Determining the adoption of e-transaction authentication frameworks in Nigerian Commercial Banks

Chijioke Amaka[1], Agozie Eneh [2], Collins Udanor [*3], Onyesolu M.O[4], Uchenna Nduka[5]

[1,4] Department of Computer Science, Nnamdi Azikiwe University, Anambra State, Nigeria
[2,3]Department of Computer Science, University of Nigeria Nsukka, Enugu State Nigeria
*E-mail: collins.udanor@unn.edu.ng
[5]Department of Statistics, University of Nigeria Nsukka, Enugu State Nigeria

Abstract — The Internet is a network of networks which gives the business user a global reach. Though many users of the Internet are happy surfing the web and interacting with friends on the social media, there is skeptism when it comes to doing financial transactions over an open network like the Internet. Security of e-transactions has continued to be the number one concern of every user of such platform. The Internet offers great opportunities to businesses but at the same time poses great danger. The only assumption that can be made about the Internet is that it does not offer any security whatsoever. In this work the authors through survey and extensive literature sought to know if Nigeria was mature to adopt e-transaction services. Results from the survey obtained from IT managers among 13 top Nigerian banks show that 70 percent of the respondents have knowledge of legal framework for authenticating e-transaction in Nigeria as well as have knowledge of enterprise security policy. While less than 70 percent have knowledge of any disaster recovery plan. SSL and Firewalls were found to be the most popular authentication services in use across these banks.

Keywords: e-transaction security, secure electronic transaction, cryptography, e-banking

I. INTRODUCTION

The digital market place has brought merchants and buyers together in a virtual stage of global village market square where goods, services and money exchange hands in real time without any prior physical acquaintances. The Internet of course has made this possible. Interactions between man and machine or machine to machine over network media has made this a present day reality. However, security of e-transactions has continued to be the number one concern of every user of such platform. Network security professionals are constantly kept on their toes ensuring that every possible hole is blocked from where a malicious user would have gained access. Technologies have been evolving on constant basis to ensure secure e-transactions between merchants and their customers, etc, one of which is the SET.

Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet [1]. With SET, a user is given an *electronic wallet* (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality. IT infrastructures like the computer network, telecommunication tools like the VSAT, fibre optics, secured socket layer (SSL) protocols, firewalls and of course the Internet prepared the ground for the deployment of e-transaction infrastructures. Banks globally have leveraged on these platforms to build e-transaction services such as online or e-banking, electronic fund transfer, online payment systems, as well as e-commerce in conjunction with retail outlets and identity providers. Nigeria like any other country must not be left behind if she hopes to compete in the fast-growing.

Hitherto, Nigeria's economic activities have been largely cash driven, to the extent that over 90% of financial transactions were made by cash [2]. This is largely due to illiteracy, ignorance, inadequate infrastructure and lack of guarantee of security for e-transactions. In line with its mandate, Nigeria's apex bank, the Central Bank of Nigeria (CBN) has introduced various monitory policies that would strengthen the financial system, and cashless policy is one of such policies that is geared towards positioning the country among the top 20 economies in the world by the year 2020 [3]. This policy is to solve the problems of high cost of printing physical cash, monitory instability, excess liquidity, as well as inefficient allocation of resources and a low depth of financial intermediation. This policy has fuelled the drive for E-transactions, which is mostly cashless driven. Apart from online retail shops and e-commerce websites, retail outlets encourage their customers to do cashless transactions on POS terminals by offering some discounts. In this paper we examine the prospects of e-the financial system, and cashless policy is one of such policies that is geared towards positioning the country among the top 20 economies in the world by the year 2020 [3]. This policy is to solve the problems of high cost of printing physical cash, monitory instability, excess liquidity, as well as inefficient allocation of resources and a low depth of financial intermediation. This policy has fuelled the drive for E-transactions, which is mostly cashless driven. Apart from online retail shops and e-commerce websites, retail outlets encourage their customers to do cashless transactions on POS terminals by offering some discounts. In this paper we examine the prospects of e-transactions in Nigeria with its attendant security challenges.

II. Background research

In this section we review some background theories and technologies on the subject, as well as provide a review of related literature.

A. Drivers of e-transaction

The Internet is a network of networks which gives the business user a global reach. The Internet offers great opportunities to business but at the same time poses great danger. The Internet does not offer any security whatsoever. Anybody who has the right tools can enter into any company's computer online and steal information or perform one malicious act or the other. While the Internet is dramatically changing the way business is conducted, security and privacy issues are of deeper concern than ever before [4]. The Internet is basically an insecure communication medium. The only assumption which can safely be made when considering the Internet as a communication medium is that it offers no security whatsoever [5].

The growth of the Internet within the last decade is astronomical. A number of options are now more readily available to deliver the Internet to users. From the era of the ARPANET when the only medium was multi-user terminals to the PC era, and now to handheld devices, the Internet is delivered through Wireless Access Protocols (WAP). The pervasiveness of the Internet is motivated by emerging digital mobile terrestrial services and technologies that are bringing data services to hundreds of millions of users worldwide [5]. Some industrialized countries are already providing 4G mobile terrestrial services. The Internet can now be received on the go, anywhere, anytime. Internet appliances and pervasive computing are reducing the technical requirements for network services and are creating direct relationships between business and consumers [6]. A global electronic economy is being created where changes in one part of the globe affect many other parts [7].

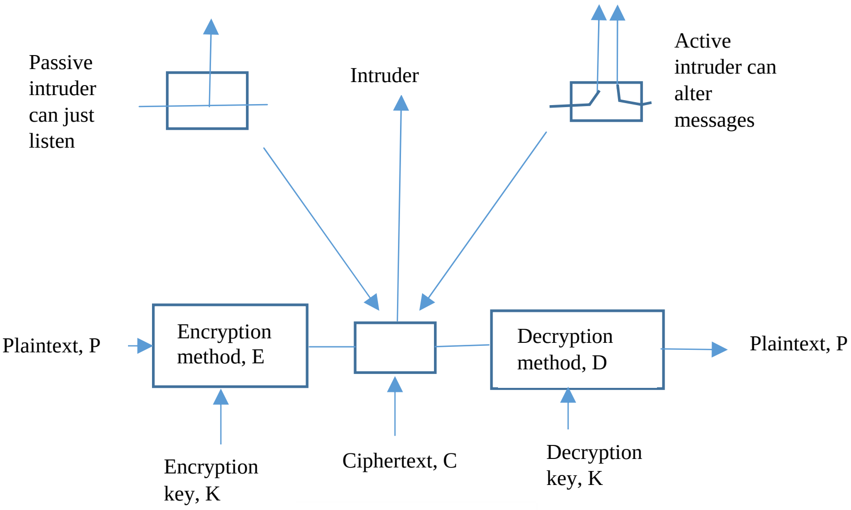
E-business or E-commerce is one of the main forces driving this digital revolution. The core activities of e-commerce are business transactions between two parties or possibly mediated by a third party, a trusted third party as it is called. In fact, the practice conducted by a company before the term e-commerce appears is Electronic Data Interchange (EDI), which is basically electronic transaction via computer networks. While it is creating new business models, and opportunities by giving products and services a global reach, it is also creating new challenges to service providers. The challenges are greater in the developing world where infrastructure is poor and technical knowledge is low, due to low investment in IT education and development, as well as non-availability of power. Despite the enactment of electronic transactions Act 2007 in Sudan [8], finds out many deficiencies, such as poor infrastructure, and lack of skilled and well-trained human resource force in the banking sector and security, which remain the key factors that constrain the applicability of e-banking. The major concern of electronic transactions is how to protect transactions from eavesdroppers (which can steal and modify the information in the transactions) and how to make sure those transactions are authenticated [4].

B. Cryptography as an E-transaction Driver

E-transaction security has come to occupy an increasingly central place in our lives over the past twenty years. This has been a direct result of the enormous increase in the development and use of networked and distributed systems over this period. Financial transactions on the Internet are gaining currency now. Distributed financial transactions even if they are in the simple form of withdrawing money from an ATM, using Point of Sale (PoS) for payment and other banking transactions have become part of many peoples' lives today. Financial institutions such as banks provide their services online. The advancement of communication technologies has also resulted in huge quantities of digital data in the publicly shared network media. This calls for serious need to secure the communication channels. Secure communication depends upon encryption of messages exchanged between communicating parties.

This section explains the cryptographic techniques used in implementing the authentication services deployed in Nigerian banks as discovered from the results of our survey above. The approach of cryptography is a method of securing data in open networks like the internet and assumes the following:

i. It is feasible for each computer in the network to encrypt and decrypt message contents efficiently with arbitrary keys, and that these keys are not readily discoverable by exhaustive search or cryptanalysis. Keys cannot be compromised otherwise the flaws in these systems can be used to subvert the protocol.
ii. That both symmetric and asymmetric encryption algorithms are the basis for the protocol presented.
iii. An intruder can interpose a computer in all communication paths, and thus can alter or copy parts of messages, replay messages or emit false material.
Figure 1 is the graphical illustration of the cryptographic processes.



$$C = E_k(P)...(1)$$

Figure 1: encryption and decryption model

The algorithm is composed of encryption (E) and decryption (D) processes which usually are identical or simply consist of the same steps performed in order. The encryption and decryption is based upon the type of cryptography scheme being employed and some form of key. Encryption process is represented: C = E_k(P) while Decryption process is represented: P = D_k(C), where P = plain text, C = ciphertext, E = the encryption process, D = the decryption process, and K = the key.

With the advances taking place in cryptography, governments, organizations, military units, and some corporate houses started adopting the applications of cryptography. This leads to the drastic development of cryptographic techniques. Cryptography is considered to be one of the fundamental building blocks of computer security [9]. Data can be encoded with the aid of cryptographic techniques (Encryption) in order to ensure that it appears unintelligible to the public or third party and coherent only to the intended receivers of it. Encryption of data is usually accomplished by the combination of plain text data (the input) with a secret key using a particular encryption algorithm. The result (output) is a cipher-text. Unless someone or a computer has the secret key, they cannot convert the cipher-text back to plain text. This encryption methodology is at the core of any of the secure protocols [10]. Although many types of difficult problems can be classified as cryptography problems, but what people are mostly concerned with today is the ability to keep transmissions private through the use of data encryption techniques and has become a paramount issue due to the changing nature of communications since the information revolution.

Cryptography makes use of the following mechanisms:

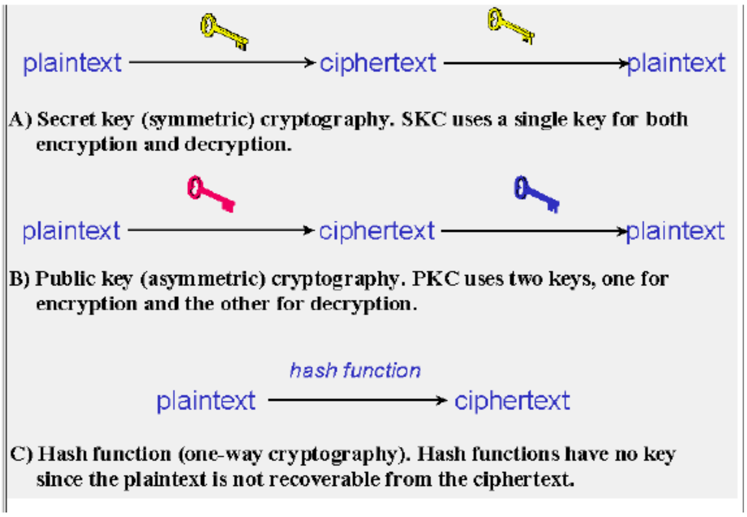
i Data encryption for confidentiality

ii Digital signatures to provide non-repudiation, authentication and message integrity

iii Digital Certificates for authenticating users, applications and services, and for access control (authorization).

Gray in [11] notes that, in data and telecommunication, cryptography is necessary over any untrusted medium, particularly the Internet and that modern cryptography today performs five primary function such as privacy/confidentiality, Authentication, Integrity, Non-repudiation and key exchange (key distribution and management). These primary functions of cryptography match the important security requirements of e-transactions. Hence, the security of any network system is ensured if cryptographic protocols are well implemented. All the fundamental services offered by cryptography has enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner. The security of cryptography is mainly based on secrecy of the key rather than the cryptographic algorithms. Therefore, there is need for keys to be shared without compromise. This gave rise to key management as additional function of modern cryptography. For the purpose of this research work, cryptographic algorithm is treated in a very abstract way. The work is more concerned with what security properties such algorithms provide and not with details of how they are implemented.

There are three cryptographic schemes used for security of e-transaction, as shown in figure 2: Secret key cryptography, public key cryptography and cryptographic hash function. Each scheme is optimized for specific function and application(s). Secret key cryptography is ideally suited to encrypting messages, thus providing privacy and confidentiality.



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Figure 2: Three types of cryptography: Secret-key, Public-key, and Hash Function [10].

Public key cryptography on the other hand can also be used for non-repudiation and user/message authentication. Public-key cryptography could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography. Eman in [12] asserts that, adopting public key cryptography is important to provide high level of confidentiality, integrity and authentication services for online transactions, but it needs a trusted way of distributing public keys. Public key infrastructures (PKI) is a solution for assuring the authenticity of public keys via qualified digital certificates (DC). Public key cryptography has two basic applications: Digital signature and key management and distribution. Public key cryptography requires a PKI for assuring the authenticity of public keys via qualified digital certificates, managing digital certificates and encryption keys for people, programs and systems

Finally, hash functions are well suited for ensuring data integrity because any change made to the contents of the message will result to the receiver calculating a different hash value than the one placed in the transmission by the sender. Since it is highly unlikely that two different messages (inputs to hash function) will yield the same hash value (second pre-image resistance property of cryptographic hash function), data integrity is ensured to a high degree of confidence.

There are two specific requirements of key management for Public key schemes; Secrecy of private key and assurance of public keys. The most crucial requirement of assurance of public key can be achieved through the public key infrastructure (PKI), a key management systems for supporting public cryptography. PKI provides assurance of public key, identification of public keys and their distribution. Several techniques have been proposed for the distribution of public keys.

E-transactions involve prescribed sequence of interactions between entities designed to achieve a certain end. This is known as protocol. Protocols are designed to facilitate communication. Before network devices are able to exchange data, it is necessary for the devices to agree on the rules (protocol) that will govern a communication session. Two common protocols in e-transactions are communication protocols and security protocols. A communications protocol is designed to establish communication between agents, which is setup a link, agree on syntax, etc, while security protocols, (sometimes known as cryptographic protocols), and involve providing security services in a distributed system. The goals of security protocols are: to establish a secret key between two entities; authentication of one entity to another; and ensuring secrecy, integrity, non-repudiation etc. Often, they involve the exchange of messages between nodes, requiring a trusted third party (eg. a session server). They may use different cryptographic mechanisms like symmetric or asymmetric encryption, public key cryptosystems, hashes, digital signatures and digital certificates. Security protocols undergo a lot of design and analysis and there are some difficulties that may arise;

i. The environment in which security protocols operate is very complex.

ii. The goals to be achieved and the properties that have to be ensured are very subtle

iii. Listing all of the capabilities of the penetrator is very difficult. Although it is impractical to list out all the capabilities of a penetrator, designers will try to make good approximations.

C. E-transaction Security challenges

The security in question in this work is how to protect transactions from undue disclosure, prevent attack, or how to detect attacks and recover from them. An attack is a deliberate attempt to compromise a system; it usually exploits weaknesses in the system's design, implementation, operation or management [13]; [14]; [15]. Attacks can be active or passive. An active attack involves attempts to alter system resources or affecting their operations, while passive attack involves attempts to learn or make use of information from the system but does not affect system resources. Active attack is difficult to prevent but should be detected while passive attack is difficult to detect, and should be prevented.

Many reports regarding online fraud in Nigeria create scepticism for conducting transactions online, especially through an open network such as the Internet which offers little or no security whatsoever. This calls for urgent attention in improving the security measures required to protect the network, users, businesses, and organizations, especially now that Nigeria has adopted the electronic payment system known as the Treasury Single Account (TSA) in all the Federal Government's financial transactions. By this, all Ministries, Agencies, Departments (MDAs), and Schools, are now paying one form of fee or the other through different online platforms, like REMITA, for example, the Federal Government's licensed partner. Many Schools have introduced web portals and now accept debit/credit cards for payments and other daily activities that are online based that demand serious security framework.

As the scale of e-transactions has grown, it has become very attractive to criminals and the volume of fraudulent e-transactions is also growing rapidly. The Nigerian Inter Bank Settlement System (NIBSS), in 2014 disclosed that Nigeria recorded 1,461 cases of fraud compared to 822 in 2013. Meanwhile, the central switch discloses that fraud in the Nigeria payment system and that of the global community has been on the increase over the past few years as technological advances impact on the way people do their businesses. Therefore, there is urgent need to develop, and implement a security protocol that will provide security services for online transactions. The consequences of lack of e-transactions security are potentially disastrous. This places a high premium on ensuring that e-transaction security is not misused. Security can basically be considered as a study of what the potential misuses of such systems are and how they can be averted.

D. Review of Related Literature

E-Transaction is a phenomenon that has emerged in Nigeria and has been considered as a key component in the trend towards globalization and the creation of the "e-society" as one of the driving forces transforming societies worldwide [16]. Some view electronic transaction as a source of problems, others realized that it also offers many opportunities to fulfil their role more effectively and meet the increased expectations of effective transactions. Some of the benefits of electronic transactions are prevented from being realized because of security threats and lack of legislative enactment [16]. Establishing e-transaction services can bring significant advantages for users and for the businesses but the participants are most concerned of security. Ajeet et. al. in [15] notes that the following are the important security requirements area for successful e-transactions: Authentication, Secrecy/Confidentiality, Data/Information Integrity, Non-repudiation and access control. Mohammad (2002) notes that e-transactions as the new way of commerce creates vast opportunities, but at the same time, poses security challenges. The security and privacy issues are of deeper concern than ever before. The Internet is basically an insecure communication medium. Most people are sceptical about the security of the Internet. The author in [4] also notes that people are happy using the World Wide Web for browsing, searching, reading or downloading information from the Internet but when considering e-transaction activities such as fund transfer, online payment, e-payment, sending a credit card number over the Internet, they are reluctant because of the alarming rate at which network security incidents are occurring. Unfortunately organizations are still faced with the challenges of trying to understand the types of attacks faced by the infrastructural assets [17].

There are a number of ways of classifying and characterizing the counter measures that may be used to reduce vulnerabilities and deal with threats and attacks to information system assets. The most common counter-measure is the functional requirements: those that require computer security technical measures (hardware, software or both) and those that are fundamentally management and non-technical issues. Pita and Wipawan [18] opines that**,** in order to address e-transaction security requirements, well-established cryptography mechanisms and protocols were believed to be a 'magic pill', and most adequate security toolkit.

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analysing protocols that overcome the influence of adversaries and which are related to various security requirements of e-transaction such as data confidentiality, data integrity, authentication and non-repudiation [19]**;**[20**]**. Application of cryptography include ATM cards, computer passwords and electronic commerce [19]. A cryptographic protocol also called security protocol is a message exchange that uses encryption in order to achieve security goals such as secrecy or authenticity over an open network that might be controlled by a hostile party.

III. MATERIALS AND METHOD

This research work adopted a survey approach in which a questionnaire with questions bothering on e-transaction technologies awareness and adoption in the banking industry was distributed to IT infrastructure managers at the headquarters of thirteen (13) top commercial banks in Nigeria. For the purpose of this paper we shall focus only on two of the items, which are awareness of legal framework for authenticating e-transaction in Nigeria and the percentage distribution of authentication services used by banks in Nigeria.

IV. RESULTS

The findings are shown in table 1 and figure 3, respectively. Table 1 shows the survey results on legal framework for authenticating e-transaction in Nigeria. The table shows that about 70 percent of the respondents have knowledge of legal framework for authenticating e-transaction in Nigeria. About 46 percent of the legal framework came from the Central Bank of Nigeria (CBN), 15 percent of the legal framework is industry based and less than 8 percent of the legal framework is International.

TABLE 1. Legal framework for authenticating e-transaction in Nigeria

Item	Response (%)
Knowledge of legal framework for authenticating e-transaction in Nigeria	
Yes	69.23
No	30.77
Specify the legal framework	
CBN	46.15
Industry	15.38
International	7.69
Knowledge of Enterprise security policy	
Yes	76.92
No	23.08
Knowledge of any disaster recovery plan	
Yes	69.23
No	30.77
The appropriate one	
Networks redundant links	23.08
Service and equipment replication	15.38
Off-site backups	46.15
Knowledge of fraud reporting	
Yes	92.31
No	7.69
Techniques use for fraud reporting	
Audit trails	61.54

A little above 76 percent of the respondents have knowledge of enterprise security policy. Also, less than 70 percent of the respondents have knowledge of any disaster recovery plan. About 46 percent of the respondents identified Off-site backups as the disaster recovery plan, while 23 percent of the respondents identified Networks redundant links as the disaster recovery plan, and about 15 percent of the respondents use Service and equipment replication as the disaster recovery plan. On knowledge of fraud reporting, about 92 percent of the respondents said yes.

From the above findings it may be safe to say that Nigeria is adopting e-transaction services and there is a legal framework in place for its growth and effective use, which the operators are aware of.

On types of authentication services, figure 3 shows the percentage distribution of authentication services used by banks in Nigeria. The figure shows that SSL with (23 percent) and Firewalls (23 percent), respectively are the most popular authentication services used.

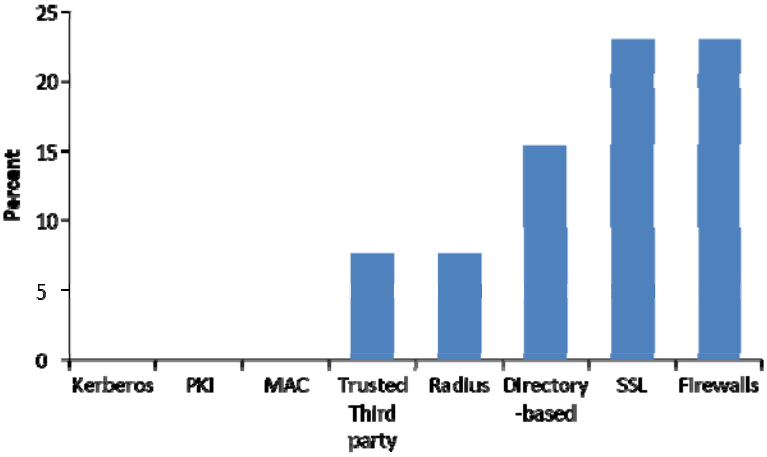


Figure 3: Percent distribution of Authentication services used by banks in Nigeria.

`This is followed by Directory-based (15 percent), Radius (8 percent) and Trusted Third Party (8 percent). However, no bank used Kerberos, PKI, and MAC for authentication services. In the following section, the paper discusses the findings of some authors with respect to the results of this work.

A. Discussion

A number of authors agree that Nigeria's developmental goals will be accelerated if she adopts e-transaction in various daily socio-economic activities, but they also sounded a note of caution. Odior and Fadiya in [21] stated that the development of innovative cashless banking has the potential to transform economic activity and achieve developmental goals if an effective cashless banking system can be developed, which will have the desired impact on the Nigerian economy. They also reiterated that central banks and governments must play a key role in promoting the development of popular forms of e-banking channels. The issue of identity theft is a major challenge to wider adoption of e-transaction like e-banking.

While many ICT users find it easier to do a whole lot of things online, they are very sceptical when it comes to financial transactions using online platforms. Ayo and Ukpere in [22] observes that because of lack of safety, security, privacy and reliability in the e-payments platforms there is an increase in cash circulation. They proposed the introduction of a smart card-based ATM with biometric authentication to combat the problem of identity theft. Ayo et.al [23] observed that the major use of the Internet among Nigerian populace is for email and social networking, they suggested a B2C e-commerce system usage, using a combination of information system adoption models. Asokan et. al. in [24] agrees that electronic funds transfer over financial networks is reasonably secure, but securing payments over open networks like the Internet poses a new set of challenges. Kim et. al. [25] sees customers' perceptions of the security of e-payment systems as a major factor in the evolution of electronic commerce in markets.

V. CONCLUSION

This paper has investigated the implementation and adoption of e-transaction in the Nigerian context. While e-transaction is rapidly gaining popularity and acceptance among users, there is still a perceived fear about its reliability and security. It is also discovered that there is a policy for the implementation of e-transaction from the government and bank regulating bodies, but like every new technology it is not without its teething problems. Overall, the prospects of its gains seem to out-weigh its perceived challenges. Many authors and users believe that it is the right direction in accelerating the country's socio-economic growth to ensure that Nigeria is at par with other global players.

E-transaction, especially when viewed in economic terms encourages policies that promote cashless society and solves the problems of high cost of printing physical cash, monitory instability, excess liquidity, as well as inefficient allocation of resources and a low depth of financial intermediation.

REFERENCES

[1] Margaret Rouse, Secure Electronic Transaction (SET), Available at: http://searchfinancialsecurity.techtarget.com/definition/Secure-Electronic-Transaction

[2] Edesiri G. Okoro and Promise E. Kigho,The problems and prospects of E-transaction (The Nigerian Perspective), Journal of Research in International Business and Management. Vol. 3(1) pp. 10-16, January, 2013

[3] Olanipekun, W. D., Brimah, A. N. , & Akanni, L. F., Integrating Cashless Economic Policy in Nigeria: Challenges and Prospects, International Journal of Business and Behavioral Sciences Vol. 3, No.5; May 2013.

[4] Mohammad Nabil Almunawar (2002), Securing Electronic Transactions To Support E-Commerce. Tinjauan: Policy and Management Review, Vol 4. 2001-2002, pp. 64-78, Available at: https://arxiv.org/pdf/1207.4292.pdf

[5] Hawker, A. Security and Controls in Information Systems, London, Routledge, 2000.

[6] Ugwu, Ejike, EZE, Everestus Obinwanne & UGBENE, Ifeanyichukwu Jeff, On The Technological Promises And Challenges Facing E-Businesses In Nigeria. Computing, Information Systems & Development Informatics, Vol. 3 No. 5 , December, 2012

[7] IBM, (2003) Introduction to Pervasive Computing for Business Partners, ftp://ftp.software.ibm.com/software/pervasive/info/BPIntro.pdf

[8] Mustafa Hassan Mohammad Adam. Electronic Banking Problems and Opportunities: The Sudanese Context, European Journal of Business and Management, Vol. 5 No.22, 2013, Available from: https://www.researchgate.net/publication/323987080_Electronic_Banking_Problems_and_Opportunities_The_Sudanese_Context [accessed Oct 13 2018].

[9] Seshadri R, Trivedi T.Raghu(2011), Efficient Cryptographic Key Generation using Biometrics Int. J. Comp. Tech. Appl., Vol 2 (1), 183-187 Singh, J. (2014): Review of E-commerce Security Challenges. International Journal of Innovative Research in Computer and Computer Engineering, Vol.2. Issue 2.

[10] Christopher Leidigh, Fundamental Principles of Network Security White Paper #101, available: https://www.apcdistributors.com/white-papers/Management%20Systems/WP-101%20Fundamental%20Principles%20of%20Network%20Security.pdf (Viewed 28/10/2018)

[11] Gary C. Kessler, An Overview of Cryptography (Updated Version,3 March 2016), available at: https://commons.erau.edu/cgi/viewcontent.cgi?article=1137&context=publication

[12] Eman Hableel, Young-Ji Byon, Joonsang Beak (2013), Public key infrastructure for UAE: a case study Proceeding SIN '13 Proceedings of the 6th International Conference on Security of Information and Networks, Pages 336-340

[13] Al-Awadi Maryam, Renaud Karen(2008), Success Factors in Information Security Implementation In Organizations, in proceedings AlAwadi 2008S UCCESSFI Available at: https://www.researchgate.net/publication/266231077_SUCCESS_FACTORS_IN_INFORMATION_SECURITY_IMPLEMENTATION_IN_ORGANIZATIONS

[14] Mohanty, P., Panigrahi, S., Sarma, N., & Satapathy, S. S. (2010). SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY. Journal of Theoretical & Applied Information Technology, 13.

[15] Ajeet Singh, Karan Singh, Shahaz ad, M.H Khan, Manik Chandra (2012), A Review:Secure Payment System for Electronic Transaction, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, 2012

[16] Aliyu Sanni Abubakar,Francis Ojo Adebayo, Analysis of Electronic Transactions Bill in Nigeria: Issues and Prospects Mediterranean Journal of Social Sciences MCSER Publishing, Rome-Italy Vol 5 No 2 January 2014

[17] Mouna Jouini, Latifa Ben Arfa Rabai, Anis Ben Aissa (2014), Classification of security threats in information systems, Procedia Computer Science, 32 (2014) 489 – 496

[18] Pita Jarupunphol and Wipawan Buathong, Secure Electronic Transactions (SET): A Case of Secure System Project Failures. IACSIT International Journal of Engineering and Technology, Vol. 5, No. 2, April 2013

[19] Rathi, N.A. and Gupta, S.R. (2016): Analysis of Security mechanism in E-commerce transaction. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol 5 Issue 1, January 2016 131 ISSN: 2278 – 1323

[20] Vorapranee Khu-smith, Enhancing the security of electronic commerce transactions, Thesis submitted to the University of London. for the degree of Doctor of Philosophy, Available at: https://www.ma.rhul.ac.uk/static/techrep/2003/RHUL-MA-2003-7.pdf

[21] Odior Ernest Simeon, Fadiya Bamidele Banuso (2012), CASHLESS BANKING IN NIGERIA: CHALLENGES, BENEFITS AND POLICY IMPLICATIONS, European Scientific Journal une edition vol. 8, No.12

[22] Ayo Charles K. and Ukpere Wilfred Isioma(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

[23] Ayo C. K, Adewoye J. O. and Oni A. A(2011). Business-to-consumer e-commerce in Nigeria: Prospects and challenges. African Journal of Business Management Vol. 5(13), pp. 5109-5117, Available online at http://www.academicjournals.org/AJBM

[24] Asokan N, Janson P. Steiner M., Waidner M (2000). State of the art in electronic payment systems, Advances in Computers, Volume 53, Pages 425-449

[25] Kim Changsu, Wang Tao, Namchul Shin, Ki-Soo Kim(2010), An empirical study of customers' perceptions of security and trust in e-payment systems, Electronic Commerce Research and Applications, Volume 9, Issue 1, Pages 84-95

AUTHORS PROFILE

Chijioke Amaka obtained her Bachelor of Engineering in Computer Science and Engineering from Enugu State University of Science & technology and has a Master's Degree in Computer Science at Nnamdi Azikwe University Awka. Currentlry she is lecturing at the Federal Polythnic, Okoh, Anambra state Nigeria. She is currently rounding off her PhD.

Agozie Eneh obtained his Bachelors in Computer Science from the University of Nigeria Nsukka and his Masters and PhD in Middlesex University, England, specializing in Network Security. Currentlry he is lecturing in the Department of Computer Science, University of Nigeria, Nsukka Nigeria.

Collins Udanor obtained his Bachelor of Engineering in Computer Science and Engineering in Enugu State University of Science & technology and has a Master's Degree in Computer Science (Data Communication), and PhD in Electronic Engineering at the University of Nigeria Nsukka, where he is currentlry lecturing in the Department of Computer Science.

Uchenna Nduka holds a Master's Degree from the Department of Statistics, University of Nigeria Nsukka and is currently rounding off his PhD programme with the Federal University of Technology, Owerri, Imo State, Nigeria. He currently lectures in the Department of Statistics, University of Nigeria Nsukka.