International Journal of Applications of Fuzzy Sets and Artificial Intelligence (ISSN 2241-1240), Vol. 8 (2018), 89-102

A smart crypto-biometric agent based architecture for e-transaction platforms

[1] Veronica I. Osubor, [2]Joseph Ogedengbe

[1] viosubor@uniben.edu

[2] soarwithjoof4sky7@yahoo.com

[1, 2] Department of Computer Science, Faculty of Physical Sciences, University of Benin, Benin City. NIGERIA

Abstract

This paper proposes a smart crypto-biometric agent for performing account portability and banking transactions in any brick and mortar and electronic transactions irrespective of the account type and account location using both crypto and biometric technology. It will capture both physiologic attributes of customers as well as generate a soft code for encrypting data in transit. The outcomes of this study will allay the worries of customers because it will tackle the problems of financial transactions verification and introduce a better and more secure way for e-transaction processes in any platform.

Keywords: *Cryptosystem, Biometric, Bank Verification Number, Secured Transaction.*

Received: March 15, 2018

1. Introduction

The increasing incidences of cybercrime, identity theft, internet frauds and high profile compromise of conventional security systems (password and PIN) have necessitated higher demand for greater security and access to sensitive personal

information in financial system **[1]**. In developing countries, infractions in security and several economic and financial threats to economic development have plagued the growth of businesses caused by security threats, money laundering, cyber frauds, identity theft, etc. **[2]**. Several payment platforms that exist for electronic payment and cashless transactions such as internet banking, Point of Sales (POS) terminal, and Automated Teller Machines (ATM) come with lots of risk unknown to customers **[3]**. Also, violations in credit policies and monitoring system have weakened financial intermediary system in recent times of most developing countries **[4]**. All these have continued to attract academic, economic and industrial assessments on how well Transaction Verification Systems (TVS) would thwart issues of credit defaulters and scams **[5]**. Several countries have developed various strategies in addressing insecurity issues in the banking sector. But in Nigeria, the apex bank (Central Bank of Nigeria) launched Bank Verification Number (BVN)-a centralized biometric identification system with the aim of curbing transaction hazards associated with social security and credit risk which cannot be underestimated **[6]**. BVN uses biometric technology to register customers in the financial system and uniquely identify bank customers across banking industry globally. The major objectives of the initiative are to protect bank customers, reduce fraud and strengthen the Nigerian banking system. Biometric enrolment is helpful to people who cannot read and write. Their finger prints and pictures would serve the same purpose as signatures. Multiple account holders would be covered with a single registration in any of the banks where they have accounts **[7]**. BVN will help the banking system reduce situations where loan defaulters, for instance, move from one bank to the other and the banks extend new credits to them, without knowing their history. Banks would be able to track transactions across all banks in Nigeria with more ease **[8, 9]**. Banks request customers to supply their BVN to perform transactions or linking of their account(s) to their BVN. Some customers cannot retrieve their BVN because either the phone number used to register their BVN have been blocked, stolen, SIM card damaged, or SIM card number assigned to another subscriber. A bank

customer who fails to register and update their BVN will have their accounts placed on a no-debit-status (NDS).

Since at the point of BVN enrolment, the customer biometric and relevant bio-data are collected, retrieving personal details of customers should not be tailored to BVN alone. Other features should be used to retrieve full details of registered customer and perform any transaction in any proxy or brick and mortar (physical) banks without visiting the prime bank (i.e. the bank were the account was opened). These may include using Finger Prints and secured cipher keys. Although using BVN will authenticate the account owner, but transactions online may be compromised over a vulnerable network. Some of these processes can be handled intelligently and securely using software agent.

Shirazi and Soroor **[10]** explained that software agents are autonomous entities which either work on their own or cooperate with other agent architectures and have enormous potentials to be applied in critical systems such as strategic information systems and e-commerce. Software agents are like guards and locomotives of most e-commerce **[11]**. These strengths of Software agents will improve online transaction and increase user trust on e-transaction platforms. It was in this light that the researchers proposed a smart cryptographic biometric agent-based system for electronic or cashless transaction platforms.

2. **Review of Some Related Work on E-transactions**

Gowda **[11]** opined that greater portion of daily activities such as shopping, socializing and working are being transferred to the internet environment. Lots of these activities are embedded in e-transaction systems and platforms with varying benefits and potential insecurity. The increasing incidence of insecurity and privacy breaches has made e-transactions (including e-payment, m-payment, e-commerce and m-commerce) not to achieve its full potential. Many bank customers refuse to perform online transactions due to lack of trust or fear of personal information theft **[12, 13]**. The traditional authentication mechanism was based on physical identity to provide security or access control methods.

Encryption and authentication algorithm require high computing power of computer equipment. Therefore, how to improve and optimize the authentication and mechanism had increased in modern e-commerce environments **[14]**. O'Raghallaigh **[15]** emphasized that any secure e-transaction or e - commerce system must meet four integral requirements (Privacy, Integrity, Authentication, and Non - repudiation). Privacy is an integral part of any e - transaction strategy and investment in privacy protection has been shown to increase consumers spending, trustworthiness and loyalty. Digital signature has been applied to prevent technical attacks **[2, 16, 17]** and non-technical attacks such as phishing and socio engineering task **[18, 19]**.

E-transaction security has its own peculiar flaws and it is one of the highest visible security components that affect the end user through their daily payment interactions **[17, 20]** suggesting cryptographic based approach to e-transaction security is very fundamental to information security and has become a very critical aspect of modern communication system. Users want more simplified, convenient and secure online payment systems **[3, 12]**. Vital information could be simultaneously processed to match with data from e-transactions which allow for efficient and effective integration into organizational processes **[4]**. Clearly, e-transactions require consumers to disclose large amount of sensitive personal information to the vendor, placing themselves at significant risk **[5]**. Ayo and Ukpere **[21]** proposed a unified Smart card-based ATM with biometric authentication. Most importantly, the number of ATM required is drastically reduced, which reduces the cost of production and renewal, and there is enhanced safety, security, and privacy. Asakpa et al. **[22]** espoused that biometric system is a physiological or behavioral characteristics which can be used to identify and verify the identity of the individual. Nwannenna **[7]** advocated that multimodal-biometric system will not only authenticates persons uniquely but also eliminates any possibility of double registration. Some major banks now adopt using Short Messages Services (SMS) to enable e- transactions from one account to the other

of the same bank or dissimilar bank. If this medium is not properly secured, it can be compromised by intruders and the biometric template is susceptible to invasion **[8]**. Chijioke **[6]** has argued that enrolling a customer for BVN requires physical means of identity (Voter's card, National ID card, driver's license, etc) which may not have unique names owing to account opening before BVN initiative, different account names at various banks, change of name of account owner by marriage or other circumstance such as divorce. Fatokun **[9]** noted that for BVN account linking, the only means/platform for retrieving customers bank account details was the BVN 11 digits which may be difficult to retrieve if the Customer is illiterate; telephone number used to link the BVN is lost; damaged, blocked or assigned to another subscriber by the service provider; the BVN requested do not tally or is at variance with the accounts details of the customers in banks Databases and Extension/timeline for account resolution exceeds stipulated period. For physically challenged persons with amputee arms, the finger print enrolment might be impossible which makes them completely out of keying into the cashless society. Since BVN and e-transactions rely heavily on databases, building a secured system that ensures non-compromise of database content will be a welcome development towards ensuring customer's confidence and trust on the BVN initiatives **[8, 22, 23]**.

In the context of this research, some common difficulties or constraints of BVN enrolment of citizens are only focused on commercial banking sectors leaving other financial institutions (micro finance banks, agricultural banks, insurance companies, etc) out of place. Also, people living in hinterlands may have to travel several kilometers or miles before they can be enrolled for BVN. In some locations, banks face poor network challenges to enable them capture the biometrics and upload into Nigeria Interbank Settlement Scheme (NIBSS) database **[6]**. In this work, a combination of multi-modal biometric system and cryptosystem concept was proposed.

3. Methodology

3.1 System's Design

The fusion of biometric system and cryptosystem for BVN validation and transaction authentication is an innovative, secured knowledge-based system. The system was designed to both capture physiologic attributes of customers as well as generate a softcode for encrypting data in transit. Base on evidences that a multi-modal biometric system provides better security for user confidential data, the translation of these confidential data into a more secured non-human readable code will further strengthen the level of security especially via internet gateway payment platform used by banks. The proposed system consists of five modules as depicted in Figure 1.

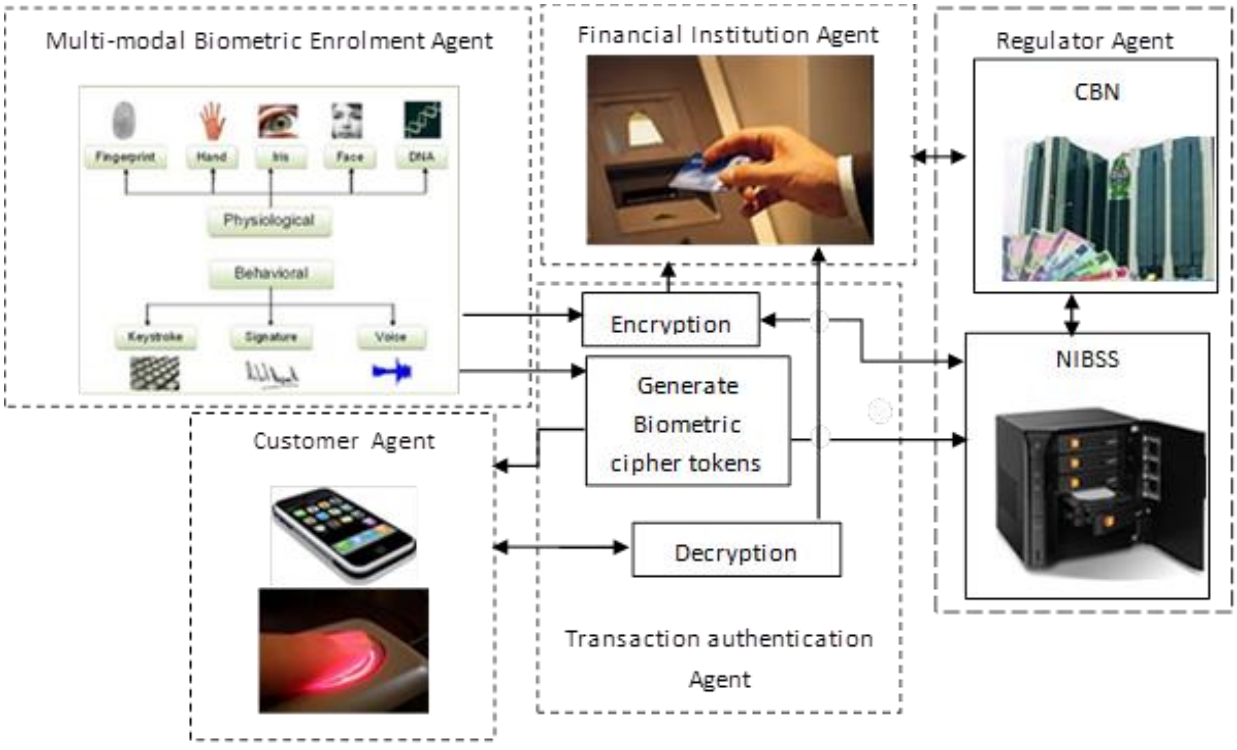

Figure 1: *Proposed system's architecture*

Each agent forms an intelligent agent. The multimodal biometric enrolment agent captures customer biometric for BVN enrolment. The captured BVN passes through the transaction authentication agent where it is encrypted and sent to the financial institution agent for storage. Also, biometric cipher tokens are generated alongside the BVN and are sent to the customer agent via SMS and the regulator agent. For persons in Diaspora (living abroad), the multimodal module should be done by any third registered parties/agents via the internet. The transaction authentication agent serves as a secured validation and transaction authentication gateway for all stakeholders. It generates secured keys (public and private keys). During Validation of BVN, the Public Key and the BVN are sent to the Regulator agent and used to secure customer's account BVN linking. At the financial institution agent, the BVN, public and private keys are sent to the customer's agent via Short Messages (SMS) or imprinted on Automated Teller Machine (ATM) card chips.

The financial institution agent establishes relationship among the bank personnel, customers and bank regulators and the payment gateway/service providers. As shown in figure 1, the cashier is responsible for collecting deposits and other transaction requests from the client (customers). The regulator agent moderates financial institutions and ensures that they operate in conformance with the Central Bank regulations. The payment gateway or service providers are third party financial institutions like Interswitch, Remita, E-transact, etc. that facilitate transaction processing between same or dissimilar payment gateways/channels. The Regulator agents comprise of Central Bank of Nigeria and Nigeria Interbank Settlement Scheme (NIBSS). They ensure that banks adhered strictly to banks regulation. They also ensure that the BVN and cipher tokens created during BVN enrolment are safely stored. The transaction authentication agent is responsible for encrypting/decrypting biometric data created during BVN enrolment, generating of cipher token which will be used to authenticate transactions via cashless transaction platform (ATM, internet and Point-of-Sale (POS) terminals).

3.2 System's Modeling

The use case and sequence diagrams were used to model the conceptual framework of the proposed system **[24]**. Figure 2 shows the use case diagram and figure 3 depicts the sequence diagram of the proposed system.

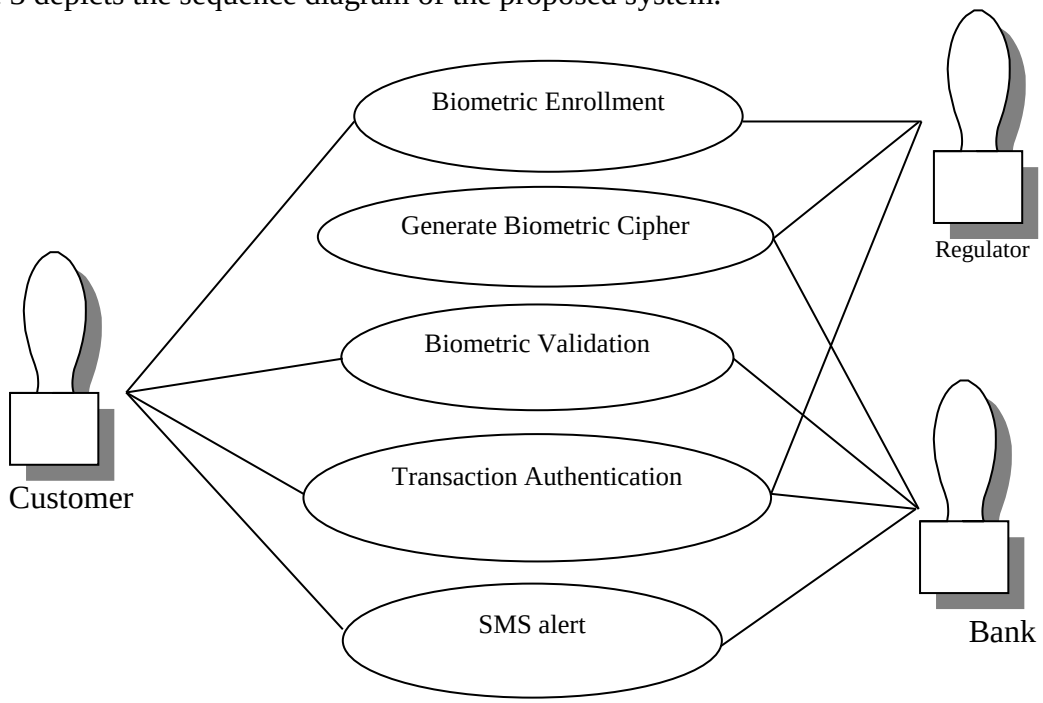

Figure 2: *Use case diagram of the system*

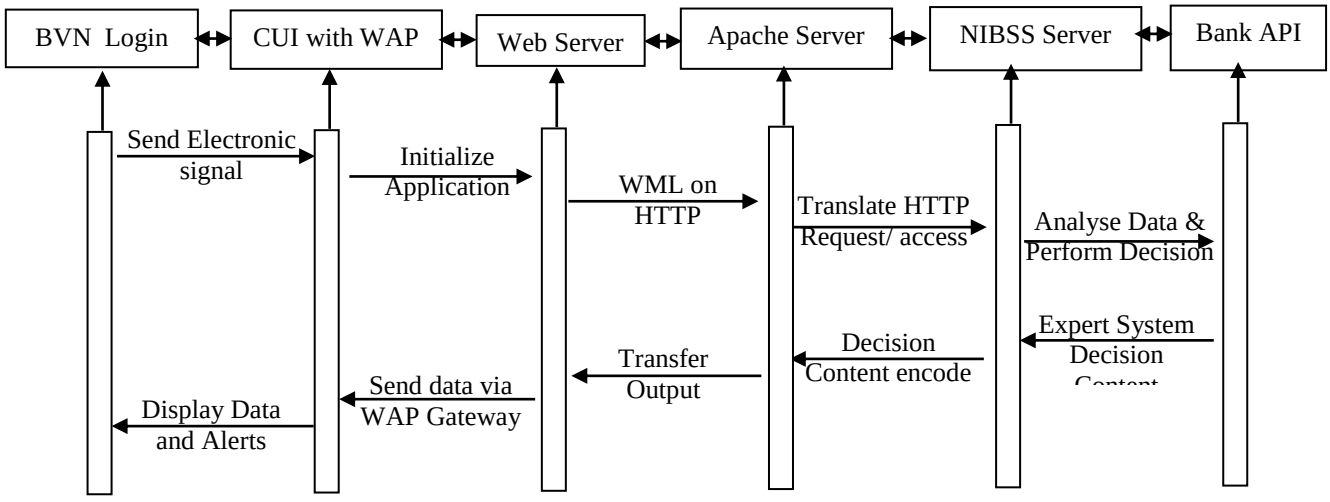

Figure 3: *Sequence diagram of the system*

4. Results and Discussion

4.1 Implementation

While system design stage usually suggest what user interface, input data and actual output that are created, the implementation stage brings them all together. The minimum software required for implementing the smart crypto-biometric e-transaction are Windows 7, Java Language, Java Agent Development Environment (JADE), and My Structured Query Language (MySQL). The minimum hardware requirements are 800 MHz Pentium III processor or equivalent; 512 MB of RAM and 1.5 GB of hard disk space, any fingerprint reader (digital Personnel), and any webcam(inbuilt/external). The following screenshots (figure 4-6) were captured to demonstrate the implementation of the application program.

Figure 4 depicts the enrolment template for customer BVN enrolment. Here, the personal data, physiological biometric features of the customer are captured and stored. Figure 5 shows how customer can open different bank account(s) using biometric features (vocal, Facial or fingerprint). A customer can perform any transaction using any biometric features (fingerprints, facial capture, vocal). The retrieved details comprises of the number of bank accounts the customer has opened, the amount left in the various accounts and valid identity. The customer specifies the amount to withdraw and complete the transaction (Figure 6).

4.2 Findings

It is very glaring that the implementation of smart crypto-biometric multi-agent system will improve the existing framework used for securing e-transactions. While BVN enrolment was a temper proof that uniquely identify customers throughout the entire financial sector, the cryptosystem will ensure maximum security of financial data in transit. It was observed that securing biometric data of BVN will further enhance the securing of financial transactions. It was also observed that relying on BVN alone might make the system vulnerable to intrusion attacks, phishing, hackers, etc. The RSA Encryption algorithms have

been proven to be very hard to crack or compromise. Also, customer can link their accounts with their BVN using other means like voice, fingerprint and not rely on BVN numbers which can be difficult to remember by most customers especially the uneducated ones. Implementing a multimodal crypto-biometric framework will further enhance the trust on financial institutions and will reduce the incidence of double enrollment and reduce cyber frauds.

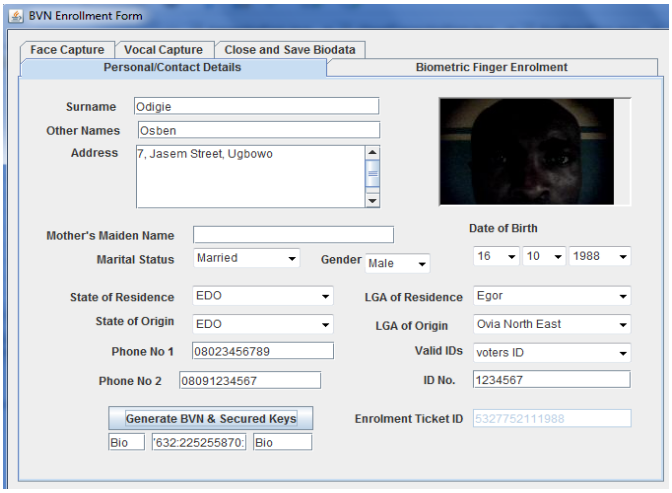

Figure 4: *Personal Data Template*

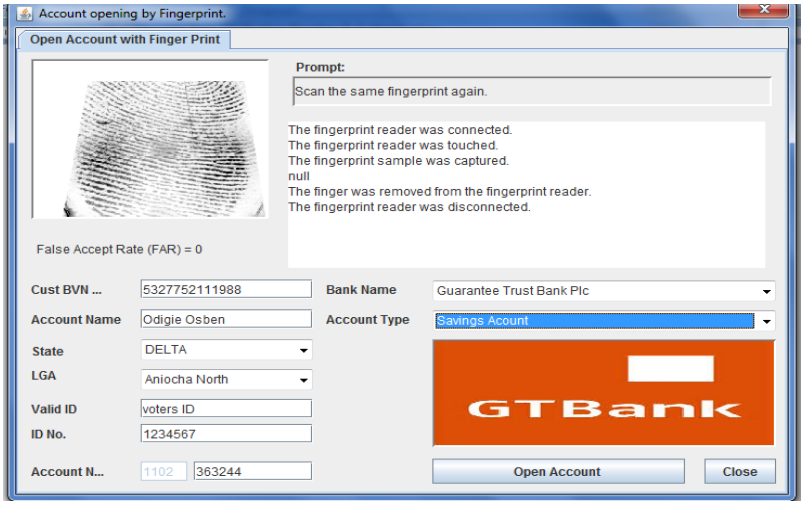

Figure 5: Open account using Biometric features (finger print)

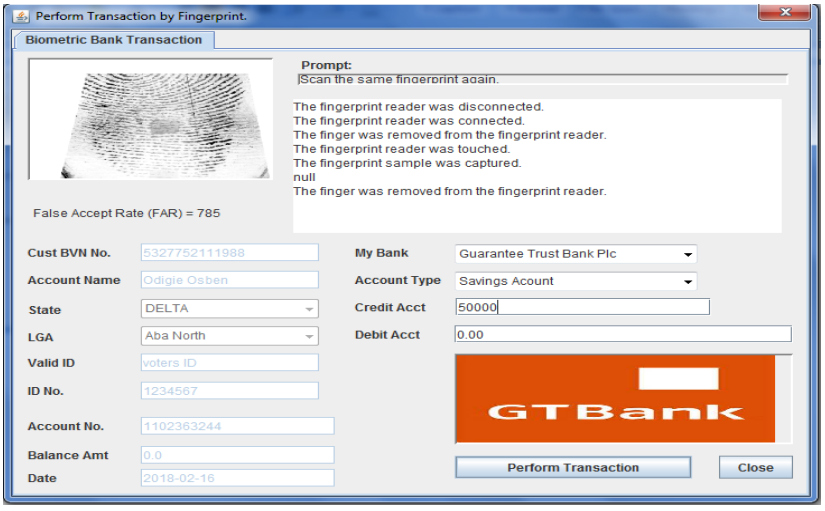

Figure 6: *Perform Bank Transaction by Biometric (finger print)*

5. Conclusion

In this study we examined the benefits of biometric and cryptosystems to the financial institutions. Also, the vulnerability of biometric data via internet platform was discussed and the gains of securing BVN enrolment data and implementing secured transaction using cryptographic techniques were mentioned. It was observed that securing biometric data will further enhance securing financial transactions. BVN initiative was quite amazing but relying on BVN alone might make the system vulnerable to intrusion attacks, phishing and hackers. The system designed and implemented was very robust and interactive and provides a more secured, reliable and precise platform that will address some of the shortcomings militating the effective implementation of secured financial transactions in countries who have adopted online banking and e-transaction system. The complications in ensuring all account holders in various banks irrespective of their location to link their BVN enrolment to accounts were addressed by combining innovative technologies procedures and systems of this magnitude. It was recommended that such intelligent system will help secure

BVN enrolment of financial institution customers within and in the Diaspora and permit transactions using existing financial platforms.

References

[1] Al-Slamy, N. M. (2008), E-commerce security, *Intl. J. Comp. Sci. Network Secur.*, 8(5), 340-344.

[2] Kirti, S. (2013), E-commerce security – A life cycle Approach, *Intl. J. Latest Trends Engr. Technol*., 2(3), 85-94.

[3] Jeberson, W., Gurmit, S., Sahu, G. (2011), Analysis of Security Measures Implemented on G2C Online Payment Systems in India, *Intl. J. Comp. Sci. Inform. Technol.*, 1(1), 19-27.

[4] Moftah, A., Abdullah, S., Hawed, H. (2012), Challenges of Security, Protection and Trust on E-commerce: A case of Online Purchasing in Libya, *Intl. J. Adv. Res. Comp. Commun. Engr.*, 1(3), 141-144.

[5] Rane, P., Meshram, B. (2012), Transaction Security for E-commerce Application, *Intl. J. Electron. Comp. Sci. Engr.*, 1(3), 1720-1726.

[6] Chijioke, N. (2015), Nigeria: BVN-The issues and rationale. http://allafrica.com/stories/201502251343.html , accessed 19 November 2016.

[7] Nwannenna, C. (2015), Design and Development of a Multi-Modal Biometrics System with De-duplication functionaity, Information Technology for Inclusive Development, in: *25th National Conference Proceedings of Nigeria Computer Society*, pp. 186-192, Abuja, Nigeria.

[8] Jain, A., Nandakumar, K., & Nagar, A. (2008), Biometric template Security, *EURASIP Journal on Advances in signal processing*, Special issues on biometric. doi:10.1155/2008/579416 .

[9] Fatokun, A. (2016), *Re:Clarification on Accounts with BVN Related Issues*, Circular issued by Central Bank of Nigeria, Abuja to All Deposit Money Banks (DMBs) in Nigeria. https://www.cbn.gov.ng/out/2016/bpsd/bvn%20issues%20circular.pdf , accessed 7 Oct 2017.

[10] Shirazi, M., & Soroor, J. (2007), An intelligent agent-based architecture for strategic information system applications, *Knowledge-Based Systems*, 20(8), 726-735.

[11] Gowda, R. (2013), Role of Software Agents in E-Commerce, *Intl. J. Comp. Engr. Res.*, 3(3), 246-251.

[12] Raju, B., Anjana, J., Gulfishan, F., & Jyoti, B. (2010), The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology, *Intl. J. Comp. Sci. Inform. Secur.*, 8(1), 307-312.

[13] Rashad, Y., & Noor, A. (2011), Security and Privacy Issues as a Potential Risk for Further E-commerce Development, *Conference on Information Communication and Management – IPCSIT 16.*

[14] Seyyed, M., Fariba, G., & Reza, Z. (2011). Study of Security Issues on Traditional and New Generation of E-commerce Model, *International Conference on Software and Computer Applications-IPCSIT 9*, pp. 113-117.

[15] O'Raghallaigh, E. (2010), *Major Security Issues in E - Commerce*, http://webscience.ie/docs/Webscience Accessed 28 January, 2017.

[16] Marchany, R.C. Tront, J.G. (2002), E-Commerce Security Issues, in: *Proceedings of the 35th Hawaii International Conference on System Sciences*, pp. 2500-2508, Hawai.

[17] Niranjanamurthy, M., Dharmendra, C. (2013), The study of E-Commerce Security Issues and Solutions, *Intl. J. Adv. Res. Comp. Commun. Engr.*, 2(7), 1-12.

[18] Bolt, M. (2010), *Privasy-Invasion Software*, Blekings Institute of Technology. Sweden.

[19] Shah, R., Hossin, A., & Khan, A. (2016), Intelligent Phishing Possibility Detector, *Intl. J. Comp. Appl.*, 148(7), 4-8.

[20] Shazia, Y., Khalid, H., Rashid, J. (2012), Cryptography Based E-Commerce Security: A Review, *Intl. J. Comp. Sci. Issues*, 9(2), 132-137.

[21] Ayo, C., Ukpere, W. (2010), Design of a Secure Unified E-Payment System in Nigeria: A Case Study, *Afr. J. Bus. Manag.*, 4(9), 1753-1760.

[22] Asakpa, S., Alese, B., Adewale, O., Adetunnmbi, A. (2015), Secret Sharing scheme for securing Biometric Template. Information Technology for National Saftey and Securing, in: *26th National Conference Proceedings of Nigeria Computer Society*, pp. 1-9, Akure, Nigeria

[23] Revenkar, P., Anjum, A., Gandhare, W. (2010), Secure Iris Authentification using Visual Cryptography, *Intl. J. Comp. Sci. Inform. Secur.*, 7(3), 217-221.

[24] Osuagwu, E. (2008), *Software Engineering, A Pragmatic and Technical Perspective*, Olliverson Industrial Publishing House, Owerri, Nigeria.