American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-9, Issue-9, pp-36-43
www.ajer.org
Research Paper Open Access

Securing Automated Teller Machine (ATM) Transaction Using Biometric Fingerprint

URANG Awajionyi S. and Ojekudo Nathaniel A.
Graduate Student, Department of Computer Science, Ignatius Ajuru University of Education, Port Harcourt, Rivers State, Nigeria.
Department of Computer Science, Ignatius Ajuru University of Education, Port Harcourt, Rivers State, Nigeria.

ABSTRACT
The current banking system is very popular with the feature of offering customers a high quality service 24 hours a day, but with a low quality security for the transaction. The traditional method of personal identification number (PIN) at the ATM has stood the test of time, mainly due to its speed and storage, but with a greater risk to customers and the bank. ATM security has often been compromised, hence the need to ensure the operation of ATM transactions using the biometric fingerprint. This research proposes to secure transactions at ATMs using a biometric fingerprint. The proposed system is an improvement of the existing system through the use of a biometric fingerprint and a BVN to secure transactions at ATMs. The proposed new system will also be profitable as it is based on the existing system.

KEYWORDS*: ATM, Fingerprint, BVN, PIN*

Date of Submission: 29-08-2020 Date of acceptance: 14-09-2020

I. INTRODUCTION

Nothing is completely certain. You can choose locks, break safes and guess your passwords online sooner or later. How can we protect the assets we value? One solution is to use biometric data, fingerprints, iris scans, retinal scans, facial scans and other personal information that is more difficult to falsify. Not long ago, if your fingerprints were taken, you are likely to be accused of a crime; Now, innocent people are turning to fingerprints to protect themselves. And you can find fingerprint scanners on anything from high security buildings to ATMs and laptops. Let's take a closer look at how they work.

A biometric system is a recognition system that allows personal identification by determining the authenticity of a particular physiological or behavioral characteristic of the user. This identification method is preferred to traditional methods that involve passwords and PINs for several reasons.

I. The person to be identified is required to be physically present at the point of identification 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. It is a measure of an individual's unique physical or behavioral

Characteristics to recognize or authenticate its identity. 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.

1.1 Statement of the Problem

A lot of criminals tamper with die ATM terminal and steal user’s credit card and password by illegal means. Customer are even kidnapped at gun point, and force to reveal the PIN of their bank credit card, some are held for days, until they have completely empty the account of victim. The frequency of frauds and criminal activities on ATM machine is on the increase and urgent steps needed to taking to stop the crime. The use of biometric fingerprint on ATM machine will secure ATM transaction and reduce the criminal activities on ATM machine to almost zero percent.

1.3 Motivation of the Study

Securing ATM transaction using biometric fingerprint is a biometric technique that uses the unique patterns on a person’s fingerprint to be able to access ATM. This process is done by identification and verification of the person.

This solution for bank security is beyond traditional business security. The solution offer help that will improve security ATM transaction for customers using ATM machine in Nigeria and the world at large.

** Securing a transaction at an ATM using a biometric fingerprint is a biometric technique that uses a person's unique fingerprint patterns to access the ATM. This process is done by identifying and verifying the person.

This solution for bank security goes beyond the traditional security of companies. The solution provides help that will improve the security of ATM transactions for customers using ATMs in Nigeria and around the world.

1.4 Aim and Objectives of the Study

The aim of this study is to develop a secured system that will be used in securing ATM transaction using biometric fingerprint. The objectives include the following:

i. To propose a secured system for ATM transaction using biometric finger print only.
ii. To compare the security level of the system with other system.
iii. To propose and replace the use of PIN and Bank credit card.

1.5 Significance of the Study

Fingerprints have been used as the most popular* biometric authentication, identification and verification because of their high acceptability and uniqueness. For securing ATM transaction, fingerprint has been proven to be more secure and is preferred to over the traditional methods involving the passwords and PIN numbers for various reasons

The person to be identified is required to be physically present at the point of identification. Finally, identification based on biometric fingerprints eliminates the need to remember a password or PIN numbers.

1.6 Scope and Limitation of the Study

One of the advantages of digital printing technology is precision. Identical matches are almost impossible because fingerprints contain a large amount of information, so it is unlikely that two fingerprints are identical. Another advantage of fingerprint technology is that the memory size required to store the biometric model is relatively small. Finger analysis has some weaknesses, most of which can be mitigated. There is a fraction of the population in the world that cannot register. Another limitation is that over time, sometimes in just a few months, the characteristics of an individual's fingerprints may change, making identification and verification difficult. This problem concerns manual workers who work hard with their hands. There are also privacy issues related to finger scanning technologies. Some fear that finger scanning can be used to track a person's activities. Others fear that the data collected may be used inappropriately for medical-legal purposes.

Fingerprint

Detail of fingerprint recognition process.

A fingerprint recognition system is done using three steps known as Image
acquisition, Minutiae extraction and Minutiae matching. The block diagram of basic fingerprint recognition system is shown in fig 1 below.

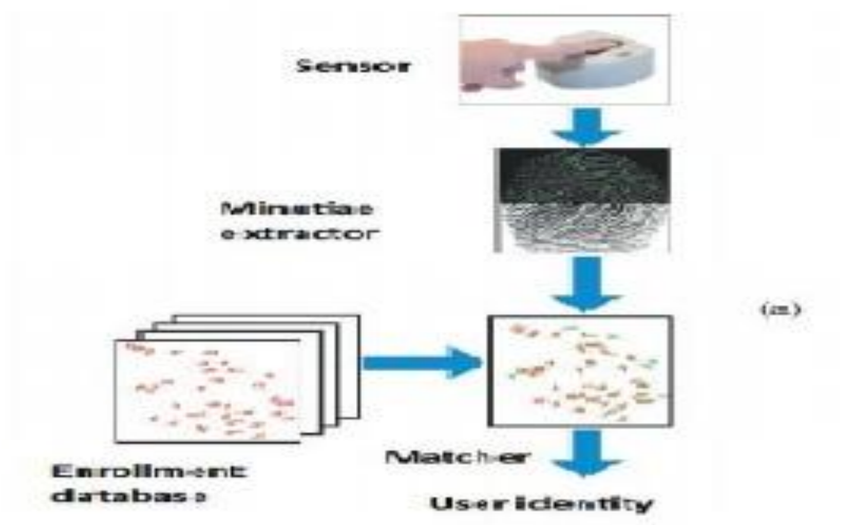

Figure 1.1: A typical automated fingerprint recognition system (Okokpujie K. et al, 2016)

The first step was the acquisition of fingerprint image by above device mentioned in the algorithm, and the results could be sent to the following process. Secondly, pre-processing the images acquired. After obtain the fingerprint image, it must be pre-processing. Generally, pre-processing of one's is filtering, histogram computing, image enhancement and image linearization. Lastly, the characteristic value was extracted, and the results of the above measures would be compared with the Information of owner's fingerprint in the database so as to verify whether the character is matched, and then the system returned the results matched or not Fingerprints are one of those bizarre twists of nature. Human beings happen to have built-in, easily accessible identity cards. You have a unique design, which represents you alone, literally at your fingertips, fingerprints are a unique marker for a person, even an identical twin. Fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity. This part touches on two major classes of algorithms and four sensor designs (optical, ultrasonic, passive capacitance, and active capacitance) The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

The three basic patterns of fingerprint ridges are the arch, loop, and whorl:

i. **Arch**: The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
ii. **Loop**: The ridges enter from one side of a finger, form a curve, and then exit on that same side.
iii. **Whorl**: Ridges form circularly around a central point on the finger.

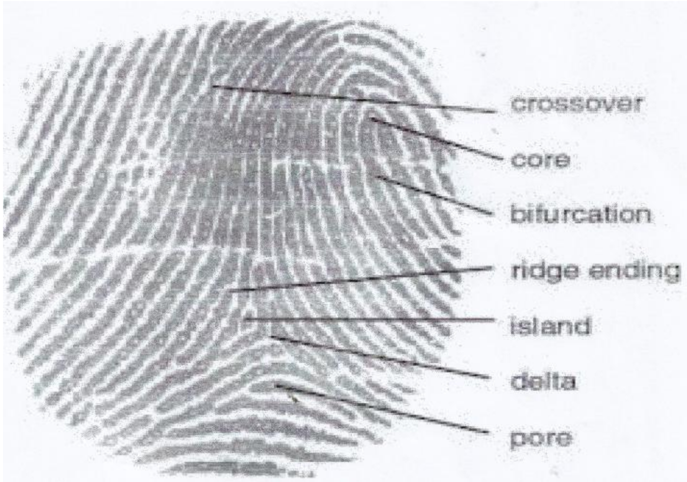

Figure 1.2 Local features of fingerprint pattern by Wang et'al (2010)

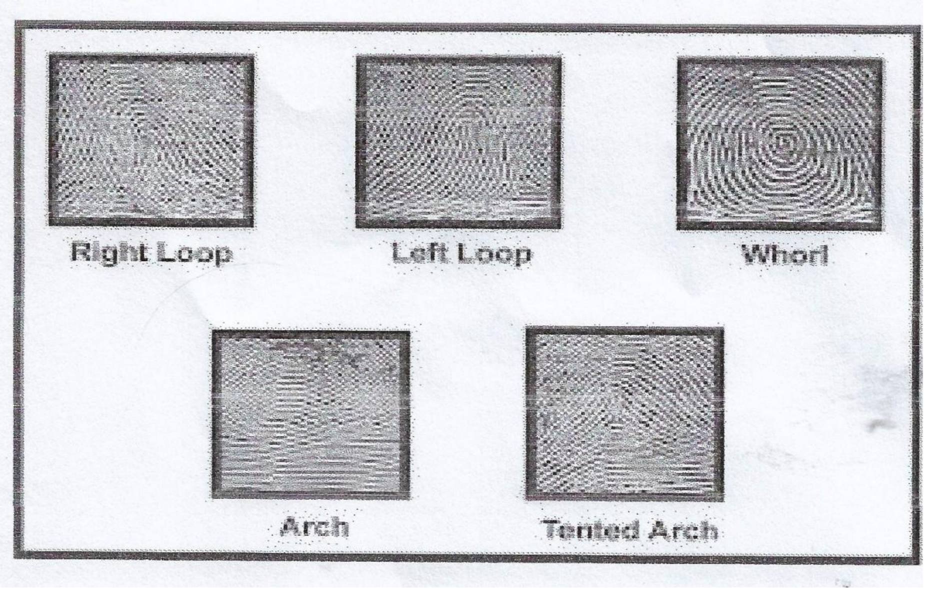

Figure 1.3: The Classes of ridges patterns in global features of fingerprint by Monowar et' al (2009)

2.1 Advantages and Disadvantages of Biometric Technologies.

Table 2.1 compares some of the biometric systems used lately, from the point of view of accuracy, cost, and devices required and social acceptability by Levent Arslan (2016).

Biometric Technologies	Accuracy	Cost	Device required	Social acceptability
DNA	High	High	Test Required	Low
Iris recognition	High	High	Camera	Medium-low
Retinal scan	High	High	Camera	Low
Facial recognition	Medium-low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand geometry	Medium-low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Signature Recognition	Low	Medium	Optic pen, touch panel	High

Table 2.2: Comparison of the Biometric methods by Levent Arslan (2016)

	Eye-Irish	Eye - Retina	Fingerprint	Hand's geometry	Writing signature	Voice
Reliability	Very high	Very high	High	High	High	High
Easiness of use	Average	Low	High	High	High	High
Attack's precaution	Very high	Very high	High	High	Average	Average
Acceptance	Average	Average	Average	High	Very High	High
Stability	High	High	High	Average	Average	Average
Identification and authentication	Both	Both	Both	Authentication	Both	Authentication
Interference	Glasses	Irritation	Dirtiness, Injury, Roughness	Arthiritis, Rheumatism	Changeable Or easy signatures	Noise, cold
Use	Nuclear installations, medical services, penitentiary centres	Nuclear installations, medical services, penitentiary centres	Police, industrial	General	Industrial	Remote access in banks or data base.
Price for node ml 997 (USD)	5000	5000	1200	2100	1000	1200

From this comparative table 2.2 we can deduce that the most adequate methodology is the fingerprint authentication.

II. RELATED WORK

Many recent studies have focused on using biometric techniques in enhancing the security of the ATM. However, a few studies have also exploited the use of GSM Technology, while some have adopted a combination of both techniques.

Table 2.1 summarizes some of the related studies, the techniques they adopted, the contribution and limitations of the studies.

Table 2.1 Summary of past related studies

AUTHORS	TECHNIQUE **ADOPTED**	**CONTRIBUTION**	**LIMITATIONS**
Oko S. and Oruh, J. (2012)	Finger print biometric token	Developed ATM based fingerprint verification and simulated it for ATM operations by incorporating the fingerprints of users into the bank's database.	1. The system developed was inefficient because there was no finger print matching algorithm. 2. The system developed was not built as an enhancement of the existing system.
Ravikumar et al. (2013)	Fingerprint recognition in digital image processing using both primary and reference fingerprint to authenticate users instead of the traditional pin number	A new business model which would enhance ATM security was proposed.	Another reference fingerprint belonging to a nominee or a close family member was adopted which also lead to a security could breech, thus compromising the security of the account owner. 2. The proposed system was not built
Padmapriya V. and Prakasam S. (2013)	A combination of fingerprint biometric token and GSM technology	Proposed a system architecture that incorporates both the finger print and GSM technology into the existing PIN-based authentication process.	2 A nominee or third Part's finger print was incorporated in the architecture. 3 There is a discord between the main user and the nominee user in the proposed system architecture.
Jimoh R.G. and Babatnnde A. N. (2014).	Short Message Service (SMS) verification.	Developed an algorithm for enhancing ATM authentication system using Short Message Service (SMS) verification. 2.Conducted a usability testing of die proposed system	1. The developed algorithm only considered a minimum withdrawal amount.
Das, S.S. and Debbanna S.J. (2011)	Finger print biometrics	Developed a system for the withdrawal interface of the ATM while incorporating the finger print biometric in the authentication process	1. A nominee or third Party's finger print was Incorporated in the design.
Santhi B. and Ram Kumar K. (2012)	Finger print biometric and GSM technology	Proposed an algorithm that provides two phases of security using both biometric and GSM technology as alternatives	
Prithika M. and Rajalakshmi P. (2013)	Ins Recognition and Palm Vein (IRPV) recognition technology	Proposed using the Iris Recognition and Pahn Vein (IRPV) recognition technology to prevent card duplication and crimes via the ATM	1. The proposed system was not built as an improvement on the existing System
Okereke E. Ihekweaba G. and Okpara F.K. (2013)	Facial recognition technology	A system which incorporates facial recognition technology into the identity verification process used in ATMs was proposed	1. The proposed system was not built as an improvement on the existing system. 2. The study relied on open-source facial recognition program and did not discuss the local features that will be analyzed for the facial verification process.
Ibidapo et. ai. (2010)	Fingerprint biometrics	A fingerprint mechanism as a biometric measure to enhance the security features of die ATM was developed.	
Selvaraju N. & Sekar G. (2010)	Advanced Encryption Standard (AES) algorithm	The Advanced Encryption Standard (AES) algorithm was adopted to improve the security level of ATM Banking Systems.	

III. THE EXISTING SYSTEM

The existing ATM system authenticates transactions via the card and PIN-based system. Thereafter, it grants access to bank customers to several services such as cash withdrawal and deposits, account to account transfers, balance enquiry, top-up purchases and utility bills payment. The ATM system compares the PIN entered against the stored authorization PIN for every ATM users. If there is a match, the system authenticates die user and grants access to all the services available via the ATM. If there is a mismatch on the other hand, the user authentication process fails and the user is given two more opportunities to enter a correct PIN. If an incorrect PIN is entered for the third time, the card gets blocked and retained by the ATM.

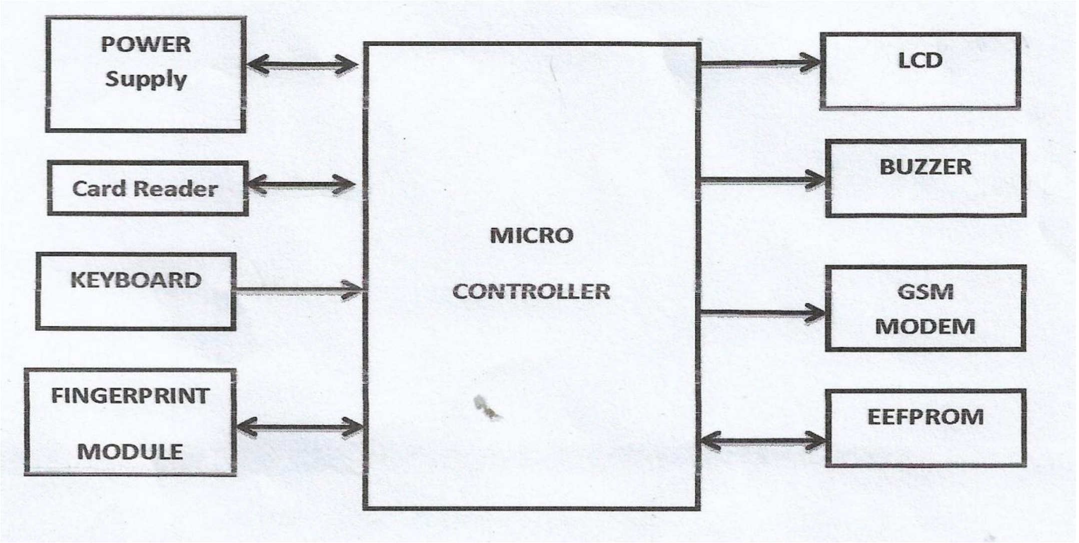

Figure 3.1: Overview of existing architecture: source Avinash Kumar Ojha, (2015).

ADVANTAGES

1. It is very fast
2. The card is carried about anywhere you go, instead of physical cash
3. It can be used for payment at shop and online
4. Money is a bit secure than carrying physical cash

D IS A VANTAGES

1. Once the PIN is forgotten you cannot use the card
2. A little scratch on the chips the card is render useless
3. Card can be stolen and PIN hacked
4. Card and PIN can be collected at gun point
5. Card develop fault and may be damage when leave in a pocket wallet
6. Money is not completely secure
7. Card can be trapped inside the ATM machines
8. Customers with multiple accounts in different bank carries multiple ATM Cards

IV. THE PROPOSED SYSTEM

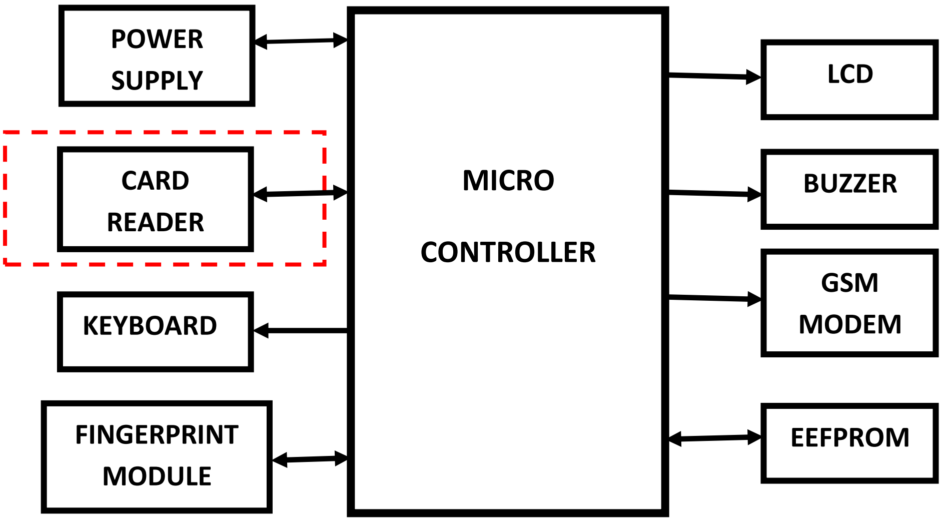

Figure 4.1: The Proposed Architecture

The proposed system is an improvement of the existing system, and it does not require card and PIN to operate. The proposed system work with biometric fingerprint only, the customer uses fingerprint at ATM and if matched correctly, then all banks of the customer have account with appears, the customer will select the bank to transaction with, then select the account type with that bank , then chose to withdraw, check account balance and so on. Customer will now choose or select the bank he wants to withdraw* money from and specify if the account is Current or Savings, this is a means of securing ATM transaction using biometric fingerprint.
This proposed system has a lot of advantages over the existing Card and PIN method as stated follows:

ADVANTAGES

1. Banks will save money use in buying the ATM machine Cards.
2. Customers will no longer carry plenty ATM cards around.
3. Money will be more secured.
4. All customer bank accounts are link together as one.
5. No more worried of card theft, ATM card trapped and faulty cards.
6. Online shopping is also possible using new fingerprint PCS
7. Faster than the traditional methods

Implementation Algorithm

The algorithm for the proposed system described is as follows:

```
Start
1.   Get Fingerprint image
2.   IF Fingerprint is matched?
3.   IF Yes, Go To 5 Else GO To 2
4.   Proceed To Bank Transaction
5.   SELECT Banks
6.   SELECT Account Type Current or Savings
7.   Do Cash Transactions
Stop.
```

V. CONCLUSION AND FUTURE WORK

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. ID cards can be lost, forged or misplaced; passwords can be forgotten or compromised, but ones' biometric is undeniably connected to its owner. It cannot be borrowed, stolen or easily forged. Using the proper PIN gains access, but the user of the PIN is not verified. 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 using fingerprint identifier may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. Biometrics is not only a fascinating pattern recognition research problem but, if carefully used, could also be an enabling technology with the potential to make our society safer, reduce fraud and lead to user convenience by broadly providing the following three functionalities (a) positive identification (b) large scale identification and (c) screening.

REFERENCES

[1]. Adepoju, A.S and Alhassan, M.E. (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), 1-10.

[2]. Aliyu, A.A. and Tasmin, R.B. (2012) Information and Communication Technology in Nigerian Banks: Analysis of Services and Consumer Reactions. In proceedings of 3rd International Conference in Business and Economic Research (3rd ICBER 2012) 150-164.

[3]. De Luca, A., Langheinrich, M. and Hussmann, H. (2010). Towards Understanding ATM Security — A Field Study of Real World ATM Use. Retrieved from: https://cups.cs.cmu.edu/soups/201 Q/proceedings/al 6 deluca.pdf Accessed on November 26, 2014.

[4]. Jimoh, R.G. and Babatunde, A. N. (2014). Enhanced Automated Teller Machine using Short Message Service authentication verification World Academy of Science, Engineering and Technology. International Journal of Computer, Information Science and Engineering, 8(1), 14-17.

[5]. Kyle, C. (2004). Biometrics: An In Depth Examination. SANS Institute Information Security Reading Room. SANS Institute 2004.Retrieved from: http://www.sans.org/reading-room/whitepapers/authentication/biometrics-in-depth- examination-1329.Accessed on November 26, 2014.

[6]. Leow, H.B. (1999). New Distribution Channels in banking Services. Banker's Journal Malaysia, No.l 10, 48-56.

[7]. Liu, N. Y. (2013). Bio Privacy: Privacy Regulations and the Challenge of Biometrics.

[8]. Oko, S. and Orah, J. (2012): Enhanced ATM security system using biometrics. UCSI International Journal of Computer Science Issues, 9(5), 352-357.

[9]. Ravikumar, S., Vaidyanathan, S., Thamotharan, S. &Ramakrishan, S. (2013), A new business model for ATM.

[10]. Rosenblatt, S. (2013). Two-factor authentication: What you need to know. Retrieved from: http://www.cnet.com/news/two-factor-authentication-what-you- need-to-know-faq/ last updated on April 14, 2014. Accessed on November 23, 2014.

[11]. Shoewu, O. and Edeko, F.O. (2011). Outgoing call quality evaluation of GSM network services in Epe, Lagos State. American journal of scientific and industrial research, 2(3), 409-417.

[12]. Siddique, M.I and Rehman, S. (2011). Impact of Electronic crime in Indian banking sector - An Overview Int. International Journal of Business & Information Technology, 1(2), 159-164.

[13]. Okokpujie K., Olajide F., John S. and Kennedy C.G., (2016). Implementation of the enhanced fingerprint authentication in the ATM system ssing ATmega128 with GSM feedback mechanism. Conference paper on Â banking in Nigeria.

[14]. Jimoh, R. G., & Babatunde, A. N. (2014). Enhanced Automated Teller Machine Using Short Message Service Authentication Verification. *African Journal of Computing & ICT*, *7*(1), 115-120.

[15]. Kumar, K. R., Santhi, B., & Janani, N. (2012). Enhanced ATM Security with PII Using Otpip Algorithm. *Research Journal of Applied Sciences, Engineering and Technology*, *4*(24), 5406-5409.

URANG Awajionyi S, et. al. "Securing Automated Teller Machine (ATM) Transaction Using Biometric Fingerprint." *American Journal of Engineering Research (AJER)*, vol. 9(9), 2020, pp. 36-43.