Analysis of Security Issues in Electronic Payment Systems

Princewill Aigbe
Department of Mathematics and Computer Science
College of Natural and Applied Sciences
Western Delta University, Oghara, Nigeria

Jackson Akpojaro
Department of Mathematical and Physical Sciences
College of Basic and Applied Sciences
Samuel Adegboyega University, Ogwa, Nigeria

ABSTRACT
The emergence of e-commerce has created new financial needs that in many cases cannot be effectively fulfilled by the traditional payment systems. Recognizing this, virtually all interested parties are exploring various types of electronic payment systems, issues surrounding electronic payment system and digital currency. Broadly, electronic payment systems can be classified into four categories: online electronic cash system, electronic cheque system, online credit card payment system, and smart cards based electronic payment system. Each payment system has its advantages and disadvantages for the customers and merchants. We highlight the analysis of the security levels in relationship with fraud vulnerability, and determine how this relationship affects or boosts the confidence of the users.

General Terms
Electronic payment system, e-commerce

Keywords
eCash, credit card payment system, vulnerability, digital signature, biometric finger print, merchant

1. INTRODUCTION
The exchange of goods and services conducted face-to-face between two parties' dates back to before the beginning of recorded history. Eventually, as trade became more complicated and inconvenient, humans invented abstract representations of value. As time passed, representations of value became more and more abstract, progressing from barter system through bank notes, payment orders, checks, credit cards, and now electronic payment systems. Traditional means of payment suffer from various well-known defects or problems: money can be counterfeited, signatures forged, and checks bounced. On the other hand, properly designed electronic payment systems can actually provide better security than traditional means of payments, in addition to flexibility of use [7].

An electronic payment system (EPS) is a system of financial exchange between buyers and sellers in the online environment that is facilitated by a digital financial instrument (such as encrypted credit card numbers, electronic checks, or digital cash) backed by a bank, an intermediary, or by legal tender [14]. The Internet is now a commercial place in which payments are rendered for goods, information and services. To support such e-commerce some form of money must be exchanged over the Internet. The Nigerian economy have maintained appreciable growth due to the volume of e-commerce activities, particularly on the online retail genre of business, which has a large support from the local and international banks [27]. A secure payment method - electronic payment system - is required as a compensation for information, goods and services provided on the web (for example, access to copyrighted materials) and as a convenient way to pay for external goods and services [15]. It helps to automate sales activities, extends the potential number of customers and may reduce the amount of paperwork.

Summarized findings of this work are stated as follows:

- It provides a review of the various online payment systems.
- Analyze the various authentication mechanisms of the online payment systems and levels of confidence each provides.
- Analysis reveals that electronic payment systems with authentication mechanisms which involve two or more authentication factors tend to be more secured, reduced fraud vulnerability, and boost users' confidence in using electronic payment systems.

2. CATEGORIES OF ELECTRONIC PAYMENT SYSTEMS
Today, there exist a wide variety of electronic payment systems - most of them incompatible with each other. The broad categories of electronic payment systems are [12]:

- Electronic cash system
- Electronic cheque system
- Smart card-based electronic payment system
- Online credit card payment system

2.1 Electronic Cash (eCash) Payment System
Electronic cash (e-Cash) also called digital cashis digital moneythat provides private customers with a safe, fast and low-cost means of payment on the Internet. Created by lots of individual parties, it moves through multiple networks instead of the current bank system and is best suited for micropayments, [1]. Electronic cash is independent of any network or storage device and portable. The electronic cash units and their values can be defined independently of real currency.

The application of e-cash requires that both the merchant and the customer establish e-cash accounts at the issuing bank, which issue tokens to their customers. In this electronic payment system, tokens are the payment instruments that represent monetary values. A customer must install a "cyber wallet" onto his computer, which will store the money requested from the bank, [4].

When the consumer contacts the bank in order to withdraw electronic cash, the bank verifies his identity, issues the amount of electronic cash and at the same time deducts the amount of

cash from the consumer's account. The electronic cash can only be spent on sites that accept the electronic cash for payment. When the goods are shipped to the consumer, the merchant can present the electronic cash to the bank, which will then credit the merchant's account for the transaction amount. In e-cash transactions, the payee does not know the payer's identity and the issuing bank may or may not keep the identity of the recipient of the electronic bank notes, which makes the customer to remain anonymous. The anonymity of the customer allows for double spending as the customer can present same tokens (payment instruments) for different payment transactions [13].

Anonymity of users and double spending of the same tokens have been the major security holes of e-cash payment system. The only security mechanism provided by e-cash payment system is the encryption of payment instruments (tokens or coins) generated by a given customer [5]. It makes use of single-factor authentication mechanism, which is not adequate for electronic payment systems involved in critical portions of payment processing. The critical payment function would be compromised if a user's single-factor authentication process failed. This means that electronic payment system (e.g., e-cash) with a single-factor authentication has poor security level [25].

2.2. Electronic Cheque (eCheque) Payment System

Electronic cheques are the equivalent of paper-based cheques. The electronic cheques are initiated during an on-screen dialog and the funds are transferred over a computer network at the time of the transaction. Authorised users are assigned a portable electronic chequebook which is an amalgam of a secure hardware device and specialised software. The electronic chequebook which stores and delivers the customer's private-key and certificate information is used for generating and signing eCheques. The electronic chequebook Interfaces with financial management and transaction processing software of the issuing bank [2]. The payer writes the eCheque on a computer, cryptographically signs it, and e-mails it via the Internet. The payer signs the eCheque using the secure hardware device, and includes its authenticating certificate, signed by the issuing bank. The payee receives the eCheque, verifies the payer's signature on the eCheque, endorses it, writes a deposit slip, and signs the deposit slip. The endorsed cheque is then sent by e-mail to the payee's bank for deposit. The payee's bank personnel verify the payer's and payee's signatures, credit the deposit, and then clear and settle the endorsed eCheque by sending it to the payer's bank. The payer's bank verifies the payer's signature once again and the amount on the eCheque is debited from the payer's account [9].

The electronic cheque payment system make use eCheque payment instrument, which is the digital form or representation of the paper cheque. The eCheque is protected by PIN and digital signature. This means that it makes use of a two-factor authentication mechanism in verifying the users during payment process. This authentication mechanism requires a user to prove his or her identity with two items of data. It is more secure than a single-factor system [24].

2.3. Smart Card Payment System

Smart cards are a credit-card-sized, plastic card with an embedded integrated circuit chip providing users with mobility and data portability, i.e. direct access to cash or services. It combines plastic and magnetic cards used for different identification purposesinto one card, which can access multiple services, networks and the Internet. The chip therefore, reduces the number of cards, making one card the access key to many accounts. The smart card as a payment instrument has processing power that allows the smart card payment system to be used for multiple functions and/or applications [3]. This of course, reduces the overall number of cards in the consumer's wallet, though there are many arguments and issues about whether or not smart card is secured and safe enough to store such information.

International standards for the smart card procedures and the smart card itself are both still evolving. In general, smart cards currently cannot display information or directly accept input from the user [22]. For the user to access the information the smart card contains, the card needs an interface to communicate with a reader or terminal, such as a merchant point-of-sale.

A vast amount of information and possible cash is stored on the smart card. If the card is lost or stolen, there is no way to recover the information or the money. This causes a true potential fraud or major fraud vulnerability of smart card payment system [11]. The smart card payment system provides three-factor authentication security mechanism for the verification and authentication of a given user. These are personal identification number (PIN), digital signature, and fingerprint biometric. This mechanism increases the security level of this payment system.

2.4. Online Credit Card Electronic Payment System

The concept of credit has been around for centuries. Starting in the early 1800s, local merchants allowed trusted customers to make purchases without paying the total cost upfront. This intuitive concept allowed sellers to reach a larger base of customers who could then pay their debt over time. The idea of enabling purchases by extending credit spread quickly, and in the early 1950s, a terminal moment occurred: the invention of the credit card, [26].

A credit card is an account that lends money to the consumer, meaning consumers are allowed to purchase goods or services on credit. The credit card, being a token of trust, transfers the risk of granting credit from a merchant to the card-issuing bank. Both consumers and merchants must register with a bank. The participants involved in credit card payments include [16]:

- *Customer/Cardholder:* The consumer doing the purchase, using a credit card that has been issued by its issuer.
- *Issuer:* The financial institution (i.e. bank) that issues the card to the cardholder. The issuer guarantees payment for authorised transactions.
- *Merchant:* The merchant offers the goods and services, and has a financial relationship with the acquirer.
- *Acquirer:* The financial institution of the merchant. The acquirer processes credit card authorisations and payments.

A cardholder visits a cyber-storefront via a browser. After selecting the items to be purchased, the customer (online shopper) fills out a payment request, and selects from the credit cards he wants to use and the customer transmits the payment request to the payment gateway (or merchant's web server). At the payment gateway, the information is send to the merchant. The merchant generates a request-for-payment authorisation from the cardholder's financial institution. His digital

signature, transaction identifier and payment instructions are included in the encrypted request and forwarded to a payment card-processing centre or payment gateway of the acquirer, where it is decrypted, processed and verified [6].

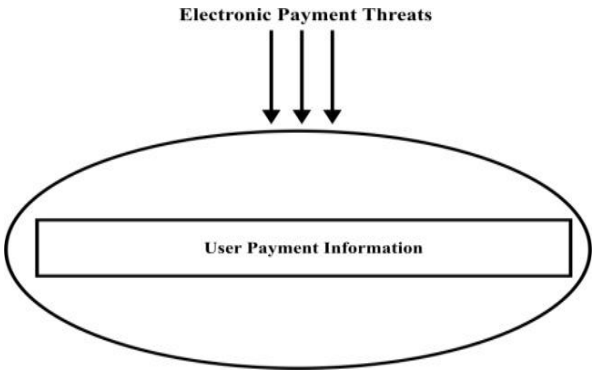
After the transaction is verified, the payment card-processing centre converts the authorisation request into the format used by financial networks and then forwards it for approval to the cardholder's bank (issuer) for authorisation. The issuing bank returns an approval or denial response to the payment gateway in response to the authorisation request. The payment gateway will send this response (authorisation or failure) to the merchant. If the bank approves the authorisation, the payment gateway sends a notification in the form of a digitally signed and encrypted message to the merchant, which can be claimed later from the merchant's bank for deposit.

Once the merchant has received the payment gateway's digital signature, he will ship the goods to the cardholder knowing that the customer transaction has been approved. The merchant will request settlement from the issuer, via the payment gateway via the acquirer. The online credit electronic payment system applies a two-factor authentication mechanism in verifying the users during payment process [8].

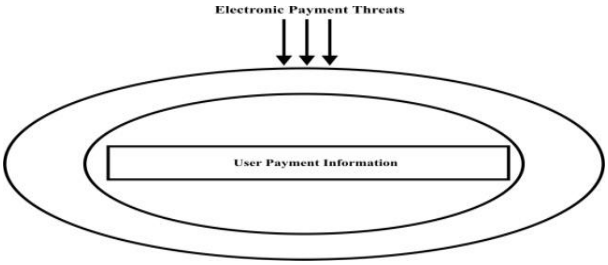
3. ANALYSIS OF THE DIFFERENT AUTHENTICATION MECHAMISMS FOR ELECTRONIC PAYMENET SYSTEMS

The target information that must be kept secret from being compromised in any given online payment transaction cycle is the user payment (financial) information. It is therefore necessary that a method and system for authenticating the identity of a user by an authority makes use of multiple layers of protection. The method and system can be augmented by requesting for different security credentials such as PIN, cryptographic key, digital signature, biometrics, etc, to establish multiple layers of authentication. Varying the layers of authentication factors result in greater or lesser security, and the accuracy for any given layer of authentication factor must be concrete enough without compromising the integrity of online users' payment information and the entire system. This means that the authentication factors mechanism should be strong to withstand the various kinds of internet threats used by cybercriminals. The layers of authentication mechanisms used by the different electronic payment systems are illustrated in figure 1.

i. One-Layer Authentication Factor Mechanism



ii. Two-Layer Authentication Factor Mechanism



iii. Three-Layer Authentication Factor Mechanism

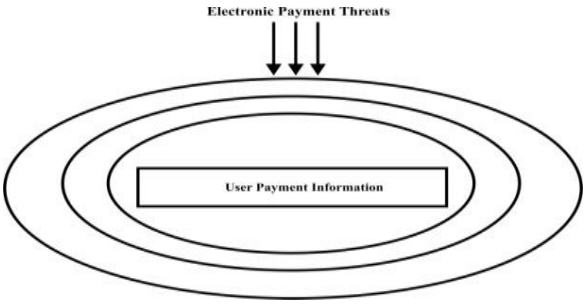


Figure 1: Layers of Authentication Factors Mechanisms

The different electronic payment systems illustrated so far exhibit different levels of authentication factors. The authentication-factor determines the extent to which an electronic payment system is secured. A single-factor authentication mechanism uses or requires a user to prove his or her identity with an item of data only. This means that the electronic payment system is easily compromised if this single authentication-factor fails [19].

A two-factor authentication presents two independent pieces of information in two coherent and dependent steps of just one single process whereas, A three-factor authentication presents three independent pieces of information in three coherent and dependent steps of just one single process.

Authentication by multiple independent factors seeks to decrease the success that the requester is presenting false evidence of its identity in multiple independent, but coherent processes. The number and independency of factors is important, since more independent factors imply higher probabilities that the bearer of the identity evidence indeed holds that identity in another realm [20]. Table 1 shows the categories of electronic payment systems with their number of authentication-factor and authentication types.

Table 1: Electronic payment systems with their authentication factors and types

Electronic payment systems	Number of authentication factor	Authentication type
Electronic cash (eCash)	1	Token encryption
Electronic cheque (eCheque)	2	PIN, digital signature
Smart card	3	PIN, digital signature, biometric (finger print)
Online credit card	2	PIN, digital signature

Electronic payment systems that incorporate three or more authentication factors are stronger than systems that only incorporate one or two of the factors. The electronic payment systems should be implemented so that multiple factors are presented for payment verification process [18].

The electronic payment system with a higher number of authentication/verification factors may have higher secure level. This means that an electronic payment system with higher authentication/verification factors will have a stronger security level compare to electronic payment system with one factor hence, contributing to the security strength which lowers or reduces the fraud vulnerability of the electronic payment system, and this eventually boost users confidence [21].

If A_F denotes authentication factor, F_V fraud vulnerability, U_C user confidence, and S_L security level then, intuitively we can state that: authentication factor (A_F)∝security level (S_L), i.e., authentication is directly related to the security level; conversely, authentication factor (A_F)$\propto \frac{1}{F_V}$, i.e., authentication factor is inversely related to fraud vulnerability, while security level (S_L)∝user confidence (U_C) implies that security level is directly related to user confidence.

The graphical representations of the three different authentication mechanisms which illustrate the four variables in the mathematical relationships [23] above are shown in Figures 2, 3 and 4.

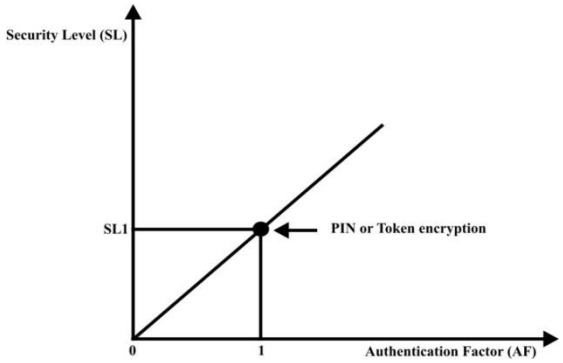


Figure 2: Single-factor authentication

Figure 2 shows electronic payment systems (e.g., eCash) that use a single-factor authentication mechanism. It suffers from the following problems:

i. Very low security

ii. Fraud vulnerability very high

iii. User confidence very low

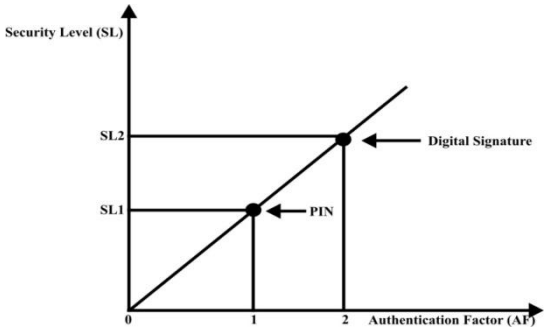


Figure 3: **Two-factor authentication**

Figure 3 illustrates electronic payment systems (e.g., eCheque, online credit card) with two-factor authentication mechanism. As the number of authentication factors increase so are the following:

i. Increase in degree of security against fraud.

ii. Reduction in fraud vulnerability.

iii. User confidence boosted.

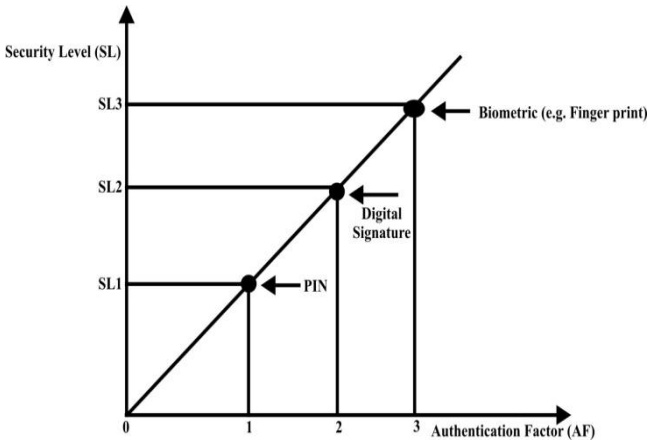


Figure 4: Three factors authentication

Figure 4 represents electronic payment systems (e.g., smart card) with three-factor authentication mechanism. It enjoys the followings:

i. Degree of security against fraud is very high

ii. Fraud vulnerability very low (i.e.it reduces vulnerability to barest minimum)

iii. High level of user confidence

4. CONCLUSIONS AND FUTURE WORK

This paper presents a complete review of the different categories of electronic payment systems in terms of online payment processes, authentication mechanisms, and authentication types. The paper further demonstrates the application of the different authentication mechanisms and types in the categories of the electronic payments system highlighted. Finally, analysis reveals that electronic payment systems with authentication mechanisms involving two or more authentication factors tend to be more secured, reduced fraud vulnerability, and boost users' confidence in using electronic payment systems.

Future work combines the above discussed authentication mechanisms, in particular, the three-factor authentication model; including biometric (finger-vein) to design an enhanced algorithm for electronic payment systems whose authentication's capability would surpass the existing online payment applications.

5. REFERENCES

[1] Au M. H., Susilo W., and Mu Y. 2011. Electronic cash with anonymous user suspicion. In proceeding of the 16th Australasian Conference on Information Security and Privacy (ACISP'11), Melbourne, Australia, LNCS, Vol. 6812, 172–188.

[2] Baldintsi F. and Lysyanskaya A. 2012. On the Security of One-Witness Blind Signature Schemes", IACR Cryptology ePrintArchive.

[3] Batina L., Hoepman J. H., Jacobs B., Mostowski W., and VullersP.2010. Developing Efficient Blinded Attribute Certificates onSmart Cards via Pairings. CARDIS, Vol. 6035, 209–222.

[4] Blazy O., Canard S., Fuchsbauer G., Gouget A., Sibert H., andTraore J. 2011. Achieving optimal anonymity in transferablee-cash. In Proceeding of the 4th International Conference onCryptology in Africa (AFRICACRYPT'11), Dakar, Senegal,LNCS. Vol. 6737, 206–223.

[5] Canard S. and Gouget A. 2010. Multiple denominations in e-cash with compact transaction data. In Proceeding of the 14thInternational Conference on Financial Cryptography and DataSecurity (FC'10), Tenerife, Canary Islands, LNCS. Vol. 6052,82–97.

[6] Hezlin H., Balachander K. G. and Mohan V. A. 2011. Evidenceof Firms' Perceptions toward Electronic Payment Systems (EPS)in Malaysia. International Journal of Business and Information, 6(2).

[7] Jun S. and Punit A. 2011. The more secure the better: A study of information security readiness. Industrial Management and Data Systems. 111(4), 570-588.

[8] Leeuwen V. 2009. A Surge in Credit Card Fraud. H. Financial Review, p. 49.

[9] Mahen K. S. 2009. E-cheque System in India: A Distant Reality.National Law Institute University, Blogal.

[10] Mehdi M. and Nasser M. 2014. Security Evaluation of web-based electronic payment systems. New York Science Journal, 7(6), 37-48.

[11] Mohammad M. and Abdallah S. 2011. Empirical Study in the Security of Electronic Payment Systems. IJCSI Journal of Computer Science Issues,8(4), 56 - 68.

[12] Murthy, C. S. V. 2002. E-Commerce Concepts, Models, and Strategies. New Delhi, Himalaya Publishing House, p. 626.

[13] Nishide S. and Sakurai K. 2011. Security offline Anonymous Electronic Cash Systems against insider attacks by untrusted Authorities revisited. In Proceeding of the 3rd International Conference on Intelligent Networking and Collaborative Systems (INCoS'11), Fukuoka, Japan. IEEE, pp. 656–661.

[14] Oh, S., Karina S., Johnston R. B., Lee H. and Lim B. 2006. A Stakeholder Perspective on Successful Electronic Payment Systems Diffusion. Hawaii International Conference on System Sciences (HICSS – 39), Hawaii.

[15] Perlman R. J, Kaufman C. and Perlner R. A. 2010. Privacy- preserving and Trust. In Proceeding of the 9th Symposium on Identity and Trust on the Internet (IDtrust'10), Gaithersburg, Maryland, USA. ACM, pp. 69–83.

[16] Rehman S. U, Wasi S. and Siddiqui J. A. 2009. Towards an easy to pay system (ETPS) for e-commerce. International Conference on E-Business and Information System Security.

[17] Refka A., Marc P., and Olivier B. 2011. Integration of New Electronic Payment Systems into B2C Internet Commerce. The International Symposium on Collaborative Technologies and Systems (CTS), Philadelphia, United States.

[18] Samsudin W. and Khaled M. 2011. The influence of perceived privacy on customer loyalty in mobile phone services: An Empirical Research in Jordan. IJCSI, 8(2), 45-52.

[19] Saurabh V., Ranali P., Mahesh S. and Priyanka R. 2014. Android – Based Mobile Payment System Using Three – Factor Authentication. International Journal of Emerging Technology and Advance Engineering, 4(3), 797 – 801.

[20] Shieh W.G. and Horng W. B. 2010. Security Analysis and Improvement of the Remote user Authentication Scheme without using Smart Cards. ICIC Express Letters, 4(6(B)), 2431-2436.

[21] Smita P. and Noumita D. 2014. Study and Implementation of Multi-Criterion Authentication Approach to Secure Mobile Payment System. International Journal of Engineering Science And Advanced Technology (IJEAST), 3(3), 117-122.

[22] Sumanjeet S. 2009. Emergence of Payment Systems in the Age of Electronic Commerce: The tale of Art. Asia Pacific Journal of Finance and Banking Research, 5(3).

[23] Tao W., Shin N. and Kim K. S. 2011. An Empirical Study of Customers' perceptions of Security and Trust in E-payment Systems. Electronic Commerce Research and Applications, 9(1), 84–95.

[24] Yang J. H. and Chang C. C. 2010. An efficient fair electronic payment system based upon non-signature authenticated encryption scheme. International Journal of Innovative Computing, Information and Control, 5(11(A)), 3861-3873.

[25] Ziba E. and Melidi T. 2011. A New untraceable off-line Electronic Cash System. Electronic Commerce Research and Applications, pp. 59-66.

[26] Zielke B. 2011. Why Credit Cards are not the Future of Online Payment. Javelin and Strategy Research.

[27] Osuagwu, P. 2014. Lack of Strategic Investors, bane of Nigeria's e-commerce Growth. Vanguard, Wednesday, October 15, 2014, p.25.