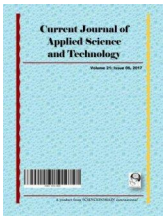

Current Journal of Applied Science and Technology

28(5): 1-6, 2018; Article no.CJAST.31471
ISSN: 2457-1024
(Past name: British Journal of Applied Science & Technology, Past ISSN: 2231-0843, NLM ID: 101664541)

An Improved Multimodal Biometric Architecture for Securing Online Payment

M. I. Omogbhemhe[1*], I. B. A. Momodu[2] and S. Awojide[3]

[1]Department of Mathematical and Physical Sciences, Samuel Adegboyega University, Ogwa Edo State, Nigeria.
[2]Department of Computer Science, Ambrose Alli University, Ekpoma, Edo State, Nigeria.
[3]Department of Mathematical and Physical Sciences, Samuel Adegboyega University, Ogwa Edo State, Nigeria.

Authors' contributions

This work was carried out in collaboration between three authors MIO, IBAM and SA. Author MIO designed the architecture, managed literature searches, citations/references and wrote the first and final draft of the manuscript. Author IBAM participated in the design of the architecture, coordinated and supervised the work, Author SA analyzed the architecture and manage literature searches. Authors have read and approved the final manuscript.

Article Information

DOI: 10.9734/CJAST/2018/31471
Editor(s):
(1) Samir Kumar Bandyopadhyay, Department of Computer Science and Engineering, University of Calcutta, India.
Reviewers:
(1) P. C. Lai, Universiti Tenaga Nasional (UNITEN), Malaysia.
(2) Donald Rotimi Ogungbade, Osun State Polytechnic, Nigeria.
(3) Darmesh Krishanan, Management and Science University (MSU), Malaysia.
(4) J. Ramola Premalatha, VIT University, India.
Complete Peer review History: http://www.sciencedomain.org/review-history/25858

Short Communication

Received 7th January 2017
Accepted 9th March 2017
Published 11th August 2018

ABSTRACT

The need for cashless economy in the banking sector has introduced electronic banking popularly called the e-banking system. This system helps to limit the volume of physical cash in circulations. It encourages the use of electronic (computer platform) to perform payment through bank transfer. This kind of system has been seen to be very useful in moving any economy from cash-based economy to a cashless economy with numerous advantages. However, the current security features of this platform that enable the online payment through bank transfer are very weak. This is so because, during the use of the current online payment platform, the user is expected to provide some security digit codes usually four digit number as personal identification number (PIN) used during registration in the platform to authenticate the money transfer. Since people can easily misplace their PIN, there is need to use a more robust method in securing this platform. Hence, this

**Corresponding author: E-mail: mikeizah@gmail.com;*

paper has presented the use of more than one human physiological feature in securing this platform. The primary research objective of this paper is to design a better multimodal biometric architecture suitable for securing online payment platform.

Keywords: Multimodal biometric; online payment; architecture; banking.

1. INTRODUCTION

Till today money is an abstract way of representing value and it has been the system for making payments between two parties. In the course of time, new representations of value were introduced. These include bank notes, payment orders, cheques and later credit cards. All these have been inculcated into the latest payment system called electronic payment systems. As the transition to electronic payment systems take place, the stock of currency held outside the banking system which constitutes a potential source of unproductive economic resources because they are not available for credit expansion is integrated into it thereby expanding the deposit base of the monetary system. E-payment systems refer to the processes of exchanging monetary value among parties in business transactions and transmitting this value over the information and communication technology (ICT) networks. E-payment can also be refers to as application of electronic means in the interaction between Government and Citizens and Government and Businesses. It is a form of direct banking without physical appearance at the Bank through the means of electronic, interactive communication channels and other technology infrastructure. The risk carrying physical cash has been eliminated with the help of electronic payment. E-payment has a higher ability to encourage e-commerce. Since people can perform and perfect their transactions through buying and paying electronically, the e-commerce will be highly sustained. The current e-payment platform uses PIN to authenticate and validate payment from registered user. During payment, the platform will request the PIN from the user and if the PIN is correct, the payment or transfer will be validated. However, there exist possibilities of misplacing PIN or PIN theft, when such happen the person's financial details will be at risk. When PIN theft occurs, the payment platform will not be able to know that the correct PIN is not from the valid or right owner but will validate the transaction from the imposter. Meanwhile, this kind of problem scenario is not from the platform but from the user. However, since it is possible to use biometric features which cannot be stolen from the owner for authentication and validation, such will be best in securing electronic-payment platform. The central objective and interest of this paper is providing the road map for securing this e-payment platform using more than one human physiological feature. Meanwhile biometric is the utilization of human physiological characteristics to differentiate an individual. It utilizes biological characteristics or behavioral features to recognize an individual [1]. It is a new way to verity authenticity [2]. The reason biometric will be viable in the banking sectors, is because, if used as a means of identification and validation, it will enhance information and platform security. Similarly, architectural design shows how a system is to work and provide a road map for the implementation. Thus, this paper has presented a multimodal biometric architecture suitable for securing online payment platform. This will go a long way to assisting software developers on how best to secure online payment platform using multimodal biometric which will help to archive maximum security in online payment, thereby encouraging the cashless economy.

2. RELATED WORK

E-payment is a form of payment system that enables a user to make payment (transfer) through electronic tools like internet without involving physical cash. E-payment can be refers to as the subset of e-governance which is the application of electronic means in the interaction between Government and Citizens, Government and Businesses and Citizens and Government. It is a form of direct payments without physical appearance at the Bank through the means of electronic, interactive communication channels and other technology infrastructure. E-payment has been broaden because of the rapid growth of Information and Communication Technology. Till today there exist some threat to the existence of e-payment system, one of such is insecurity. However, there are standard security features already developed to handle them. Some of the available solutions include public-key cryptography, digital signature and certificate, secure socket layer (SSL) and secure electronic transaction [2]. [3] develop a three level security model for security banking transaction. This is made up of security module and the network control module. The security module is further

divided into three sub level modules which include user authentication device server authenticate and transaction data security module. Ayo et al 2006 designed e-payment system. Their system still used PIN to carry out its security. [4] developed a model for detecting irregularities in banking transaction using neural network. [5] developed a model for securing e-banking system using graphical password authentication scheme. The model identified series of steps to follow for an application to validate the use of banking system using password and image sound. One strong limitation of this model is the used of password that can easily be hacked by impostors. Also [6] developed a framework for securing online Bank system. The framework uses smart card that contain a secret key of the legitimate user to access the user's account. It also implements encryption and description in its operation. The limitation of this model is that when the smart card is stolen, it can be efficiency used by the imposter. [7] presented a model for securing banking system. The model makes use of PIN and card number to secure the customer information

2.1 Need for Implementing Biometric in Online Payment

According to [8] financial institutions need more intrusive security procedure in their software than many other applications. The applications used by many financial institutions today for online payment faces weak security features, since they uses personal identification number (PIN) to validate transactions. This is true because, people can easily copy someone PIN to commit fraud on those people's financial details. PIN authentication is vulnerable to hacking [9,10]. In order to improved security measures in many data-driven applications, authentication like biometric plays important roles [11]. [12] pointed out that "Biometrics provide very powerful tools for the problems requiring positive identification and provide enabling technology that have potential to make our society safer, reduce fraud and lead to user convenience". Compared to other security measures, application of biometric technology may provide a better method to curb on line fraud, since it uses certain physical and behavioral traits that are distinctive to an individual to identify and verify the person through authentication; other forms of authentication methods have presented problems of improper authentication to users, for adequate on-line data protection and authentication, there is need to offer improved solution through biometric system [13,14]. According [15], "Institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services", also [16] affirmed that "fingerprint technology in particular, can provide a much more accurate and reliable user authentication method". Biometric utilizes biological characteristics or behavioral features to recognize an individual. It is a new way to verify authenticity [17]. [18] maintained that the idea of using biometric for bank user authentication is a new idea because of the limited researches in this area.

2.2 Need for Multimodal Biometric in Bank

Multi modal biometric systems utilize more than one physiological or behavioural characteristic for enrolment, verification or identification. According to [19] a multibiometric system can have multiple sources of information: multi-sensor, multialgorithm, multi-instance, multi-sample and multimodal (many biometrics combined, like iris, fingerprint, face, etc.). Multiple biometric systems can be combined in order to increase the security of specific applications. Multi modal biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. The combined strengths of these scheme present computer users a secure and usable authentication scheme that reduces fraudulent practices in payment transaction in the banking sector. For example a system with fingerprint and face recognition would be considered "multimodal" even if the "OR" rule was being applied, allowing users to be verified using either of the modalities [20]. [21] advised that more than one biometric features should be implemented for biometric system, if higher security is needed.

3. PROPOSED ARCHITECTURE

The section shows the multimodal biometric architecture (see Figure 1). The architecture has different reporting module for error checking and recovering. Similarly each biometric module in the architecture has its own database that helps to direct and acceleratess the processing of biometric data. Implementing this architecture requires the use of fingerprint scanner and face camera for capturing and verifying the biometric data.

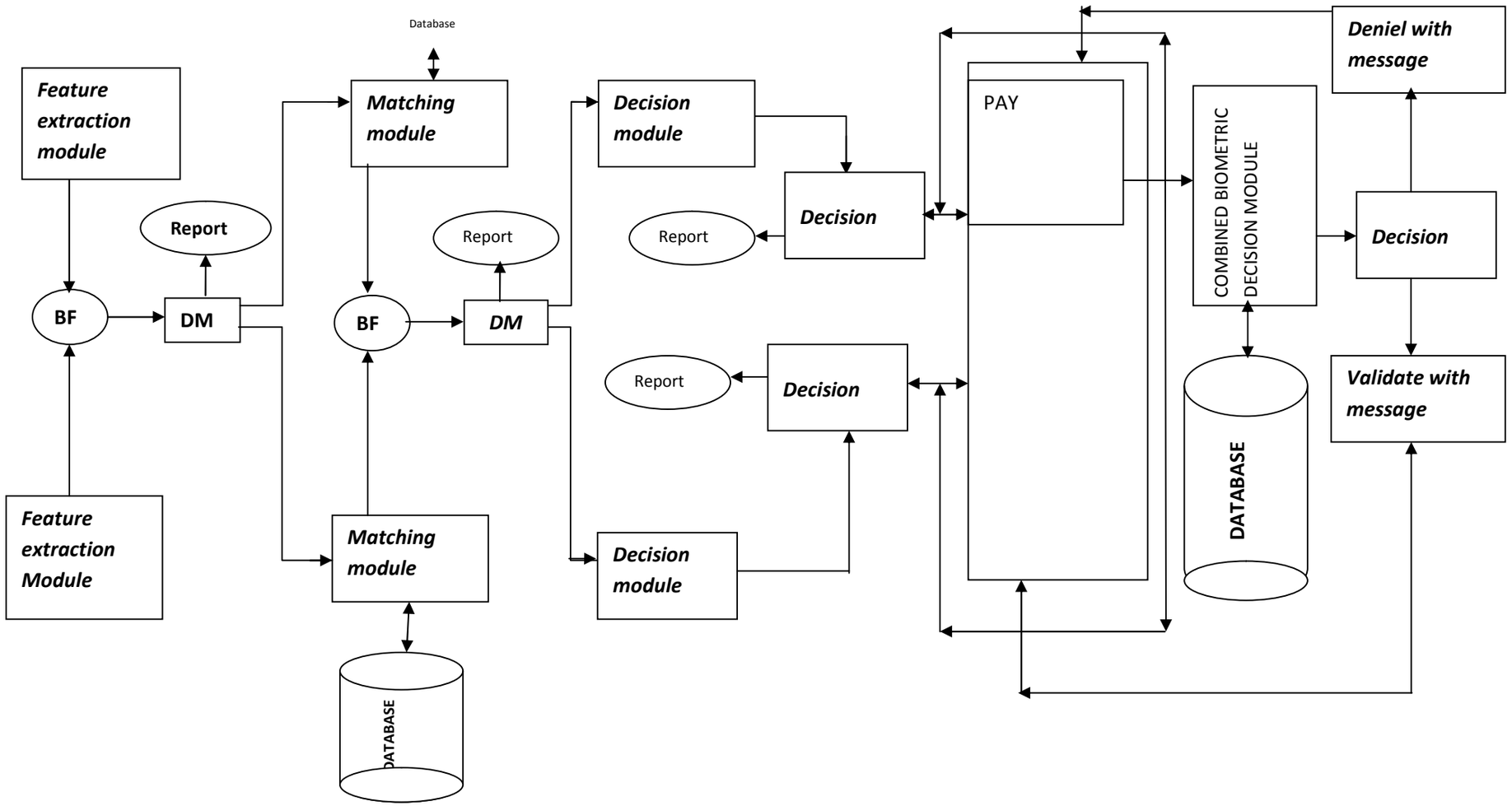

Figure 1. Proposed architecture

4. DISCUSION

4.1 The Feature Extraction Module

This sub model is used for extracting the biometric template through the use of the biometric input device and comparing it with the existing one captured during registration in the database to ascertain if the biometric exist or not. The modules in this sub model are.

4.2 Matching Function

This is the function that will compare the biometric image captured with the one in the database. It will then ascertain whether the captured biometric is valid or not and return the result to the combined decision sub model.

4.3 Database Template

This consists of the existing biometric image that is captured during customer's registration. It is the database that can be checked by the matching function to ascertain if a particular biometric exists or not.

4.4 Decision Module

This module take decision whether a particular person is valid to use the payment platform or not.

4.5 Combined Decision Sub Model

This is the model that determines whether the valid fingerprint and face belong to one person. This model has a database that record all the information (fingerprint, face, and account data) belonging to a particular person. If the information provided in other sub models (fingerprint, 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 payment operation will be validated.

It is important to note that, this kind of technology will eliminate the use of PIN which can be stolen from valid user and result to the use of more than one biometric images in processing payment data. It will help to provide high security to customer financial details because customers closest person cannot take advantage of them in making online payment using their account without their knowledge.

5. CONCLUSION

This paper has presented a multimodal biometric architecture suitable for implementing a highly secured online payment platform. The architecture eliminates the use of PIN as a means of securing online payment. Pin has been identified as a weak tool in data security since it can be stolen from an individual to commit financial fraud. Hence the multimodal biometric architecture presented in this paper will make use of both the customer fingerprint and face to process and validate any online payment before payment can be done using the platform.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Omogbhemhe MI, Momodu IBA. A multi-factor biometric model for securing e-banking systems. International Journal of Computer Applications. 2017;159(4).
2. Ayo CK, Ukpera WI. Design of a secure unified e-payment system in Nigeria: A case study. African Journal of Business Management. 2010;4(9):1753-1760.
3. Emeka RN. Improving the security of the internet banking system using three-level security implementation. International Journal of Computer Science and Information Technology & Security (IJCSITS). 2014;4(6).
   [ISSN: 2249-9555]
4. Adeyiga JA, Ezike JO, Omotosho O, Amakulor W. A neural network based model for detecting irregularities in e-banking transactions. Afr J Comp & ICT. 2011;4(3-2).
5. Mahadevi P, Sukumar R. Modeling anti phishing system for e-banking based on graphical password authentication scheme. International Journal of Innovative Research in Science, Engineering and Technology. 2015;4(Special Issue 5).
6. Khaled AN. A framework for secure online bank system based on hybrid cloud architecture. Journal of Electronic Banking Systems; 2015.
   (Article ID 614386, 13 pages)
   Available:http://www.ibimapublishing.com/journals/JEBS/jebs.html

7. Shewangu D. Cyber-banking fraud risk mitigation, conceptual model. Banks and Bank Systems. 2015;10(2).
8. Sommerville I. Software Engineering. Addison Wesley, 9th ed; 2011.
9. Vandommele T. Biometric Authentication Today; 2010. Available:http://www.csc.hut.fi/en/publications/B/11/papers/vandommele.pdf
10. Jung ho E. The design of robust authentication mechanism using user's biometrics signals. International Journal of Security and Its Applications. 2014;8(6):71-80.
11. Rashmi H. Biometrics authentication technique with kerberos for email login. International Journal of Advances in Engineering and Technology. 2015;7(6): 1735-1744.
12. Gunajit S, Pranav KS. Internet banking: Risk analysis and applicability of biometric technology for authentication. International Journal of Pure and Applied Sciences and Technology Int. J. Pure Appl. Sci. Technol. 2010;1(2):67-78.
13. Shouvik B, Anamitra B, Roy K, Ghosh M, Nilanjan D. A biometric authentication based secured ATM banking system. International Journal of Advanced Research in Computer Science and software Engineering. 2012;2(4):178-182.
14. Okediran OO. A biometric identification based scheme for secured e-payment. Journal of Computation in Biosciences and Engineering. 2014;1(2):1-5.
15. Selina O, Jane O. Enhanced ATM security system using biometrics. International Journal of Computer Sceince. 2012;9(5-3): 352-357.
16. Amtul F. E-banking security issues – is there a solution in biometrics? Journal of Internet Banking and Commerce. 2011; 16(2):1-9.
17. Ruppinder S, Naringer R. Comparison of various biometric methods. International Journal of Advances in Science and Technology. 2014;2(1).
18. Catalin L, Vasile-Gheorghiţa G, Valeriu L Improving the security of internet banking applications by using multimodal biometrics. Journal of Applied Computer Science & Mathematics. 2015;19(9).
19. Ross K, Nandakumar AK, Jain M. Handbook of multibiometrics. Springer; 2006. [ISBN 978-0-387-22296-7]
20. Feng G, Dong K, Hu D, David Z. When faces are combined with palmprints: A novel biometric fusion strategy. Proceedings of First International Conference, ICBA 2004, Springer. 2004; 701-707.
21. Joseph M, Steven K, Micheal K. 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. 2015;4(2):108–119.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sciencedomain.org/review-history/25858