Enhanced Modified Security Framework for Nigeria Cashless E-payment System

Fidelis C. Obodoeze
Dept. of Computer Science Renaissance University, Agbani, Enugu, Nigeria

Francis A. Okoye
Dept. of Computer Science & Engr. Enugu State University of Science & Technology (ESUT) Enugu, Nigeria

Samuel C. Asogwa
Dept. of Computer Science Michael Okpara University of Agriculture Umudike, Nigeria

Frank E. Ozioko
Dept. of Computer &Information Science Enugu State University of Science & Technology (ESUT) Enugu, Nigeria

Calister N. Mba
Dept. of Computer Engr. Caritas University Amorji-Nike, Enugu,Nigeria

***Abstract*—In January 2012, the Nigeria Apex Bank, Central Bank of Nigeria (CBN) rolled out guidelines for the transition of Nigeria's mainly cash-based economy and payment system to cashless and electronic payment (e-payment) system ending over 50 years of mainly cash-based operated economy and payment system. This announcement elicited mixed reactions firstly excitement due to the enormous benefits this transition will impact on Nigeria economy and at the same time elicited panic due to unpreparedness of the economy to transit successfully to electronic payment in a system hitherto filled with bobby trap of security challenges. Ten months later after the introduction of the policy, only a handful of the major stakeholders are fully compliant mainly because of the complexity and the high prohibitive cost of implementation of CBN adopted security framework, the Payment Card Industry Data Security Standard (PCI DSS). This paper surveys the security challenges facing the full implementation of the cashless epayment policy of Nigeria and at the end introduced an enhanced modified security framework for Nigeria's cashless economy that may be easier and cheaper to implement by the majority of the stakeholders after studying the loopholes in the current Nigeria epayment system models.**

Keywords-Cashless economy; electronic payment security; CBN; Nigeria;PoS; ATM; Bank Server; PCI DSS.

I. INTRODUCTION

In January 2012, Central Bank of Nigeria (CBN), the Nigerian apex bank rolled out guidelines for the switching of Nigeria's payment system which was hitherto largely cash-based to cashless and electronic payment system. The pilot test of this transition started in Nigeria commercial capital city, Lagos, to test run the workability of the project. By introducing this cashless epayment system in Nigeria, CBN aimed at reducing the amount of physical cash circulating in the economy and encouraging more electronic-based transactions [1].

Nine months into the pilot 'Cashless Lagos Scheme', security concerns have emerged. With Nigeria gradually transiting from cash to an electronic based economy, by virtue of the implementation of the Central Bank of Nigeria's (CBN) cashless policy, cyber criminals and hackers in the country who hitherto attacked businesses and individuals across the Atlantic have started re-directing their energies towards exploiting possible loopholes in the electronic payment system in order to perpetuate fraud [2]. Analysts have warned financial institutions and other stakeholders in the electronic payment industry to step up investments in security of electronic transactions, or risk been overwhelmed by the spate of sophisticated cyber-attacks that would soon arise as a result of the sheer volume of financial transactions online [3]. According to a report from Symantec's latest Internet Security Threat, Nigeria has moved six positions up the ladder, to occupy the 59th position globally, amongst countries with greatest Internet Security threat. Industry analysts have expressed concerns about Nigeria's rising cybercrime profile. Accordingly, the apex bank, CBN, had directed all players in the banking and electronic payment sector to speedily attain Payment Card Industry Data Security Standard (PCI DSS) compliance which is the security standard adopted by the CBN for Nigeria cashless epayment system. This, according to the apex bank, is to ensure that card users in the country would continue to experience enhanced payment data security. But up till now, out of the 21 banks currently operating in Nigeria, only Access Bank Plc has achieved compliance [4]. It was discovered in [4] that only Interswitch and ETransactPlc among switching services providers, have achieved compliance; ValuCard being the only third-party card processing firm to achieve full compliance. The major reason for the massive non-compliance to the CBN's recommended security standard, the PCI DSS, is not far-fetched. It has been discovered that the major reasons for massive non-compliance by the major stakeholders to the PCI DSS are firstly because of PCI DSS high cost of implementation and maintenance, secondly because of its implementation complexity.

For instance, it will cost a business stakeholder (a merchant) in Nigeria about $20,000 to fully implement PCI DSS and additional $1000 per year for payment of software update on Electronic Point of Sale (EPOS) [5]. Also the merchant has to bear additional cost of periodic system vulnerability and compliance scan by paying a third-party firm appointed by PCI DSS operators to ensure full compliance to PCI DSS. This cost is highly prohibitive in Nigeria; in fact only commercial banks and perhaps the electronic payment switching companies can afford this cost. This explains why only Access Bank Plc and payment switching companies Interswitch, ETransact and card provider ValuCard have become fully compliant. An average Nigeria merchant does not have up to $20,000 as its total operating capital (TOC). Apart

from the cost of implementation and maintenance, it equally costs additional expenses for a merchant or any other stakeholder to send his/her staff for training on how to implement PCI DSS.

Another major reason for non-compliance to PCI DSS in Nigeria is the issue of complexity of implementation. The PCI DSS was not designed with simplicity and user-friendliness in mind. The full implementation of PCI DSS is very complex and complicated and at such very difficult to learn and grasp by IT security professionals. Because of this reason, it costs epayment stakeholders a lot of fund and time to train their IT Desk and security officers to learn the PCI DSS implementation.

Apart from these reasons, there is equally much suspicion about the real intentions of the PCI DSS originators- the credit card companies (the VisaCard, eBay, PayPal and MasterCard). It was reported that many court cases have arisen as a result of imposition of fines/penalties on merchants by the PCI DSS originators in the USA. It was argued that fines were imposed by the originators on merchants even where there was not clear case of fraud, that the real intentions of the PCI DSS originators is to make profits from fines they impose on merchants[4].

II. Current Epayment Architecture In Nigeria

The following stakeholders are currently involved in the Nigeria cashless and electronic payment (Epayment) system introduced by the apex bank CBN:

- *Consumer or customer,*
- *Switching Companies (Epayment processors e.g. Interswitch and ETransact)*
- *Card processing companies (e.g. ValuCard)*
- *Merchants or retailers,*
- *Mobile Money providers (Mobile Payment Providers),*
- *Commercial Banks and*
- *The financial regulatory agency (the Central Bank of Nigeria)*

According to [6,7], electronic payment is possible for business transactions involving:

- *Business-to-business (B2B) and*
- *Business-to-Customer (B2C).*

Business-to-business (B2B) transactions mostly involves Bank-to-Bank electronic fund transfer (ETF) and Electronic Cheque Clearing System (ECCS) while Business-to-Customer (B2C) transactions involves the use of payment terminals by consumers/customers such as Point-of-Sale(PoS) terminals, Mobile payment terminals, Mobile/Internet Banking terminal, Automated Teller Machine (ATM) terminal and Online Merchant portals/ecommerce shops.

Figure 1 depicts the illustration of Nigeria current electronic payment architecture. The electronic payment switching in all the cases as depicted in Figure 1 are handled by the switching companies (epayment processors) such as Interswitch and ETransact while the Mobile payment providers, authorized by CBN, handle electronic payment such as ePurse, eMoney, Pocket Money etc. provisioning using the Telecommunication platforms (GSM) and electronic switching by the switching companies. The Nigerian electronic payment architecture uses about five (5) different models of payment transactions as depicted in Figures 2 to 6.

Figure 1. Nigeria's current electronic payment architecture

To solve the problems of security challenges and vulnerabilities associated with electronic transactions and payments, the epayment models of an indigenous economy must be studied and understood [8]. In Nigeria cashless electronic payment system, the epayment present electronic payment models are outlined below:

- *Consumer to Merchant epayment model using PoS terminal (owned by the merchant) and bank issued credit/debit cards (owned by the consumer),*
- *Consumer's ATM payment model using the bank issued credit/debit cards and ATM terminal installed in banks' premises to pay customers,*
- *Consumer to Merchant epayment model using online portals and bank issued credit/debit cards (owned by consumers),*
- *Bank to Bank Electronic Payment System model using Electronic Fund Transfer (ETF) and Electronic Cheque Clearing system(ECCS), and*
- *Mobile Payment/Internet Banking model using consumer's mobile equipment, third-party epayment software and Bank's Transaction Server to pay consumers using telecommunication gateway and switching platform.*

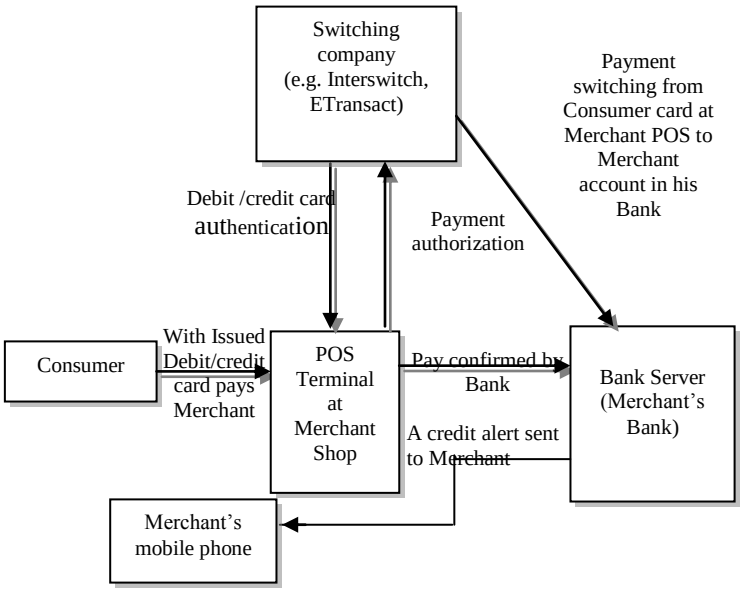

Figure2.Epayment model using Point Of Sale (PoS) terminal to pay merchant by consumer using bank issued debit/credit cards interconnecting switching platform and Bank Server

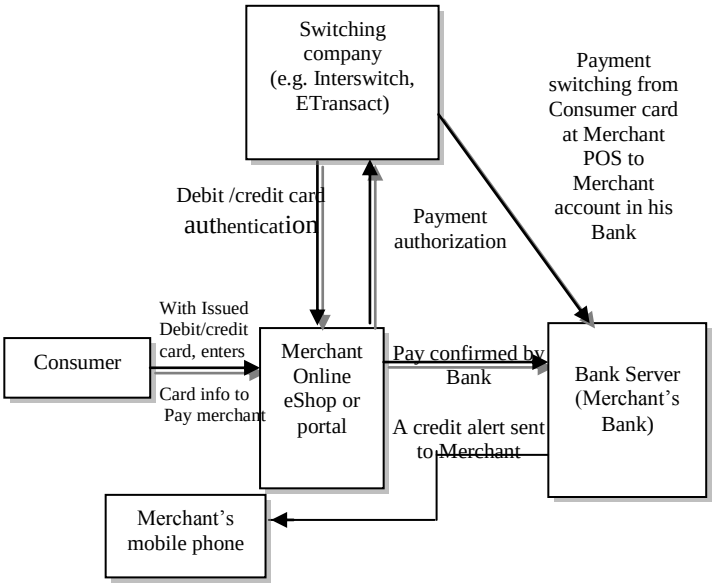

Figure 4.Epayment model using bank issued credit/debit card by consumer to pay merchant at online eCommerce shop or portal interconnecting switching platform and Bank Server

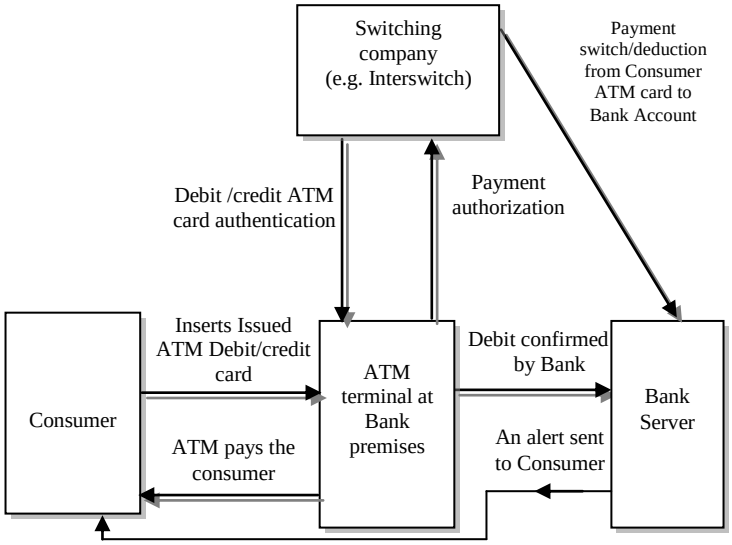

Figure 3.Epayment model using ATM terminal to pay consumer/customer having credit/debit card by Banks connecting switching company and Bank Server

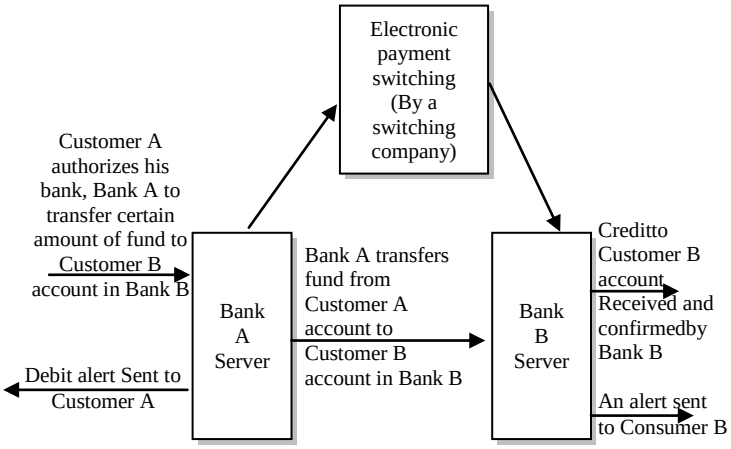

Figure 5.Epayment model involving Bank to Bank Electronic Fund Transfer (ETF) for two businesses to pay each other connecting a switching platform and two Bank Servers

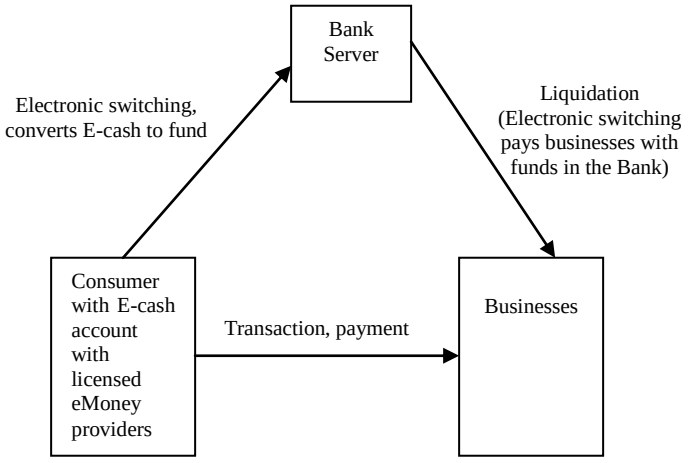

Figure 6.Epayment model using Mobile payment platform for a consumer(with eMoney account with E-Money provider) to pay a business or businesses with E-cash converted to funds in the Bank using electronic switching to switch E-cash to fund in the Bank(liquidation)

III. Security Challenges Affecting Nigeria Electronic Payment System

The following security challenges have been identified as the key issues affecting the successful implementation of electronic payment systems in Nigeria's cashless economy:

- *Identity threats,*
- *Fraud committed by inside-outside collusion by fraudsters and corrupt banks' employee in order to defraud the bank or their customers,*
- *Forgery,*
- *Armed robbers blowing up ATM terminals installed in Bank premises with explosives and dynamites in order to cart away physical cash,*
- *Cloning of credit and debit cards of bank customers' cards by hackers through various social engineering tactics to unsuspecting Nigerians to reveal their cards pin ids to enable the hackers withdraw funds from customers' bank accounts using ATM terminals.*
- *Online criminals and hackers exploiting security vulnerabilities in merchant websites to receive products or airline tickets for free or at reduced prices without paying a dime.*
- *Customers' privacy invasion and threats.*
- *Dearth of technical and security awareness and knowledge by most users which make them gullible to the antics of epayment and online fraudsters.*
- *Lack of legal or legislative bill to sanction offenders or epayment criminals so as to serve as deterrent.*

The security challenges identified above fall into three categories of security challenges: physical, data/information and operational security challenges. Any security system designed for Nigeria's epayment system must take into full account of these security vulnerabilities and challenges identified above as well as the loopholes identified in the current Nigeria epayment security models in order to be successful.

A. E-Commerce Security Elements

For a security system said to be considered adequate or successful for any electronic payment system, it must satisfy the following basic e-commerce security properties:

- *Data confidentiality or privacy or secrecy,*
- *Data integrity,*
- *Non-repudiation,*
- *Data authentication and*
- *Reliability*

Encryption and decryption provides the confidentiality or secrecy of data communication, but intruders still can tap transmission media and falsify the message [9]. Also reneging and forgery from the two parties of the transaction may exist. Data authentication and electronic signatures are applications of encryption systems that provide verification of message integrity, data origin authentication, and protection against repudiation. Data authentication is a procedure that allows parties to verify that the received messages are authentic, i.e., they are genuine and have come from their alleged sources. Before the message is sent, it is fed into an authentication code generator, which creates a code that accompanies the message to the receiver. Upon receipt of the message, the receiver performs an authentication code calculation and obtains another authentication code. If the message has not been altered, the same authentication code will be generated. Multiple algorithms can be used for authentication code generation. If there are no authentication keys, some kind of hashing function can be used, but this method suffers from collision problems, i.e., a falsified message generates the same authentication code with the original message. Encryption/decryption algorithms are often used for authentication. When the AES 128 bit cipher algorithm is used, the generated authentication code is called an electronic signature because it is from a proprietary private key and no one else can falsify his/her signature. Reliability in eCommerce and epayment system is to prevent computer failure, procedural errors and transmission errors. Hardware failures, software errors, computer viruses and natural disasters can result to failure of epayment systems and result to loss of reliability and consequent litigations [9].

IV. System Analysis Of Related Frameworks

The following section describes the system analysis of two types of related epayment security frameworks or standards- the epayment system without security and Payment Card Industry Data Security Standard(PCI DSS) adopted by the Nigeria apex Bank, the CBN.

A. Epayment Framework with no security

This electronic payment framework is assumed to have no form of security and therefore cannot be deployed in a mission-critical environment such as obtainable in Nigeria cashless electronic payment system where there are a lot security vulnerabilities and breaches on daily basis.

Shortcomings of this Epayment framework are as follows:

1) *It is the worst case because of lack of physical, operational and data security for all forms of epayment transactions. Transaction data, consumers' card data and personal information are not protected at all.*
2) *It allows hackers and fraudsters both within and outside the payment system with little or no effort to commit all sorts of cyber breaches and attacks and steal customers' funds.*
3) *It creates room for all forms of litigation since there will much loss of privacy and loss of hard-earned funds.*
4) *It is not useful since it cannot be deployed in any sensible epayment system.*

B. PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards [10]. It was originated by the team from the card companies- MasterCard, VisaCard, PayPal and Microsoft in 2009 to address information security challenges arising from use of credit, debit and pre-paid cards on payment terminals such as ATM, PoS, Online.

Shortcomings of PCI DSSare as follows:

1) *It provides data security but very expensive to implement by an ordinary stakeholder such as merchant.*
2) *It is very complex and complicated to implement and not user-friendly. It therefore costs a lot of money and time to train IT staff to master it.*
3) *Because of fines and penalties imposed by the originators on defaulting stakeholders, a lot of suspicions are created on the real intentions for the introduction of the security framework thereby casting aspersions on the objectives of the framework.*

V. THE PROPOSED FRAMEWORK

In this section we describe a framework for enhancing the security for the cashless electronic payment system of Nigeria that simplifies the implementation and reduces the total cost of ownership (TOC) especially for the merchants and consumers (the majority of the epayment stakeholders). In Nigeria, the merchants and the consumers form the majority of the electronic payment stakeholders and in order to ensure full security compliance, these stakeholders must be accommodated; the total cost of ownership (TCO) must be reduced for the merchant while user education on security compliance must be transferred to the consumers at little or no cost to them. At the same time, complexity of implementation must be reduced and the security system made simpler in order to attract full compliance by all the stakeholders.

Our proposed security framework transfers the bulk of the burden of cost of compliance (COC) and cost of ownership (TCO) to the bigger and richer epayment stakeholders such as commercial banks, switching companies, card processing firms and mobile money providers who will at the long run recoup their investments.Security vulnerability software can be provided by the switching company for other stakeholders to enable them carry out regular vulnerability system scan. The license for this software should be one-time life license updateable for a minimal fee per annum.

After thoroughly studying the current Nigerian epayment architecture (Figure 1) and the epayment models as depicted in Figures 2 to 6, we discovered that virtually all electronic payment transactions will require electronic payment switching, so the electronic payment switching companies such as Interswitch and ETransact have to bear bulk of the cost of providing data security to cover the merchants and consumers. Nevertheless, every stakeholder has a role to play to ensure full compliance of data, operational and physical security of epayment infrastructure and networks.

Our proposed framework suggests the following guidelines and standards for various categories of electronic payment stakeholders:

- *Security compliance guidelines for the consumers (on how to use credit and debit cards on payment terminals).*
- *Security compliance guidelines for the merchant (using Point-Of-Sale (PoS) and Online Ecommerce Portal).*
- *Security compliance guidelines for the Switching firms and card processing companies.*
- *Security compliance guidelines for the commercial banks.*
- *Security compliance guidelines for the Mobile Payment providers.*
- *Security compliance guidelines for the government/ regulatory agency*

A. Security Compliance Guidelines for the Consumers

The consumer or customer is the least of the epayment stakeholders in terms of responsibilities of security compliance. His duties are merely to protect his credit/debit card pins from being exposed and stolen; also to report to his bank or card provider immediately or in the event of loss or misplacement of his credit/debit card so that the account will be blocked to protect the money in his account from being stolen.

Equally, the consumer should reconcile with his bank for very transaction via debit/credit alert confirmation in his mobile phone.

B. Security Compliance Guidelines for the Merchant stakeholder

The merchant deals directly with the consumers/customers. He sells goods or services to the consumer and the consumer pays him electronically via the epayment channels or terminals such as PoS, Mobile device, online eCommerce shop or portal as depicted in Figure 7. The primary concern of the merchant is for the consumer to pay him through any of the available epayment channels and his bank account successfully credited and he obtains a credit confirmation alert in his mobile phone from his bank before he can allow the consumer or customer to go away with his goods or services.

The security requirements for the merchant using the Point of Sale (PoS) channel are as follows:

1) *To provide physical security for the PoS equipment so that robbers will not cart it away.*
2) *To install the PoS equipment in such a way as to prevent tampering by would-be-criminals either from outside or within his shop.*
3) *To capture the biometric feature of each customer (facial) using camera or close circuit television (CCTV) in case of fraud so as to identify the culprit by law enforcement agents.*
4) *To reconcile his account status and balance with hisbanker via credit alter confirmation to his mobile phone to ensure that his account is credited before allowing the consumer/customer to go away with the goods.*

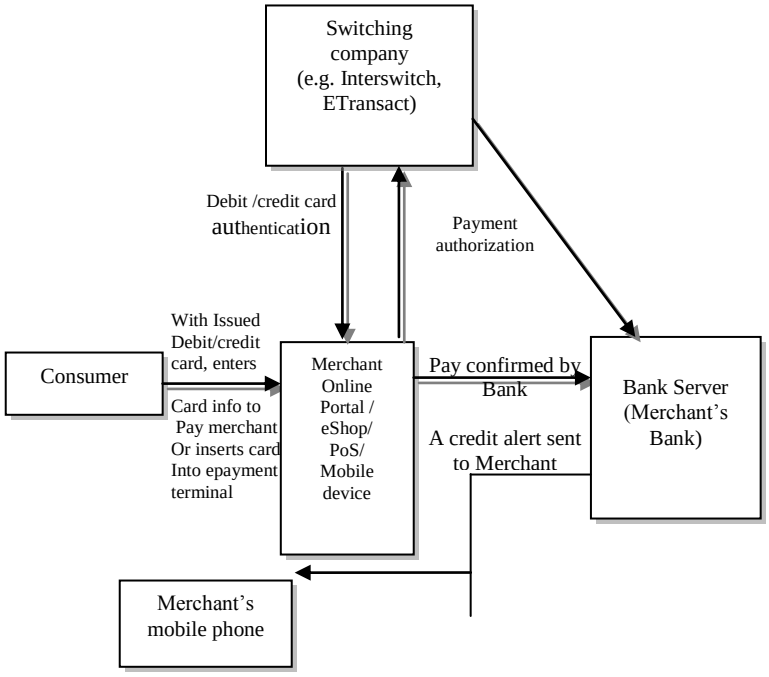

Figure 7.Merchant-customer epayment model using online eCommerce Portal, PoS and Mobile payment terminals

For the merchant-customer epayment model depicted in Figure 7, security vulnerability lies on the interfaces between the epayment terminals and the merchant's Bank Server. It is therefore the duties of the epayment switching companies to provide cryptographic data security through encryption and decryption and other additional data security such as digital signatures and hashing for every epayment transaction.

For the merchant-consumer model using online eCommerce shop or portal the merchant owes full responsibility to secure his online portal or shop to provide data security. The suggested guidelines for merchants operating online eCommerce portal or shops are listed as follows:

1) *He has to obtain certificate authority(CA) to verifybuyer/consumer's identities before selling,*
2) *He has to provide point-to-point encryption for everytransaction through the provision of secure socket layer (SSL) on http interface (i.e. https), secure shell(SH),Internet Protocol Security(IPSec) etc to ensure data confidentiality and hashing function to ensure dataintegrity.*

C. Security Compliance Guidelines for the Switching companies

The epayment switching companies play the major role in the entire electronic payment system in Nigeria. The switching firms conduct all debit/credit transaction switching from consumer credit/debit cards on epayment terminals such as ATM, PoS, mobile devices, online ecommerce portals to the authorized bank accounts of the merchants or electronic switching from a business account in a bank to another business account in another bank.

The channels or interfaces in the electronic switching, most of the time being wireless and wired Local (LAN) or Wide Area Networks (WAN) are vulnerable to all sorts of data and operational security attacks [11]. So the switching firms have to provide full compliance and protection for the data and operational capacity of all the epayment transactions and only charge other stakeholders minimal fees per annum.

The following security guidelines are suggested for the switching companies. They should:

- *Provide end-to-end data encryption using strong cryptographic cipher engines (AES 128 bit) is suggested to ensure data confidentiality.*
- *Provide strong user authentication to provide data confidentiality and integrity.*
- *Provide Message Authentication Codes (MAC) or hashing functions to provide data integrity for all the epayment transactions.*
- *Perform vulnerability and compliance system scan on all interconnected stakeholders on their network on a regular basis (maybe quarterly) at a minimal fee to the stakeholders.*

The channels or interfaces in the electronic switching, most of the time being wireless and wired Local (LAN) or Wide Area Networks (WAN) are vulnerable to all sorts of data and operational security attacks [11]. So the switching firms have to provide full compliance and protection for the data and operational capacity of all the epayment transactions and only charge other stakeholders minimal fees per annum.

D. Security Compliance Guidelines for the Commercial Banks

Commercial banks have a lot of customers that deposit their funds with them. They also deal directly with merchants who maintain business accounts with them. The epayment switching firms switch payment electronically from various epayment terminals such as ATM, PoS, Online Ecommerce portals, Mobile devices once the consumers authorizes payment using their credit/card cards.

Also switching firms switch payment electronically from one business account in one bank to another business account in another bank. All these epayment transaction switching end up in the banks' transaction servers which work 24 hours a day, 7 days a week. It is therefore the duties of both the commercial banks and switching firms to provide security to protect the Transaction server and the epayment interfaces from being security breached.

The following security compliance guidelines are suggested for the commercial banks to ensure compliance:

- *Banks should provide physical security of ATM terminals to ensure availability of ATM terminal any time and to protect the ATM terminal from being attacked by armed robbers.*
- *Banks should provide end-to-end encryption ofall transaction data from the TransactionServer to all epayment terminals via electronicpayment switching gateways. Powerful encryption engine such as AES (128 bit) is hereby suggested. This will provide data confidentiality and privacy.*
- *Banks should provide full authentication of their customers at ATM payment terminals using simple username and pin logins as well as additional biometric authentication mechanisms to capture customers' biometric feature such as photograph.*
- *Banks' core Banking solutions should be fully protected with hash functions or Message Authentication Codes (MAC) to protect the payment data from being compromised by fraudsters either from the within or outside. This will provide data integrity.*
- *Additionally, banks should ensure that all customers are sent instant SMS transaction alert or confirmation through their mobile phones to enable account reconciliation.*

The following flowchart (Figure 8) depicts the proposed enhanced modified security framework for the protection of transaction data from a consumer (paying with his debit/credit card) to merchant account in the bank using electronic switching platforms.

E. Security Compliance Guidelines for the government/ regulatory agency

The regulatory agency, the Central Bank of Nigeria (CBN) can spearhead the passing into law security compliance and liability bill that will force every epayment stakeholder to become compliance and to accept responsibility in the event of any financial loss to a business or a consumer as a result of lack of security compliance. The legislative bill should equally spell out who should pay who in the event of security liability. Also penalties should be clearly spelled out for would-be-criminals and fraudsters using long jail term sentences to discourage potential financial criminals.

CBN should also educate the users (consumers) and the other stakeholders on the need to be security compliance and how to be.

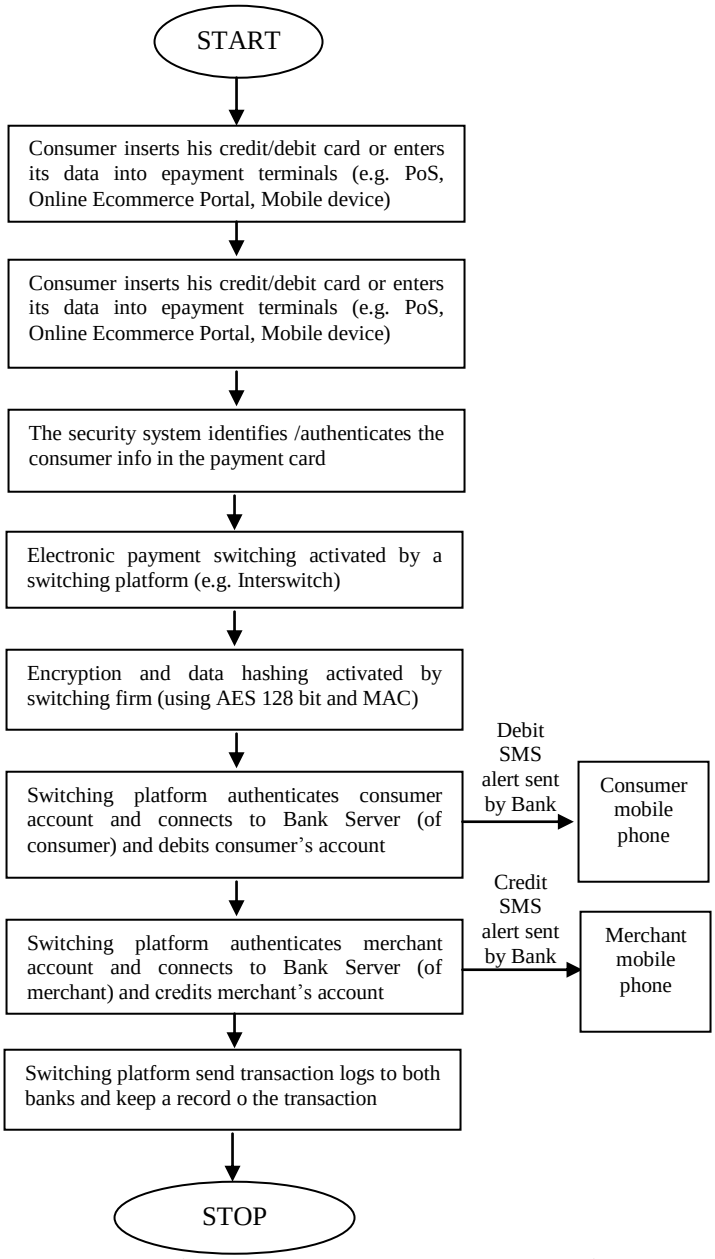

Figure 8.System flowchart depicting the proposed enhanced modified data security framework for Nigeria cashless epayment system from consumer to merchant accounts in the banks

VI. CONCLUSION

In this paper, the myriads of security as well technical and legal challenges facing the successful transition from cash-based to cashless electronic payment of Nigeria epayment system have been identified. The investigations have shown that the security models of an epayment system must be studied and understood before a data security framework is adopted for it. This study have revealed why the CBN adopted data security framework, the PCI DSS, failed to attract wide acceptability and compliance in Nigeria's epayment system. Issues of complexity in implementation and high prohibitive cost of implementation as well as lack of legal framework have been identified to be the major bottlenecks towards the compliance to the PCI DSS by major epayment stakeholders in Nigeria.

The result of the findings from this study shows that for full compliance to any adopted data security framework for any epayment system, cost and simplicity of implementations must be seriously considered.

In this paper, we introduced a simpler and less costly epayment security framework/standards which we believe will provide enhanced data and operational security as well reduce cost and complexity of implementation by the majority of the stakeholders in Nigeria cashless economy. By reducing the complexity and cost of implementation as identified in PCI DSS, the majority of the epayment stakeholders such as consumers and merchants will easily and willingly become security compliant.

The Nigerian apex bank, CBN, should seriously look inwards toward encouraging the major stakeholders such as consumers and merchants to comply with data security guidelines by adopting framework that will lower their overall cost of compliance (COC) and total cost of ownership (TCO)and as well reduce complexity of implementations considerably. It is in this regard we sincerely hope that our contributions will help in no small measure in providing the roadmap for enhanced, simpler and cheaper security standards and framework for the new Nigeria cashless electronic payment system.

REFERENCES

[1] Central Bank of Nigeria, "Further Clarifications on Cashless Lagos Project". Retrieved on 9thSeptember, 2012from http://www.cenbank.org/cashless.

[2] Mynaij.com. "Cashless Banking: Cyber Criminals Now Focus on Nigeria". Retrieved on 6thAugust, 2012 from http://news.naij.com/business_and_economy/.

[3] Mynaij.com. "Cashless Banking: Cyber Criminals Now Focus on Nigeria".Retrieved on 8thAugust, 2012 from http://news.naij.com/cashless_epayment_in_Nigeria/.

[4] Businessdayonline."Cyber Security and Nigeria's Cashless Initiative", Retrieved on 9thSeptember, 2012 from http://www.businessdayonline.com/NG/index.php/analysis/editorial/4329/cyber-security-and-nigerias-cashless-initiative.

[5] Wikipedia, "Payment Card Industry Data Security Standard". Retrieved on 9th September, 2012 from http://www.wikipedia.com/wiki/Payment-Card-Industry-Security-Standards.htm.

[6] S.G.P. Muniappa and S.A.Gosh, "Report on Internet Banking: A White paper on Indian Internet Banking", p. 12-14.

[7] C.K. Ayo and W.I. Ukpere, "Design of a secure unified epayment system in Nigeria: A Case Study", African Journal of Business Management, vol.4 (9), pp. 1753, August 2010.

[8] Y. Jing, "On-line Payment and Security of Ecommerce", Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA '09) China, May 22-24, 2009, pp. 546, 2009.

[9] Dan Zhu, "Security Control in Inter-Bank Fund Transfer", Journal of Electronic Commerce Research, vol.3, No.1, pp. 46-48, 2002.

[10] Wikipedia, "Payment Card Industry Data Security Standard". Retrieved on18thAugust, 2012 from http://www.wikipedia.com/wiki/Payment-Card_Industry_Data_Security_Standard.htm.

[11] PCI Security Standards Council, "Protecting Telephone-based Payment Card data", pp.1.

AUTHORS PROFILE

Engr. Fidelis Chukwujekwu Obodoeze is a Ph.D research scholar in the Department of Electronic and Computer Engineering NnamdiAzikiwe University Awka, Nigeria. He is currently lecturing at the Department of Computer Science Renaissance University Enugu, Nigeria. His research interests include Cryptography, Wireless Telecommunication security, Wireless Sensor Networks, Information and Data security, Artificial Intelligence and Industrial Automation. He had his Masters (MEngr.) in Control Systems and Computer Engineering at Nnamdi Azikiwe University Awka, Nigeria in 2010 and Bachelor of Science degree (B.Sc.) in Computer Engineering at ObafemiAwolowo University Ile-Ife, Nigeria in 2000.All correspondence to email: fidelisobodoeze@gmail.com

Dr. Francis A. Okoye is a lecturer and Head Department of Computer Science and Engineering Enugu State University of Science and technology (ESUT), Nigeria. He had his Ph.Din Computer Science in 2008 at Ebonyi State University Abakaliki; MSc. and BEng. in Computer Science and Engineering at Enugu State University of Science and Technology (ESUT), Nigeria in 2001 and 1996 respectively. Email: francisced@esut.edu.ng

Mr. Samuel Chibuzor Asogwa is a Ph.D research scholar in the Department of Computer Science Nnamdi Azikiwe University Awka, Nigeria. He is currently lecturing at the Department of Computer Science Michael Okpara University of Agriculture Umudike, Nigeria. He had his Masters (MSc.) in Computer Science at Ebonyi State University Abakaliki, Nigeria in 2011 and Bachelor of Engineering (BEng.) in Computer Science and Engineering at Enugu State University of Science and Technology (ESUT), Nigeria in 1999.Email:sasogwa@gmail.com

Mr. Frank EkeneOzioko is the Director of ICT Unit and Lecturer Department of Computer and Information Science, Enugu State University of Science and Technology (ESUT), Nigeria.Email: ekene.ozioko@esut.edu.ng

Engr. Calista Nnenna Mbah is a Lecturer and former Head, Department of Computer Engineering, Caritas University Enugu, Nigeria. She is currently pursuing her Ph.D programme in Computer Science at Nnamdi Azikiwe University Awka, Nigeria. She had her MSc. Computer Science at University of Nigeria Nsukka (UNN) in 2009, Nigeria and B.Eng in Computer Science and Engineering at Enugu State University of Science and Technology (ESUT), Nigeria in 2004.Email: mbacally@yahoo.com