A Multi-Factor Biometric Model for Securing E-Banking System

Mike Izah Omogbhemhe
Department of Mathematical and Physical Sciences, Samuel Adegboyega University, Ogwa Edo State Nigeria

Momodu Ibrahim Bayo
Department of Computer Science, Ambrose Alli University, Ekpoma, Edo State, Nigeria

ABSTRACT
The e-banking systems in Nigeria is witnessing a large number of users, thereby encouraging the cashless economy policy proposed by the Central Bank of Nigeria (CBN). Hence, these systems need to be highly secured and reliable. This is because any compromise by this system can breach the customer's trust in using such systems for making transactions thereby discouraging the cashless policy agenda. Based on this the CBN is proposing the use of fingerprint biometric as a means of identification of any bank customer in Nigeria. However, since most fingerprint biometric systems can accept and grant access to artificial fingerprint, it is therefore clear that only fingerprint will not be suitable in securing banking system. Thus, the primary research objective of this paper is to propose a multifactor biometric model that would assist in creating a highly secured banking application in Nigeria using human physiological features. Based on the verification carried out on the model presented in this paper, it can therefore be sanctify to providing highly secured banking system in Nigeria if fully implemented.

Keywords
E-banking system, Security, Biometric, Fingerprint

1. INTRODUCTION
The banking sector in Nigeria is witnessing tremendous changes in their operations, as a result of the CBN cashless economy policy. The policy is to limit the flow of physical cash in Nigeria economy and to improve the security of bank user's information [12]. Meanwhile securing banking system has been a major concern to so many researchers. It is worthy of note that till today Personal Identification Numbers (PIN), names and passwords are used to secure banking systems in Nigeria banks. But usernames, password, signature and PIN authentication is vulnerable to hacking [19]. Hence, there is need for the e-banking system, operations and methods to be well secured, reliable, simple to access and use. With this in our mind, the banking sector have be making more efforts in introducing biometrics as a means of verifying and authenticating customers account. In order to improved security measures in many data-driven applications, authentication like biometric plays important roles [15].

Recently the Central Bank of Nigeria (CBN) makes it mandatory for all bank customers to register their biometric information with their respective banks. However these biometric are not used yet as a means of account verification and authentication. On this account, [18] and [7] proposed the used of fingerprint biometric for a secured and reliable e-banking services. Meanwhile biometric is the utilization of physiological characteristics to differentiate an individual. It utilizes biological characteristics or behavioral features to recognize an individual. It is a new way to verify authenticity [16]. The reason why biometric is gaining more attention in the banking sectors is because if used as a means of identification it will enhance information security and encourages many (both literate and illiterate) customers to perform their transactions using the e-banking services. However, because of the possibility of many biometric systems to accept artificial fingerprint [12], there is need for a multi-factor biometric techniques in securing system of this nature. Hence, this paper presents a multifactor biometric conceptual model that can ease the implementation of a well secured and reliable banking system using human physiological features. This model provides multi-stage of biometric measures for securing banking system.

This kind of research is a ground breaking move in Nigeria banking sector as the CBN are clamoring for the use of biometric in securing e-banking system for the full actualization of secure e-banking system thereby encouraging the cashless economy policy.

2. RELATED WORKS
Till today most computer systems are faced with a lot of security challenges, the electronic means of performing banking transaction is not an exemption, this call for the need of strong security in these systems. Any electronic transaction system must be able to guarantee strong security, privacy, integrity, compatibility, efficiency, convenience, mobility and low financial risk among others which are the characteristics of biometric system [4]. Meanwhile identity theft is one of the major and most prominent problems in e-banking system. Hence, the need for strong security platform for this system cannot be under estimated. It is true that introducing e-banking system in Nigeria has helped to curb most of the problems associated with the manual system that make our economy to be cash based economy.

However, with Nigeria gradually eliminating the long existing cash based economy through e-payment system; Cyber terrorist has stated taking advantages of the poor security nature of this system in sabotaging the country effort and aim in introducing this technology thereby using it for financial fraud. Some of the major problems of this system are recorded by [6]; [5]; [2] and [1]. Similarly those that are authorized in using the system for transaction cannot be left out for using such system for fraud. Meanwhile many financial analysts have warned these institutions to work out modalities and methodologies in providing strong security for e-banking systems. Also, [17] noted that the inadequate of security potentials in e-banking system lead to financial lost in these systems.

Similarly, [8] reported that Nigeria has move six position up the ladder to occupy the 59th position globally among countries with greatest electronic transaction security threats. The question in the mind of many is that a country with such security threats how can it successfully achieve a cashless

economy? Thus the introduction of biometric verification number was made by the CBN to help capture each bank customer biometric data which will help curb these security challenges. Biometric fingerprint are unique to every human. They are generations of numerous ridges and valleys on the surface of human figure. A finger print is the flows of ridges patterns in tip of the finger. Among all biometric traits, fingerprint has one of the highest levels of reliability [11].

Biometric is the utilization of physiological characteristics to differentiate an individual. It utilizes biological characteristics or behavioral features to recognize an individual. It is a new way to verity authenticity in many transaction systems [16]. CBN are now introducing such system for securing e-transaction system in order to encourage and achieve the cash-lite policy because password, signature and pin are no more enough to authenticate identity but we should now fall to biometric measures.

However many studies has shown that a biometric system that uses a single biometric trait for recognition could also be compromise [1,8]. Hence, to eliminate this compromise (problem) we need a combination of more than one biometric feature in securing banking system.

3. METHODOLOGY

This paper mainly focuses on the direction of developing a highly secure e-banking system in Nigeria using more than one human physiological feature (fingerprint, human face and iris) to gain access to the system. The paper used design science approach to conduct the research. The approach was defined in the work of [13] as a good approach that provides a method for conducting research and provides a model for the research output. Hence, this research was carried out using this approach. Similarly, the methods used in carrying out this research are literature review, model design and key informant interview method.

Using the design science approach with this method, the steps enumerated below were followed

- Identification and definition of the Problem: This is the process of establishing the problem to be solved.
- Possible Solution: This is the identification of the possible solutions to the identified problem
- Model Design: This is developing the solution to the problem in form of a model.
- Demonstration: Demonstrating how efficient will the model solve the problem
- Evaluation: Observing how good the model supports the solution to the problem.

These steps were followed as a guide in each of the method identified in this paper.

Literature review is conducted to gain more knowledge and understanding of a chosen research area and help to bring clarity and focus to a research problem.

Evaluation is a very important component in the design science approach steps. Through it, the extent to which the model supports the solution to the problem can be determined [14].

In this paper the evaluation and demonstration steps for the model were carried out by using the Key Informant Interview Method (KIIM). KIIM can be defined as the discussion with someone that has detail knowledge about a problem and its possible solution. This kind of interview is semi-structured interview which do not require a standard steps of questions and is flexible to conduct. The method is used to discuss a topic with knowledgeable person in a particular area.

In using this method, gaining access to key informant is always a definite problem. However in this research access was gain by using email and phone number to contact the key informant.

The approach used in choosing this informant was based on their line of work, knowledge and experience in the banking software security.

4. THE MULTIFACTOR BIOMETRIC E-BANKING MODEL

This section introduces and discusses in detail the individual element in this model. This will help to gain more knowledge about the proposed model and also serve as a guide during the full implementation of the system. The proposed model is divided into four sub-systems, as listed below:

The Fingerprint Matcher: This sub system is used for the customer's fingerprint

The Face Matcher: This sub system is used for the customer's facial properties

The Iris Matcher: This sub system is used for the customer's iris properties

The Combined Decision Matcher: This sub system is for comparing decision made by all other three sub system with the matcher template.

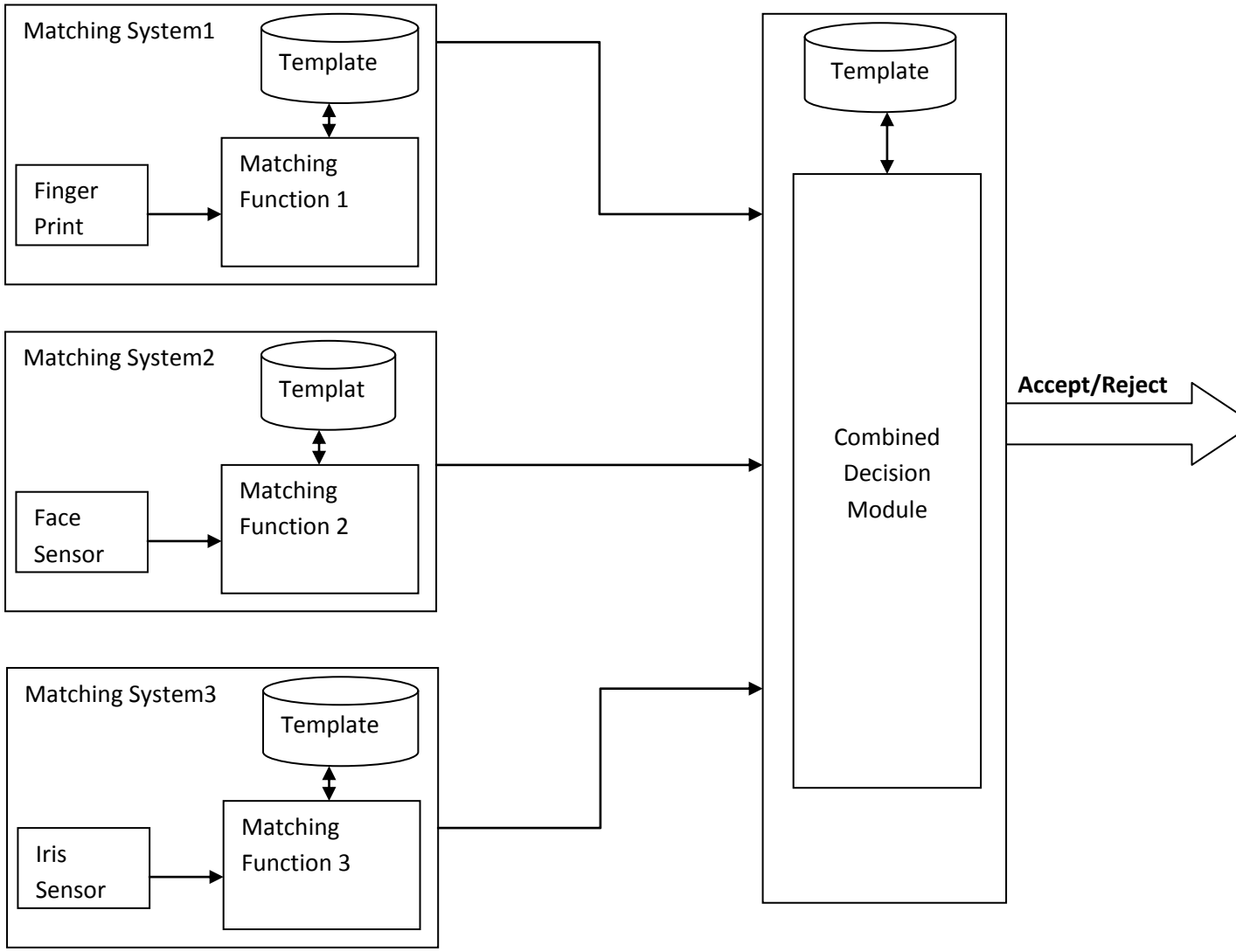

Fig 1: System conceptual model

4.1 The Fingerprint Matcher

This sub model is used for generating fingerprint template through the use of fingerprint scanner and comparing it with the existing fingerprint in the database to ascertain if the fingerprint exist or not. The modules in this sub model are

- Fingerprint scanner that is used for capturing the fingerprint image and pass it to the matching function.
- Matching function: This is the function that will compare the fingerprint captured with the one in the database. It will then ascertain whether the captured fingerprint is valid or not and return the result to the combined decision sub model
- Template: This consists of the existing fingerprint that is captured during customer's registration. It is the fingerprint database that can be checked by the matching function to ascertain if a particular fingerprint exists or not.

4.2 The Face Matcher

This sub model is used to process the facial features of the individual. The model consist of the facial camera that capture the face, the matching function that compare the captured facial features with the existing ones in the facial database (template) and the database that is used to store already captured customer's facial properties.

4.3 The Iris Matcher

This sub model is used to process the iris features of an individual. It has an iris capture camera that is use to capture the customer's iris image, the matching function module that help to perform comparison between the captured iris image and the existing image and the database that store already captured iris image.

4.4 Combined Decision Sub Model

This is the sub-model that determines whether the valid fingerprint, iris and face belong to one person. This model has a database the record all the information (fingerprint, face, iris and account data) belonging to a particular person. If the information provided in other sub model (fingerprint, iris, face) are valid, it is the job of the combined decision model to check if the information belong to one person. If the information belongs to one person access will be granted else access will be deniel.

4.5 Verification of Model

Prior to this section, it was stated that this model was verify using key informant interview method. This section discusses in detail how the method was used to verify the model presented in this paper. Before conducting the interview, a brief of the interview that communicates the aim, objectives and background information about the model was sent to the interviewee e-mail. Through phone, it was confirmed that the interviewee receive the message and the message was well understood.

During the interview, the propose model was presented in slides and all the components were presented in different slides. This help to explain the components of the proposed model and their different functions. The questions that were asked are given below:

Is the model comprehensive?

Are all the sub model relevant to the aim?

Are the model's component ok?

Do you think this model will achieve the set aim and objectives?

Any other useful suggestion to improving the model?

The necessity for this interview is to verify that the proposed model will help in achieving a highly secure banking system platform.

When the key informant was asked, he agree with the component of the model in providing strong security to the banking system. He further suggested that the combined decision making sub model database must be separated from other sub model and implemented using database view instead of database table and attaching its information to a particular customer for valid access to the system.

Based on the feedback received from the key informant during the interview, it can be concluded that the conceptual model is efficient and valid for securing banking system.

5. CONCLUSION

Based on the need for highly secured system in the banking sector in Nigeria, the CBN is proposing the used of fingerprint biometric measures in securing this systems thereby encouraging cashless economy in Nigeria. This will help to achieve strong banking systems security and also help in encouraging many customers in using these systems. However, because most fingerprint biometric can be cheated using artificial fingerprint, a multifactor biometric technique is recommended in this paper if strong security must be achieve in these systems. The paper has presented a comprehensive conceptual multifactor biometric model suitable for implementing a secured platform for banking system. The full implementation of this model will help to achieve highly secured banking application and provide better banking services in the future.

6. REFERENCES

[1] Akinyemi O.I, Zaccheous O.O and Olufemi M.O (2010). Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-banking System. Internationa Journal of Electrical and Computer Sciences IJECS. Vol 10, No:6, pp 68-73.

[2] Ayo C.K, Adewoye J.O and Oni A.A (2010). The state of e-banking implementation in Nigeria. A post consolidation review. Journal of Emerging Treads in Economics and Management Sciences. Scholarlink Research Institute Journal 2010 1(1). Pp. 37-45

[3] Ayo, C.K and Ukpera W.I (2010). Design of a secure unified e-payment system in Nigeria: A case study. African Journal of Business Management Vol. 4(9), pp. 1753-1760. Available online at http://www.academicjournals.org/AJBM

[4] Biometrika,(2011). Introduction to Biometric Systems, s.l.: Biometrika (Italy) Available at:http://www.biometrika.it/ eng/wp_biointro.html.

[5] Drygojio, A (2011) Information and Communication Security. LIDIAP Speech processing and Biometric Group. Institute of electrical Engineering. Ecole polytechnique Federalede. http//scgwww.epfl.ch/courses

[6] Fajfar, M (2004). Role and Security of Payment Systems in an Electronic Age. IMF Institute Seminar on Current Development in Monetary and Financial Law. Available at www.imf.org/external/np/leg/sem/2004/edmfl/eng/faj.pd

[7] Favour N (2013). CBN to Lunch Biometric Details of banks customers. Vanguard Newspaper December 11 2013.

[8] Fidelis O, Francis O, Samuel A, Frank E.O and Calister N.M (2012). Enhanced Modified Security Framework for Nigeria Cashless E-payment System. International Journal of Advanced Computer Science and Applications, Vol. 3 No. 11, 2012

[9] Joseph M,Steven K and Micheal K (2015). A Study of Approaches and Measures aimed at Securing Biometric Fingerprint Templates in Verification and Identification Systems. International Journal of Computer Applications Technology and Research Volume 4– Issue 2, 108 – 119

[10] Jung ho, E (2014) The Design of Robust Authentication Mechanism using User's Biometrics Signals. International Journal of Security and Its Applications Vol.8, No.6, pp.71-80

[11] Keerthi P.P. Deepak R.G. Swathi K. and Rupali N. (2014). Secure Fingerprint Using Mosaicing. IOSR Journal of Computer Science Vol 3. Issues 2. Pp. 73-79.

[12] Okoye P.V.C and Raymond E (2013). An Appraisal Of Cashless Economy Policy In Development Of Nigerian Economy. Research Journal of Finance and Accounting. Vol.4, No.7.

[13] Pe_ers K, Tuunanen T, Gengler C.E, Rossi M, Hui W, Virtanen V and Bragge J (2006)The design science research process: A model for producing and presenting information systems research". In Proceedings of the first international conference on design science research in information systems and technology (DESRIST 2006), pp. 83-106.

[14] Pe_ers K, Tuunanen T, Rothenberger M.A and Chatterjee S (2007) .A design science research methodology for information systems research". Journal of management information systems, vol. 24, no. 3, pp. 45-77

[15] Rashmi H. (2015). Biometrics Authentication Technique with Kerberos for Email Login. International Journal of Advances in Engineering and Technology.

[16] Ruppinder S and Naringer R. (2014). Comparison of Various Biometric Methods. International Journal of Advances in Science and Technology Vol. 2 issue 1.

[17] Shah, M.H., (2012). Critical Success Factors in e-Banking: A Study of Two UK Retail Bank.

[18] Sri S.D and Jhunu S.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. Vol.1 No. 5. Pp 197-203.

[19] Vandommele T (2010). Biometric Authentication Today. Available at http://www.csc.hut.fi/en/publications/B/11/papers/vandommele.pdf.