via the matching algorithm. A decision to either grant or deny access is sent to the banking application system, which then sends a PIN request to the user for the second and final

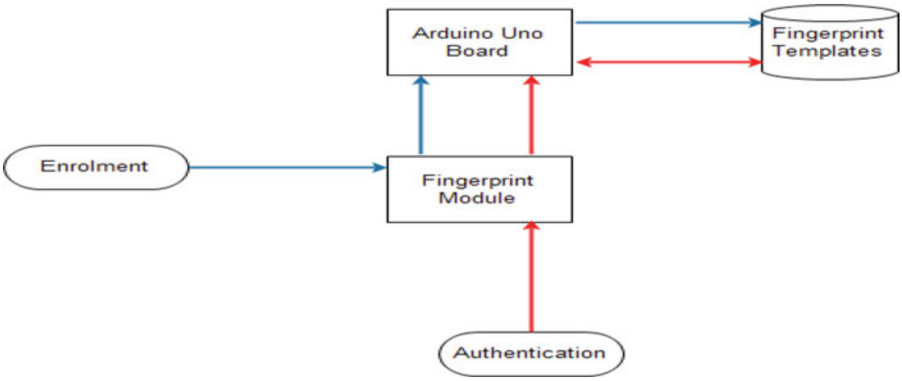

Figure 3. Block diagram of the fingerprint authentication module.

level authentication. Figures 3 and 4A and B respectively show the block diagram, the skeletal, and the compact coupling of the developed fingerprint authentication module.

Hardware design considerations

In this section, the power supply, the microcontroller, and the sensory units alongside their integration for the successful implementation of the biometric authentication subsystem are described.

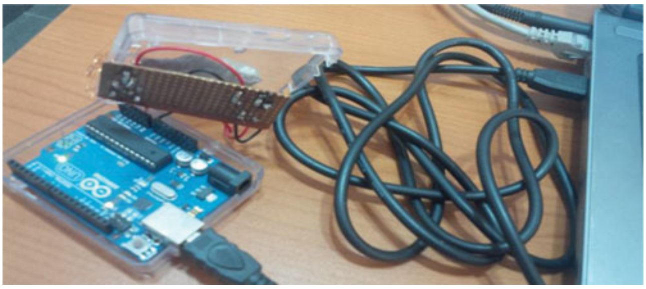

Figure 4A. Skeletal coupling of the fingerprint authentication module.

Figure 4B. Compact coupling of the fingerprint authentication module.

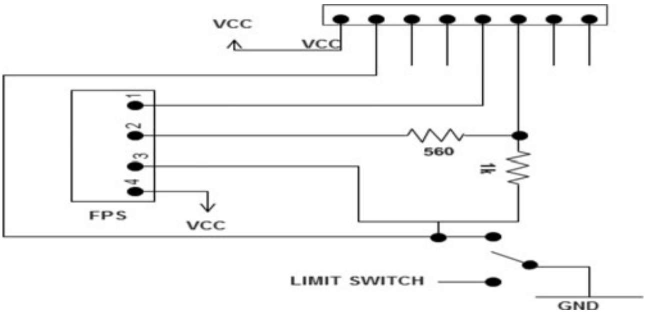

Figure 5. Step-down circuit for power supply.

The power supply unit design consideration

In view of the fact that the biometric authentication subsystem is an add-on technology (to the already existing ATM system), the power supply to the Arduino is through a Universal Serial Bus (USB) connector. The microcontroller board is rated 5V (DC), which necessarily has to be regulated to meet the power requirement of the ATmega328 chip with a rating of 3.3V and that of the fingerprint sensor rated 3.2V. The input voltage from the PC was reduced to meet the Arduino board rating by implementing the Voltage Divider Rule (VDR) theorem through the linear voltage regulator circuit.

From the VDR Theorem:

$$V_{out} = \frac{R_2}{R_1 + R_2} V_{in} \tag{13}$$

Where $\mathrm{V_{in} = 5v, R_1 = 1k\Omega, R_2 = 560\Omega}$
Therefore,

$$\mathrm{V_{out} = 3.2v}$$

Figure 5 is the power supply step-down circuit for the system.

Embedded system unit design consideration

This unit was designed around ATmega328 Microcontroller chip. The chip (embedded in Arduino board in Figure 6) has 14 digital input/output pins, out of which

Figure 6. The Arduino Uno Board (Adapted from "Embedded system design with Arduino, 8051MCU and PIC16887F: A laboratory manual" by O. M. Olaniyi, F. Sado, O. Rabiu, C. Inalegwu, & D. Maliki, 2013b, Department of Computer Engineering, Federal University of Technology, Minna, Niger State).

Figure 7. Rear & Perspective view of the GT511C3 Fingerprint Sensor (Adapted from "GT-511C3 Fingerprint scanner hardware, wiring and connector numbering" by Starting Electronics, 2014. Retrieved from https://startingelectronics.org/articles/GT-511C3-fingerprint-scanner-hardware/).

six are usable as Pulse Width Modulation outputs, 6 analogue inputs, a 16 MHZ ceramic resonator, an USB connector, a power jack, an In-Circuit Serial Programming header, and a reset button.

The fingerprint sensory unit

The fingerprint sensory unit was modelled after the GT511C3 fingerprint module shown in Figure 7. ADH Tech designed it for Serial-Transistor-Transistor Logic interconnection. Images of customers' fingerprints were captured on an on-board 32bit Central Processing Unit plus an optical sensor which identifies it. ATM users' fingerprints send analogous commands by impressing the thumb on the platen. The in-built JST-SH connector is connected to the Arduino board through its FTDI breakout with the use of a pigtail connector. Figure 9 shows the rear and perspective view of the GT511C3 Fingerprint sensor.

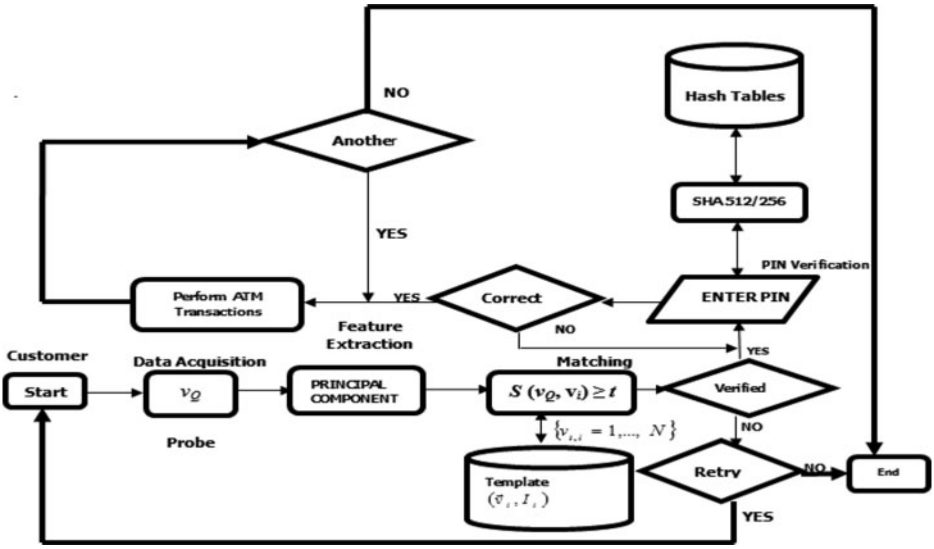

Figure 8. Data flow diagram for the bimodal authentication system (ATM = automated teller machine; PIN = personal identification number).

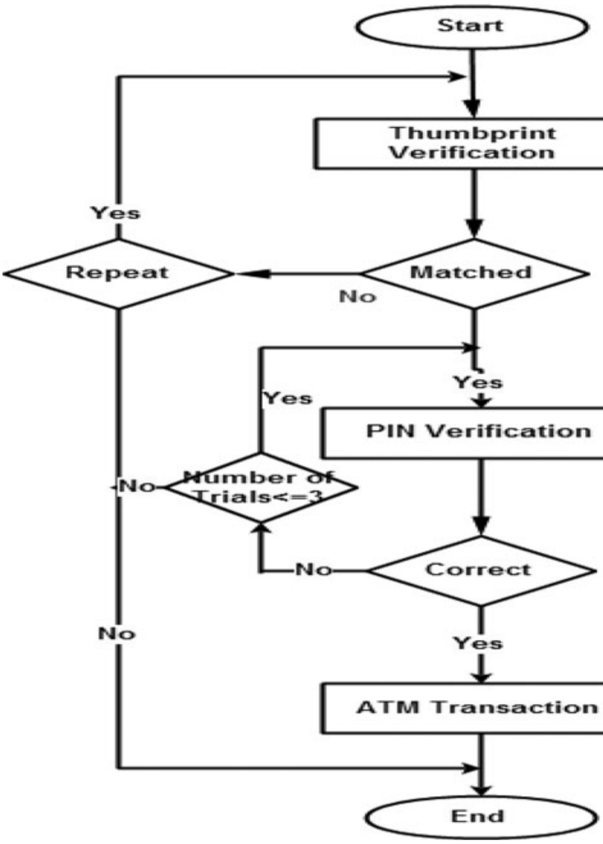

Figure 9. System flowchart for the bimodal authentication system (PIN = personal identification number; ATM = automated teller machine).

Software design considerations

With a view to establishing the correctness of the design, each component was implemented and tested. All program codes were implemented using PHP and Java programming language. Also employed during the implementation phase is the Microsoft SQL Server 2008 R2, which is a relational database suitable for integrating .net technology for backed data management system. Figures 8 and 9 respectively show the System Data Flow diagram, and the flowchart.

Experimental procedures

The evaluation of the ATM Fingerprint verification system was carried out with data obtained from randomly selected 50 customers of the First Bank of Nigeria, Minna Branch. The analysis of the data obtained from the users revealed that 36 of them were male while 14 were female.

The age distributions of the 50 customers are as shown in Table 1.

Two data groups of thumbprints were formulated, with the first data group (Data group A) containing 200 thumbprints consisting of four thumbprints obtained from

Table 1. Age distribution of surveyed customers.

No. of Customers	4	10	15	9	7	5
Age distribution	0–19	20–29	30–39	40–49	50–59	> = 60

Note. Data in Table 2 shows that 4 of the customers have been using ATM for about 8 years, while 8, 12, 7, 5, 10, 3, and 1 of them have 7, 6, 5, 4, 3, 2 and 1 year(s) ATM usage experiences respectively. Source: Fieldwork: (Ameh, 2015).

Table 2. Years of ATM usage experience of surveyed customers.

No. of Customers	1	3	10	5	7	12	8	4
Years of ATM usage experience	1	2	3	4	5	6	7	8

Source: Fieldwork: (Ameh, 2015).

the right thumb of each customer. The second data group (Data group B) is of the same size but consists of four thumbprints collected from the left thumb of each customer. All the thumbprints were enrolled over a period of 4 months with image size 202 × 258 pixels and resolution 450 dots per inch.

Failure to enroll error was encountered during the enrollment. The error arose from moisture effect on the platen of the fingerprint sensor, prolonged usage as well as hard thumbs. The moisture effect is resolved by resetting the sensor and making fresh enrollment attempt. Roughness of the thumb is handled by robbing it with lotion. The lotion was then carefully wiped off when the thumb was found to have improved or softened enough.

FRR and FAR tests were carried out on both data groups in Divisions A and B. The FRR test was conducted by matching each thumbprint with the other three thumbprints from the same thumb using the implemented fingerprint matching algorithm at various thresholds (matching scores).The FAR test was done through matching four thumbprints of one of the thumbs in the data group with the 196 thumbprints from the other 49 thumbs, also at varying thresholds. The time taken for a complete matching cycle was also randomly noted for some of the tests.

Results and discussion

Division a experimental results

From the FRR tests conducted on Data group A, results in Table 3 were obtained. The FAR tests on the same data group also yielded results as shown in Table 4.

Table 3. FRR test on data group A.

Threshold (%)	Matching Attempts (N)	False Rejects (nR)	FRR = ($\frac{nR}{N}$)	FRR = ($\frac{nR}{N}$.) (%)	Genuine Acceptance (1-FRR) (%)
1.000	600	7	0.012	1.167	98.833
0.750	600	5	0.008	0.833	99.167
0.500	600	2	0.003	0.333	99.667
0.250	600	0	0.000	0.000	100.000

Note. FRR = False Rejection Rate. Source: Laboratory Experiment: (Ameh, 2015).

Table 4. FAR test on data group A.

Threshold (%)	Matching Attempts (N)	False Acceptance (nA)	FAR $= (\frac{nA}{N}.$	FAR $= (\frac{nA}{N}.)$ (%)
1.000	784	0	0.000	0.000
0.750	784	4	0.005	0.510
0.500	784	6	0.008	0.765
0.250	784	8	0.010	1.020

Note. FAR = False Acceptance Rate. Source: Laboratory Experiment: (Ameh, 2015).

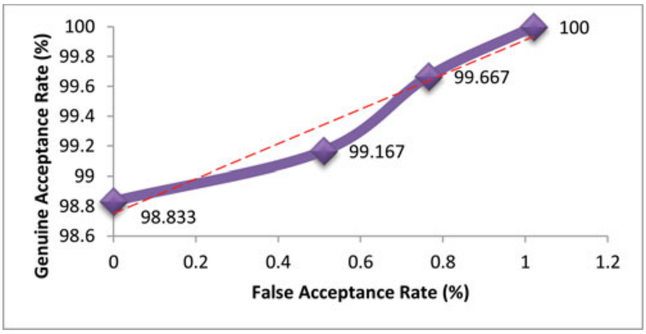

Figure 10. ROC curve for division a experiments (ROC = receiver operating characteristic).

Figure 11 shows the obtained Receiver Operating Characteristic (ROC) Curve for the results in Table 2. An ROC curve depicts the plot of genuine acceptance rate (1-FRR) against false acceptance rate for all possible matching thresholds and measures the overall performance of the system.

Division B experimental results

For the FRR tests, the obtained results are as shown in Table 5: The FAR tests yielded the results in Table 6.

Figure 12 shows the ROC curves for Division B experiments performed on Data group B.

Inspection of Figures 10 and 11 showed similar and significant performance levels of the algorithm on both data groups. Some factors that include variation in pressure, rotation, translation, and contact area during enrollment affect the qualities of the images in the Data groups. These factors forced some pairs of images from the

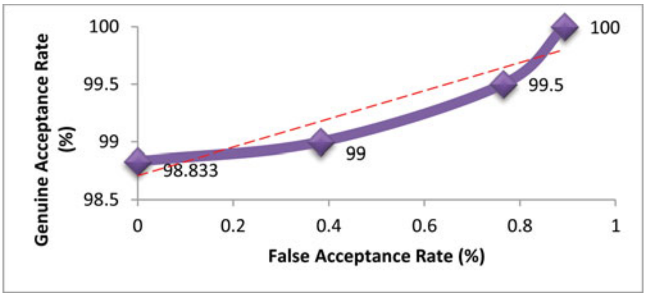

Figure 11. ROC curve for division B experiments (ROC = receiver operating characteristic).

Table 5. FRR test on data group B.

Threshold (%)	Matching Attempts (N)	False Rejects (nR)	FRR = $(\frac{nR}{N}.)$	FRR = $(\frac{nR}{N}.)$ (%)	Genuine Acceptance (1-FRR) (%)
1.000	600	7	0.012	1.167	98.833
0.750	600	6	0.010	1.000	99.000
0.500	600	3	0.005	0.500	99.500
0.250	600	0	0.000	0.000	100.000

Note. FRR = False Rejection Rate. Source: Laboratory Experiment: (Ameh, 2015).

Table 6. FAR test on data group B.

Threshold (%)	Matching Attempts (N)	False Acceptance (nA)	FAR = $(\frac{nA}{N}.)$	FAR = $(\frac{nA}{N})$ (%)
1.000	784	0	0.000	0.000
0.750	784	3	0.004	0.383
0.500	784	6	0.008	0.765
0.250	784	7	0.009	0.893

Note. FAR = False Acceptance Rate. Source: Laboratory Experiment: (Ameh, 2015).

same thumb to exhibit variations in quality, contrast, and noise levels resulting in difference in the extracted features and matching scores. The high genuine acceptance rates recorded in all cases indicate that the algorithm is suitable for implementation in the proposed fingerprint authenticated ATM system where genuine identification of individuals is paramount.

The Equal Error Rates (EER) was also generated for the experiments. EER is the best single description of the Error Rate of an algorithm and the lower its value, the lower the error rate and adequacy of the algorithm. For each matching threshold, t, EER is the value at which FAR (t) and FRR (t) are equal. Figure 13 is a plot of the FAR and FRR functions against the various thresholds.

The obtained EER (FAR = FRR) occurred at (0.613, 0.006), meaning that at a scanner sensitivity (threshold) of 0.613, there's a certainty of the same FAR and FRR of 0.006 for the algorithm. This means that about six out of every 1,000 impostors or genuine attempts would succeed (FAR) or fail (FRR). Figure 13 presents the EER graph for Division B experiments, where the EER occurred at (0.600, 0.007), implying that about seven out of 1,000 fake or real attempts would succeed or fail.

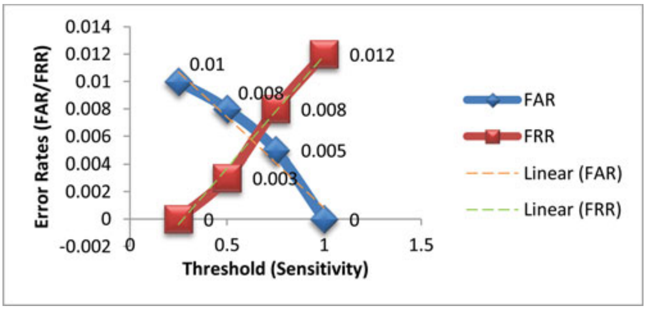

Figure 12. EER graph for division A experiments (EER = equal error rates; FAR = false acceptance rate; FRR = false rejection rate).

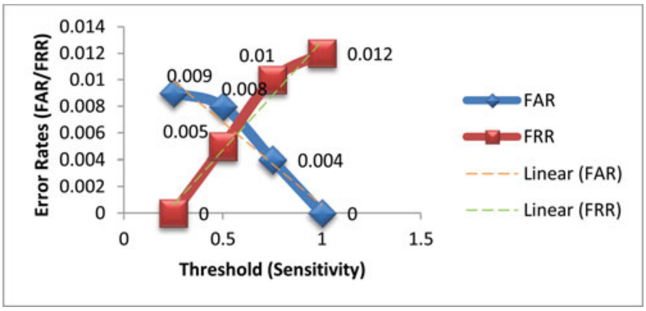

Figure 13. EER graph for division B experiments (EER = equal error rates; FAR = false acceptance rate; FRR = false rejection rate).

Table 7. Average matching time for both data groups.

Data groups	Average Matching Time (s)
Division A	1.24
Division B	1.22

Source: Laboratory Experiment: (Ameh, 2015).

Average matching time computation

The AMTs recorded for Divisions A and B experiments are shown in Table 7.

The following relationships were derived from the AMT Table 7:

$$\text{Mean} = (1.24 + 1.22)\,/2 = 1.23\text{s}$$

$$\text{Variance} = 0.0001$$

$$\text{Standard Deviation} = 0.01$$

A standard deviation as low as 0.01 confirms that the matching times are significantly close. The results portray equality and uniformity in the properties of the enrolled images in both data groups (image size, resolution, extracted features, and so forth; Iwasokun, Akinyokun, & Angaye, 2013). The relatively low AMTs obtained substantiated the fact that this system is fast enough for use for ATM authentication at minimal time.

Conclusion

This work has successfully presented a seamless combination of biometric fingerprint and PIN for the development of a formidable bimodal customer authentication system for a cardless ATM. The architecture of a bimodal authentication system for a cardless ATM was successfully developed, a prototype for the model was implemented, and an evaluation of the system performance was carried out to validate the suitability of the model to replace the existing porous ATM banking system. The obtained results prove the adequacy of the developed system in solving problems of identity theft and fraud, card holding cost, card theft, loss, swallowing, misplacement, replacement, and general mitigation of the susceptibility of the present

ATM system to manipulations and frauds. The ROC curve and the obtained EER values indicated that the proposed system proffers a veritable means of checkmating the nefarious activities of fraudsters while providing unhindered access to genuine customers.

Future research focuses are recommended in the following areas:

Start here

1. Error rate reduction and increased security through the implementation of a multi-factor biometric system, through combination of fingerprint with other biometrics such as face, for the authentication of ATM by near or remote subjects.
2. Development of the truncated SHA 512/256 Hashing Scheme over the PINs and a detailed evaluation of the performance of the hybridized algorithm.

This work has developed architecture and implemented a prototype for a bimodal customer authentication system for a cardless ATM. The results obtained proved the adequacy of the developed system in solving problems of identity theft and fraud, card theft, loss, swallowing, misplacement, replacement, and general mitigation of the susceptibility of the present ATM system to manipulations and frauds.

References

Adelowo, S. A., & Mohammed, E. A. (2010). Challenges of automated teller machine (ATM) usage and fraud occurrences in Nigeria–A case study of selected banks in Minna Metropolis. *Journal of Internet Banking and Commerce*, *15*(2), 1–5.

Alebiosu, M. I, Yekini, N. N, Adebari, F. A., & Oloyede, A. O (2015). Card-less electronic automated teller machine (EATM) with biometric authentication. *International Journal of Engineering Trends and Technology*, *30*(1), 99–105.

Ameh, A. I. (2015). Development of a bi-modal authentication system for a cardless ATM (Unpublished Masters of Engineering thesis). Federal University of Technology, Minna, Niger State, Nigeria.

Awotunde, J. B., Jimoh, R. G., & Matiluko, O. E. (2015). Secure automated teller machine using fingerprint authentication and short-code message in a cashless society. *Proceedings of the 12th International Conference of Nigeria Computer Society*, 99–110.

Brent, C. (2004). *Security versus convenience*. Global information assurance certification paper. SANS Institute. 4–5.

Das, S. S., & Jhunu, D. (2011). Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian E-Banking System. *International Journal of Information and Communication Technology Research*, *1*(5), 197–203.

Fengling, H., Jiankun, H., Xinhuo, Y., Yong, F., & Jie, Z. (2005). A novel hybrid crypto- biometric authentication scheme for ATM based banking applications. *Lecture Notes Computer Science*, *3832*, 675–681.

Iwasokun, G. B, Akinyokun, O. C., & Angaye, C. O. (2013). Fingerprint matching using neighbourhood distinctiveness. *International Journal of Computer Application*, *66*(21), 1–8.

Jain, A. K., Prabhakar, S., & Chen, S. (1999). Combining multiple matchers for a high security fingerprint verification system. *Pattern Recognition Letters*, *20*, 1371–1379.

Khalifa, S. S. M., & Kamarudin, S. (2013). The formal design model of an automatic teller machine (ATM). *Lecture Notes on Information Theory*, *1*(1), 1–3.

Mali, P., Salunke, S., Mane, R., & Khatavkar, P. (2012). Multilevel ATM security based on two factor biometrics. *International Journal of Engineering Research and Technology*, *1*(8), 1–6.

NDIC. (2015). *Source 2014 annual report and statement of accounts*. Retrieved from http://ndic.gov.ng/wp-content/uploads/2015/07/Links/NDIC%202014%

Nikola, P., Slobodan, R., & Benjamin, G. (2007). Finger-based personal authentication: A comparison of feature extraction methods based on PCA, MDF and RD-LDA. *International Conference on Computer Systems and Technologies-CompSysTech*, New York, NY.

Olaniyi, O. M, Arulogun, O. T, Omidiora, E. O., & Adeoye, O. (2013a). Design of secure electronic voting system using multifactor authentication and cryptographic hash. *International Journal of Computer and Information Technology*, *2*(6), 1122–1130.

Olaniyi, O. M., Sado, F., Rabiu, O., Inalegwu, , & Maliki, D. (2013b). *Embedded system design with Arduino, 8051MCU and PIC16887F: A laboratory manual*. Department of Computer Engineering, Federal University of Technology, Minna, Niger State. ISBN: 978-978-50862-1-8.

Starting Electronics. (2014). *GT–511C3 Fingerprint scanner hardware, wiring and connector numbering*. Retrieved from https://startingelectronics.org/articles/GT-511C3-fingerprint-scanner-hardware/

Turk, M. A, and Pentland, A. P. (1999). Face Recognition Using Eigenfaces. CVPR'91, pp. 586–591 IEEE Computer Society, 1991.

Yun, Y., and Jia, M. (2010). ATM Terminal design based on Fingerprint Recognition. *2nd International Conference of Computer Engineering and Technology*, Chengdu, People's Republic of China. 1, 92–95.