Journal of Computer Science

Original Research Paper

Optimized Authentication Model for Online Transaction Payments

[1]Owusu Nyarko-Boateng, [1]Benjamin A. Weyori and [2]Lord Anertei Tetteh

[1]Department of Computer Science, The University of Energy and Natural Resources, Sunyani, Ghana
[2]Accra Institute of Technology University, Accra, Ghana

Article history
Received:16-06-2019
Revised: 17-09-2019
Accepted: 15-02-2020

Corresponding Author:
Owusu Nyarko-Boateng
Department of Computer Science, the University of Energy and Natural Resources, Sunyani, Ghana
Email: owusu.nyarko-boateng@uenr.edu.gh

https://orcid.org/0000-0003-0300-2469

Abstract: The rapid growth of the internet across the globe has gained attention in the world of business. The internet has become the major driver for business growth in the world; due to several security lapses online; it is necessary to implement measures and standards on the internet to protect transactions online. These security lapses have led to the development of various online payment protocols to ensure the safety of online transactions such as Secure Electronic Transaction (SET), internet Keyed Payment (iKP) and The Secure Socket Layer (SSL). There are several methods of paying for online transactions; these include direct payment with bank accounts and the use of electronic card. The payments are subjected to the verification system, which ensures no one uses someone's card to transact business online. Each card has a security feature known as the Card Verification Value (CVV) number, which is used as authentication for online business. The key feature of the card which validates the card owner as the user is the CVV number, which is found at the back of the card. The problem is that when the card gets lost or falls into the hands of another person, it is likely the person might use the card for a fraudulent activity online. This is because all the information required for e-payment is on the card. In this paper, we propose an optimized conceptual model which ensures the removal of the CVV number from the all-electronic card, the paper also recommended a framework that deployed Unstructured Supplementary Services Data (USSD) technology in the online transaction and payment process. In a real-world implementation, the proposed optimized model shall enhance e-commerce payments, card user participation, reduce threats, improves the security of conducting online business and then offer the card user the opportunity to deny or accepts payment.

Keywords: CVV, Issuer, Merchant, Authentication, Bank, E-Commerce

Introduction

The popular commercial activities, especially on the internet, has gained maximum prominence in the field of commerce as more and more goods and services are seen on the internet daily for online transactions. Buying and selling online, also known as e-commerce, is efficient, easy, reliable and convenient (Takyi and Gyaase, 2012). In order to have reliable e-commerce services, there must be digital measures in place to check the security of users to ensure safety in online transactions with access control measures such as authentication and others measures like privacy, integrity and non-repudiation. The payments for online transactions are made either with a credit card, debit card, or direct bank payment. The payment process poses some level of risk because the entire payment procedures are susceptible to cyber-attack (Strategy, 2017).

Cyber fraudsters expose the weakness in online payment systems. Their criminal activities cause the loss of over millions of dollars globally every year (Takyi and Gyaase, 2012; Strategy, 2017). Cybercriminals compromise accounts and complete fraudulent transactions in many different ways (Levi and Kroc, 2001) such as replay attacks. However, fraudsters continue to attack online transactions and successfully compromise account by stealing victims

money. Cybercriminals gain access to a large cache of information that includes account names, personal information, credit card detail, banking details and much more (Hwang *et al*., 2003; Turban *et al*., 2010).

Online transactions usually require a secure payment electronic system. Credit and debit cards are mostly used for the online transaction. The card owner is mostly protected by several security measures to ensure safety in doing business online. The key feature of the electronic card which validates the card owner as the card user is the CVV number which is found at the back of the electronic card. The problem is that when a card gets lost or falls into the hands of another person, it is likely the person might use the card for fraud activity online. This is because all the information required for online payment is on the card. In this paper, we propose an optimized conceptual model which ensures the removal of the CVV number from all electronic cards. We recommended in our framework, the need to issue the CVV number to the owner which shall be used as an authentication code to verify the identity of the buyer during online transactions. Card owners must be requested to provide their card CVV numbers before payment authorization. This optimized model shall enhance digital security and tracking of financial transactions which has become significant aspects of many businesses. The new framework ensures privacy and anonymity of card owner, the integrity of merchants, the card compatibility and acceptability with other services and transaction, the efficiency of e-commerce activities, users convenience, mobility, improved security for low financial risk for online business.

Crime Rate affecting Electronic Payment System

In 2016, 15.4 million consumers were victims of identity theft, which was up by 16 percent from 2015 and the highest figure recorded since (Strategy, 2017) began tracking fraud instances in 2004. Card-not-present fraud jumped the most, increasing 40 percent compared to 2015. Account takeover fraud rose to 31 percent and instances where fraudsters opened new accounts in a consumer's name, were up by 20 percent. In all, thieves stole $16 billion, nearly $1 billion more than in 2015. The assurance of secure online transaction needs to be improved if the developing world is to benefit from the global adoption of e-commerce (Hwang *et al*., 2003; Law *et al*., 2016).

CVV Number

The use of credit card for e-commerce is on the rise as against direct electronic payment (e-payment) from the conventional bank system. In both cases, proper authentication of the card owner is mostly carried out before authorization is granted (Takyi and Gyaase, 2012). The required security check at the merchant's website is the CVV value, the card owners' name, the card number and the expiry date of the credit card. These are the four key security features required as authentication to authorize payment online. The CVV number is an anti-fraud security feature which helps online retailers to verify that you have the credit card you are using (Xiao *et al*., 2008). The CVV code is typically a three-digit number located on the back of the electronic card (Fourati *et al*., 2002) as shown in Fig. 1.

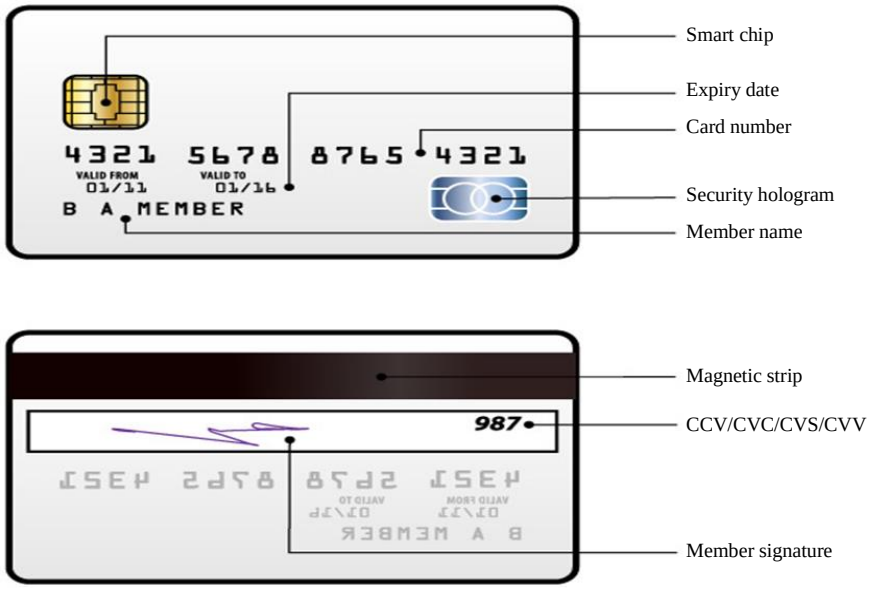

Fig. 1: Front and back view of electronic card (Source: Google)

Review of Related Work

E-Commerce

Electronic Commerce (E-commerce) is the buying and selling of goods and services or the transmission of money over the internet. E-commerce has been categorized as business-to-business, business-to-consumer, consumer-to-consumer, or consumer-to-business. E-commerce and e-business are terms which are often used interchangeably. The beginning of e-commerce can be traced back to the 1960s when businesses started using Electronic Data Interchange (EDI) to share business documents with other companies (Turban *et al*., 2010; Law *et al*., 2016). In 1979, the American National Standards Institute (ANSI) developed ASC X12 as a universal standard for businesses to send and receive information through various networks. After the number of individual users sharing electronic documents grew in the 1980s, in the 1990s, the rise of eBay and Amazon revolutionized the e-commerce industry. Consumers can now purchase endless amounts of items online, both from typical brick and mortar stores with e-commerce capabilities and then online shopping (Law *et al*., 2016).

Online Payment Systems

Electronic payment enables individuals, businesses, governments and nonprofit organizations to make cashless payments for goods and services through cards, mobile phones, or the internet (Fourati *et al*., 2002). It presents several advantages, including cost and time savings, increased sales and reduced transaction costs. The players of these transaction processes have become vulnerable to internet fraud and potentially put them at risk (Xiao *et al*., 2008; Fourati *et al*., 2002). Online payments involve a multifaceted set of practical and analytical challenges, including technological capabilities of service providers, commercial relationships, regulations and laws, security issues such as identification, authentication and verification with coordination among parties with different and competing interests (Ford, 2001).

Electronic Cards

Electronic cards are the most fundamental entity required in electronic payments (Li, 2008). Generally, there are three types of cards for online business: credit, debit and prepaid cards (Hwang *et al*., 2003; Xiao *et al*., 2008). The cards are typically made of plastic and have a magnetic stripe at the back of it. The card owner gives the merchant the card while shopping and the merchant swipe the card through a terminal or puts the relevant information into a database, which is then delivered to the credit card company, who relays a confirmation message back to the merchant that the purchase was completed. This process typically takes only a few seconds to complete (Ford, 2001; Leavitt, 2010; Shrivastava, 2012). Credit cards are a common form of electronic payment because they can be used almost anywhere for almost any kind of purchase, both online and offline businesses (Roy Laurens and Zou, 2016; Luhach *et al*., 2014). The user does not have to have cash in hand to pay for things. Some e-payment procedures include:

Person-to-Person Payments

These payment processes enable one person to pay another using an online account, a prepaid card or another mechanism that stores value. Various companies facilitating such payments are PayPal, Alert Pay and Money Bookers. These payments services can easily be accessed over the internet on electronic devices. The cards provide a comfortable, convenient and secure means of making transactions online (Luhach *et al*., 2014).

E-wallet

This is a form of prepaid account that stores user's financial values like bitcoin, debit and credit card information to make an online transaction easier (Leavitt, 2010).

Security in an Online Payment Scheme

The online payment system has had several security checks in place to ensure safety in transacting business over the internet. SET, iKP, SSL and other security protocols have been proposed over the years to ensure:

Party Authentication

Each engaging party in the system must be able to authenticate the party whom he is communicating with.

Transaction Privacy

Each engaging party must be able to ensure that the messages are not revealed to any unauthorized parties, but only to the intended recipient of the messages.

Transaction Integrity

Each engaging party can ensure that the received messages are not altered during the transmission.

Non-Repudiation of Transactions

Each engaging party cannot deny the transactions he has performed.

E-payment Processing Scheme

Figure 2 illustrates the key parties in e-payment eco-system and the flow of transaction processes in the e-payment space. The user initiates an online transaction and the process needs to go through various authentication schemes through the web server, the payment gateway, the bank and the merchant. The transactions between banks are secured, reliable and convenient (Takyi and Gyaase, 2012).

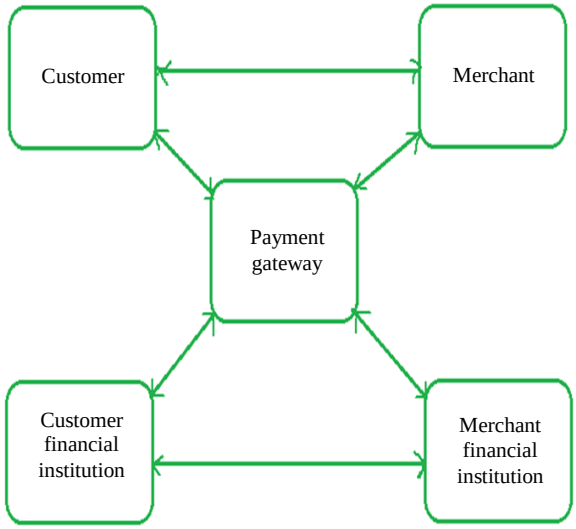

Fig. 2: Key parties in e-payment eco-system

Increasing globalization and the need to enhance e-commerce usability require a more secure, reliable and convenient e-payment system that will be easy to implement and convenient to use for all participants. This paper presents an optimized conceptual model for a secure online transaction between parties with a balanced trade-off between security, processing period and convenience (Levi and Kroc, 2001).

Generally, the e-payment model is composed of 4 main engaging parties:

- The client is a party who requests to purchase products or services from a merchant
- Merchant has products or services offered to the client
- The issuer is the client's financial institution. It has the client's account established and tasked to manage the client's account, including the fund transfer
- The acquirer is the merchant's financial institution. It manages the merchant's account, including the fund transfer

A new party called Payment Gateway acts as a medium between the issuer/acquirer at the banking private network side and the client/merchant at the Internet site for payment clearing purpose.

Protocols in the e-Payment System

The realization of e-commerce is based on standards such as TCP/IP and HTTPS, low-cost Internet access and protocols supporting e-payment activities. The implementation of e-payment protocols indicates how robust the e-commerce system should be. A reliable and robust transmission infrastructure usually plays a significant role in e-commerce security and enhanced e-payment system. An e-payment system is for online payment; hence, its essential function is to transfer money from one entity to another or make a payment over the internet provided certain agreements are met to fulfill e-commerce technical standards. Some online protocol which supports secure e-commerce are iKP family Protocols, Secure Electronic Transaction (SET), One-Time Payment Scheme (OTPS), Live Cardholder Authentication, Secure Socket Layer (SSL) and Robust E-Payment Protocol (REPP) (Takyi and Gyaase, 2012; Levi and Kroc, 2001; Li, 2008).

SET is an open encryption and security protocol designed to protect the e-payment system online. In the SET protocol, all parties are required to possess their public-key certificates, whereas iKP protocol consists of three versions depending on the number of certificates possessed by engaging parties: 1KP, 2KP and 3KP. In 1KP, only the payment gateway is required to have its certificate. Both the client and the merchant can authenticate themselves to the payment gateway and each other using Private Identification Numbers (PINs). In 2KP, only the client is not required to possess the certificate. Finally, 3KP protocol requires all engaging parties to possess their certificates.

REPP is a convenient online e-payment protocol which offers the card users the options to make changes to or stop online transactions. As suggested by (Takyi and Gyaase, 2012) REPP fares better when compared theoretically with live card user verification in terms of security, usability, verification of card user and execution.

OTPS is an e-payment protocol designed to generate unique transaction values for single use in each transaction.

USSD Payment

The Unstructured Supplementary Services Data (USSD) is a session-based and real-time communication technology in mobile communications. This technology is used in sending messages across a GSM network between a mobile client and an application server. This service operates much like SMS, but its session-based and interactive nature distinguishes the two. Unlike SMS, it does not operate by store-and-forward and its turnaround response time is much shorter for interactive applications than it is for service like SMS (Shrivastava, 2012; Roy Laurens and Zou 2016; Owusu *et al*., 2017).

This makes USSD much faster and very cost-effective as it involves simple operations that are also handset independent (old handsets to most new smartphones can all access the service). As indicated in Fig. 3, USSD applications are characterized by menu-driven and interactive services and a request is invoked by dialling a number that is composed of asterisks (*) and hashes (#). Examples of these services include sports updates, movies, weather information, news, stock market, reservation applications (for planes/trains/ movies, etc.), voting/polling applications, mobile account balance checking and top up and many others (Abedi *et al*., 2019; Van Bavel *et al*., 2019; Barkatullah and Djumadi, 2018).

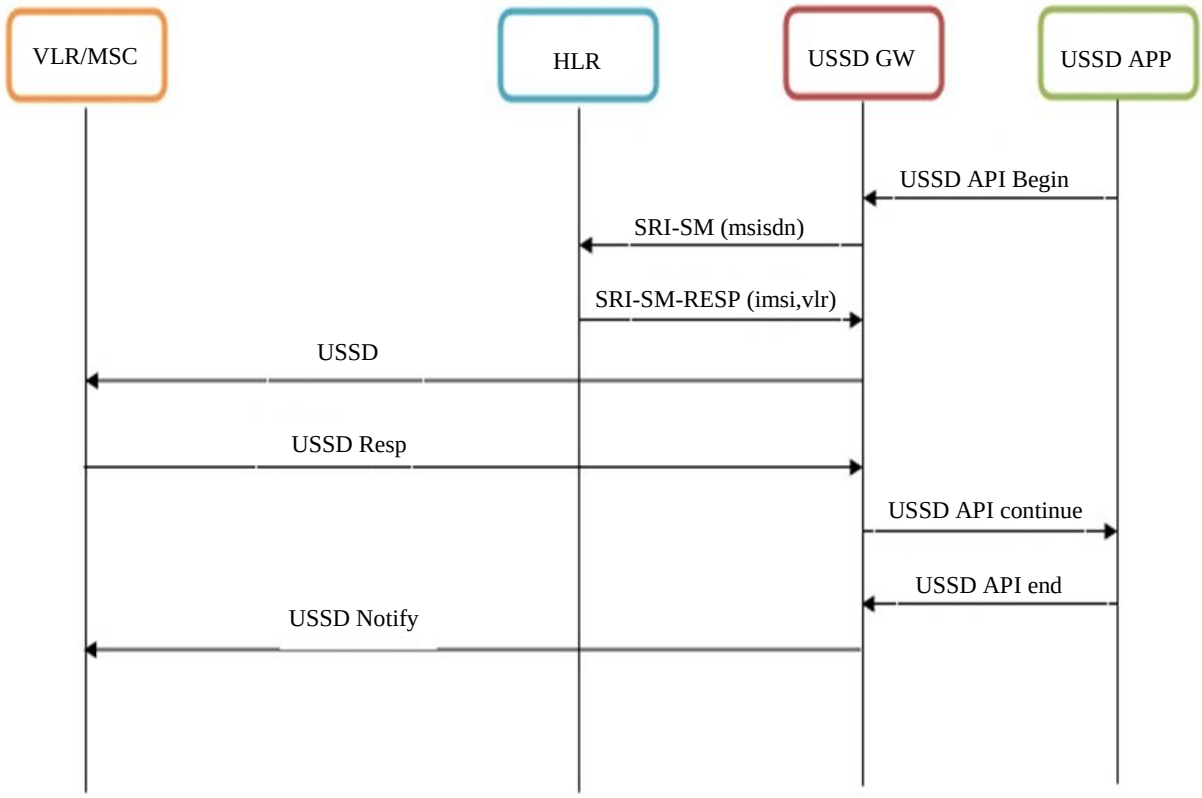

Fig. 3: USSD scheme

Password Security Using SHA Algorithms

The SHA (Secure Hash Algorithm) is a cryptographic hash function which is similar to MD5 except it **creates** more resilient hashes. These hashes may not always be unique, that means two different inputs but equal hashes; when this happens, it is called a collision. Thus, the likelihoods of collision in SHA are less than MD5. Generally, the collisions in the hash functions are infrequent. Java has four implementations of the SHA algorithm. In the real-world implementation of SHA-1, the longer hashed password is more challenging to break. The CVV number, according to the proposed framework, will deploy SHA function to make it more secure and unbreakable (Sriramya and Karthika, 2015).

The Proposed Optimized Online Payments Authentication (OOPA)

Authentication is an exceptionally essential security measure in the e-commerce security scheme. In order to ensure that the card owner is the person conducting the online transaction, there must be some form of secure authentication and non-repudiation (Shrivastava, 2012). The information on the electronic card is paramount in e-commerce. Should someone steals an electronic card, the person will automatically have access to all the information required for online purchases, thus, the name, credit card number, expiry date and the CVV number. However, if there is no CVV code at the back of the card, the criminal will not be able to purchase goods online (Xiao *et al*., 2008; Yang *et al*., 2019).

Cardholder authentication should be a critical factor in setting up online payment protocol, as most of the existing protocols are silent (Takyi and Gyaase, 2012) and remain the top challenge in the e-commerce industry. The new authentication scheme ensures the merchant become verifiable, to enable the cardholder to feel secure and confident to do business with the merchant online. Moreover, the ease of implementation for such authentication should be paramount (Owusu *et al*., 2017; Carta *et al*., 2019).

The OOPA incorporates a solution to the above weaknesses identified in the existing protocols where new authentication codes are generated by the card issuer instead of the CVV number. When the buyer checkout and proceed to payment from a merchant website, the merchant sends a notification SMS to the buyer through the mobile phone number the cardholder used for registration. The buyer then sends the CVV through USSD service to a short code (e.g., ∗0000#).

How the Proposed OOPA Model Works

In Fig. 4, a cardholder initiates transaction process by providing electronic card information without the CVV to the merchant.

Purchase Request

Card Owner makes an online transaction at the merchant website (Process M).

Authentication and Authorization Request

Merchant alert Bank to authenticate card information and available funds (Process N).

Authentication and Encryption

Bank request card owner to submit an authentication code (CVV number) through a secure (encrypted CVV number) USSD service. (Process O).

Authorization

Card owner submits encrypted authentication code to bank through USSD. (Process O).

Authentication and Authorization

Bank asks card Issuer to authenticate the authentication code of card owner. (Process P).

Encryption

This ensures submission of authentication code is securely Encrypted and Hashed. (Process Q, R).

Authorization

Bank authorizes payment of an online transaction, where the cost of services rendered must be deducted from the account of the cardholder. (Process N).

Purchase Response

The merchant sends a purchase response to the card owner in the form of successful transaction and receipt through USSD (Process M).

The Process Involved in Encrypting and Decrypting the CVV Number

Consider a cardholder known as A, who want to transact business by sending payment message and CVV to the card issuer known as B, securely.

Let e be B's public key. Since e is public, A has access to e.

To encrypt the message P, represent the message as an integer in the range 0<P:

i. P is the (finite) set of plaintexts for the CVV value
ii. C is the (finite) set of ciphertexts which is encrypted CVV
iii. K is the (finite) set of keys for end-to-end USSD communication
iv. $E = \{E_k : k \in K\}$ is the transactions encryption functions $E_k : P \rightarrow C$
v. $D = \{D_k : k \in K\}$ is a family of decryption functions $D_k : C \rightarrow P$
vi. For all $e \in K$ there exists a $d \in K$ such that we have $D_d(E_e(p)) = p$ for all plaintexts $p \in P$

where E_k and D_k are the encryption and decryption key respectively for the public key infrastructure USSD communication system.

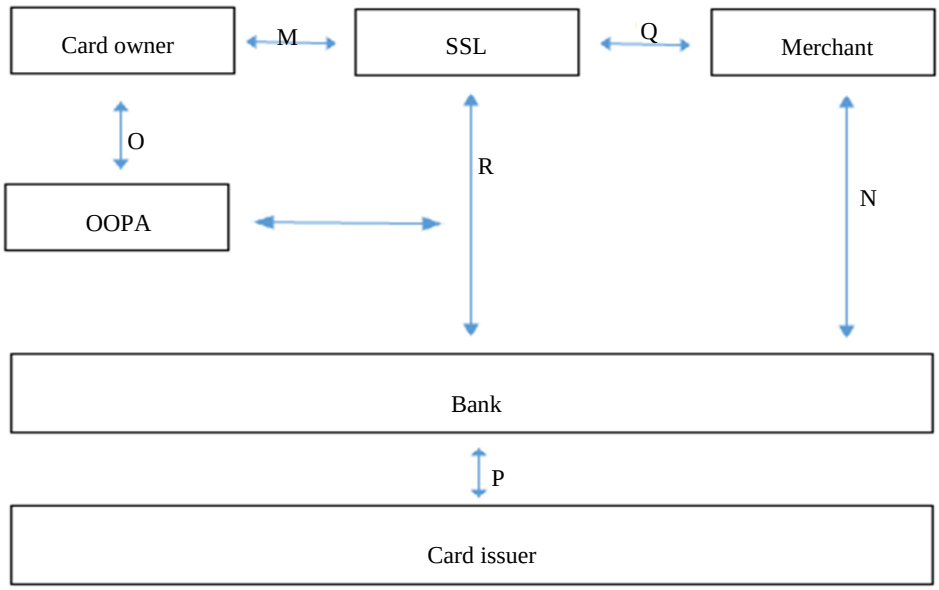

Fig. 4: Optimized Online Payments Authentication (OOPA) transaction model

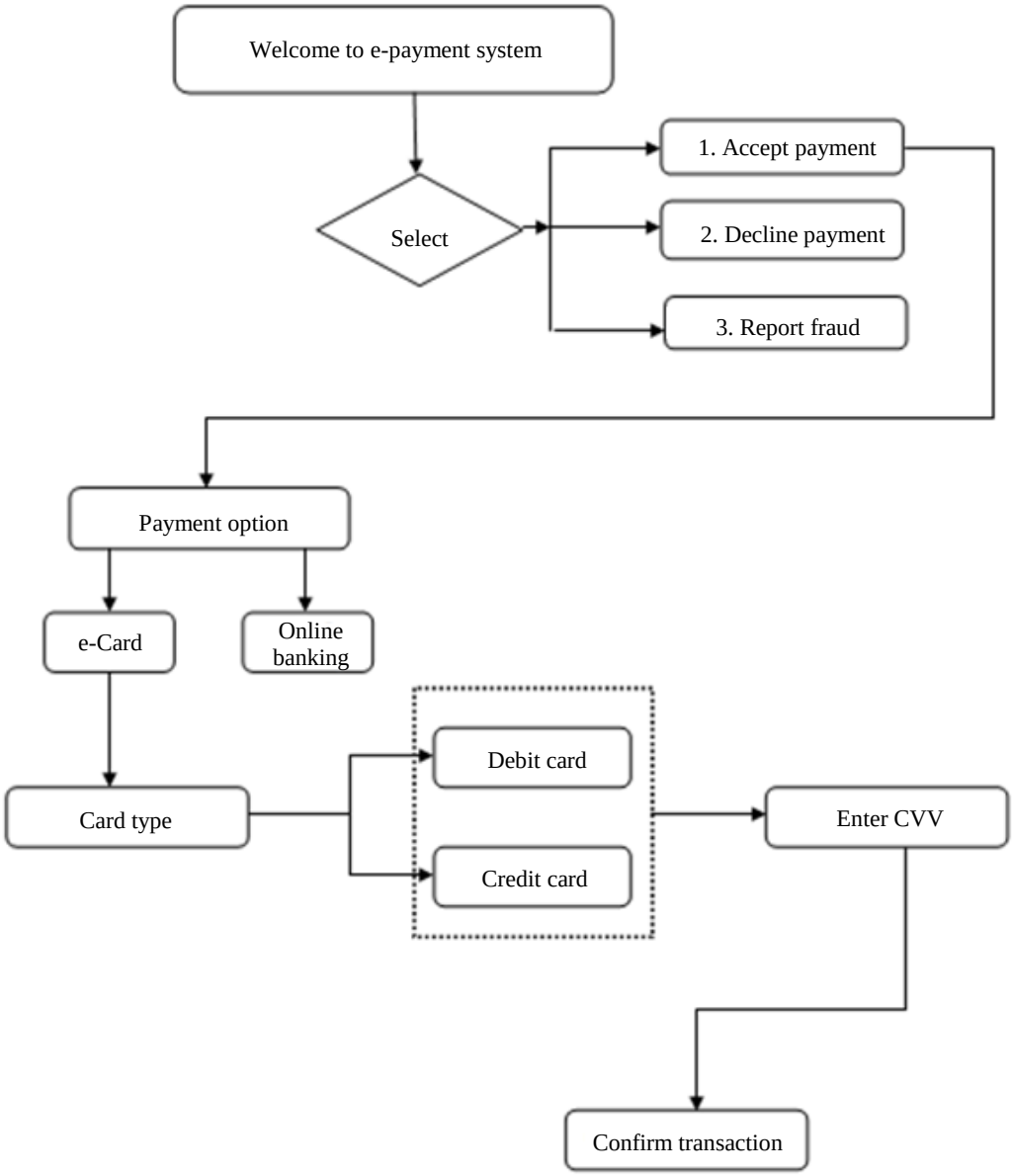

Fig. 5: USSD architecture in OOPA system

The equations show how to encrypt and decrypt the transaction detail and CVV and then forwarded to the merchant the issuer for verification.

The encrypted CVV is sent to the bank for authorization and the onward submission to the merchant for payment to be affected. The item is then delivered to the card owner to complete the transaction process (Takyi and Gyaase, 2012; Owusu *et al*., 2017; Barbosa *et al*., 2019).

USSD Architecture and Operation

The USSD architecture for the proposed OOPA model is illustrated in Fig. 5. When the service is invoked, a real-time, interactive session is established between a user, the card issuer and the bank. This allows transaction details to be exchanged between the user and the bank until the service is completed. A session needs to be allocated to every transaction request; the response for this request and the following series of requests and responses in that session all share the same request-acknowledgement-response handshake until the transaction is confirmed (Appiah *et al*., 2017; Nedjah *et al*., 2019). The communication can be established even when a call is active because the two services use different communication channels (Owusu *et al*., 2017). USSD services use a signalling channel while call services use traffic channels.

Table 1: Comparison of the proposed OOPA with existing protocols

Protocol	Security	Usability	Card owner authentication	Verification of merchant	Card owner termination	Implementation
iKP	Secured	Complex	Good	Yes	No	Complex
SET	Secured	complex	Good	Yes	No	Complex
SSL	Secured	Convenient	Seldom	No	No	Easy
REPP	Secured	Convenient	Good	Yes	Yes	Easy
OOPA	Secured	Convenient	Excellent	Yes	Yes	Easy

Authentication and Authorization Process

The card issuer receives a request for CVV authentication from the bank, the issuer checks the CVV and compare with the actual value to either accept or deny the transaction. The issuer clears the card owner and submits acceptance response to the Bank. The bank dispatches a text message to the card owner to request for the CVV number. The card owner must supply the exact CVV to match with what the Bank has in its system before the bank could instruct the merchant for payment or the system to deny and abrogate the transaction if the CVV number fails to match the value in the bank. The card owner must protect the CVV and keep it safe from any third person.

The merchant shall receive authorization from the payment gateway or the bank and then confirms the purchase to the card owner or declines. In this case, the card owner has authority to accept or deny payment. A copy of the confirmation message would be sent to the card owner's email address, including an official receipt of the transaction (Owusu *et al*., 2017; Appiah *et al*., 2017).

Comparative Analysis

Many protocols have been proposed and implemented in the e-commerce ecosystem. The chain of processes in the e-commerce space involves several security protocols which include access controls and secure authentication. There has been a continuous improvement in the authentication process in the online business and each proposed has proven to be robust and then known vulnerabilities have been identified by other researchers. REPP, as proposed by (Takyi and Gyaase, 2012), requires dual signatures, which increases processing time and it was silent on the CVV number, which still possed danger to the card user. Table 1 illustrates the various secure transmission protocols on the internet. The TCP/IP secure scheme has improved over the years from onset to SET, SSL and REPP, but each protocol has a weakness and another is an improvement over another (Fourati *et al*., 2002; Shu and Cheng, 2012).

Theoretically, the implementation of the proposed OOPA shall improve secure online transactions and the threat that CVV number posses to users would be eliminated. In the OOPA system, no CVV number shall be written at the back of the e-card, but the number shall be used as a password to authenticate the transaction. Unlike the other techniques, which was silence on the threat that CVV numbers posses to the card owner, the OOPA has dealt with that weakness. The CVV number must not be embossed on the card as has been done previously. The proposed protocol has an encrypted scheme which protects the card owner from replay attacks and eavesdropping. The user also has an added advantage to accept or deny transaction payments.

When the OOPA model is implemented in real-world as a security protocol in the online payment system, it will significantly help to decrease the fraud associated with the e-payment system. OOPA is designed to offer end-to-end security than the existing schemes such as the Robust Electronic Payment Protocol which requires a merchant to register and obtain a certificate from a trusted Certificate (SSL) Authority before an online payment service could be confirmed (Takyi and Gyaase, 2012).

Conclusion

The proposed OOPA secure model is yet to be implemented practically, but the theoretical analysis with other protocols indicate that it is an optimized model which has the potential to enhances e-commerce security, reduces e-payment frauds and improves access control and authentication scheme. However, OOPA has given all the authentication process to the bank as the primary payment gateway. Cybercriminals mostly deploy sophisticated and advanced technology to intercept or steal sensitive information online but will have difficulty to break into the OOPA architecture.

Nevertheless, the study results indicate that OOPA model has the capability and proficiency to minimize online fraud; it is also convenient and easy to implement OOPA in the e-commerce ecosystem. The proposed protocol is a fraud detection system which serves as an antidote to the topical frauds schemes in the e-payment system.

In future research, an intelligent system could be implemented to check unusual transaction pattern, authenticate transactions to avoid fraudulent activities or unauthorized access to card users accounts, as quickly as possible to save them from loss of funds. Banks and card issuers must adopt this new protocol which protects the customer from undue fraudulent activities to avoid complete loss of funds on customers electronic card.

Author's Contributions

The authors contributed equally to this paper.

Ethics

All the sections, the research organization and all other aspects of this paper were originally written by the authors unless otherwise referenced.

References

Abedi, F., J. Zeleznikow and C. Brien, 2019. Developing regulatory standards for the concept of security in online dispute resolution systems. Comput. Law Security Rev. DOI: 10.1016/J.CLSR.2019.05.003

Appiah, V., I.K. Nti and O.N. Boateng, 2017. Investigating websites and web application vulnerabilities: Webmaster's perspective. Int. J. Applied Inform. Syst.
DOI: 10.5120/ijais2017451673

Barbosa, G., P.T. Endo and D. Sadok, 2019. An internet of things security system based on grouping of smart cards managed by field programmable gate array. Comput. Electrical Eng., 74: 331-348.
DOI: 10.1016/J.COMPELECENG.2019.02.013

Barkatullah, A.H. and Djumadi, 2018. Does self-regulation provide legal protection and security to e-commerce consumers. Electro. Commerce Res. Applic., 30: 94-101.
DOI: 10.1016/J.ELERAP.2018.05.008

Carta, S., G. Fenu, D.R. Recupero and R. Saia, 2019. Fraud detection for e-commerce transactions by employing a prudential multiple consensus model. J. Inform. Security Applic., 46: 13-22.
DOI: 10.1016/J.JISA.2019.02.007

Ford, W., 2001. Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption. 2nd Edn., Prentice Hall,
ISBN-10: 0130272760, pp: 640.

Fourati, A., H.K.B. Ayed, F. Kamoun and A. Benzekri, 2002. A SET based approach to secure the payment in mobile commerce. Proceedings of the 27th Annual IEEE Conference on Local Computer Networks, Nov. 6-8, IEEE Xplore Press, Tampa, FL, USA. DOI: 10.1109/LCN.2002.1181777

Hwang, J.J., T.C. Yeh and J.B. Li, 2003. Securing on-line credit card payments without disclosing privacy information. Comput. Stan. Interfaces, 119-129. DOI: 10.1016/S0920-5489(02)00102-2

Law, M., R.C.W. Kwok and M. Ng, 2016. An extended online purchase intention model for middle-aged online users. Electro. Commerce Res. Applic., 20: 132-146.DOI: 10.1016/j.elerap.2016.10.005

Leavitt, N., 2010. Payment applications make e-commerce mobile. Comput., 43: 19-22.

Levi, A. and C.K. Kroc, 2001. CONSEPP: Convenient and Secure Electronic Payment Protocol Based on X9.59. Proceedings of the 17th Annual Computer Security Applications Conference, Dec. 10-14, IEEE Xplore Press, LA, USA.
DOI: 10.1109/ACSAC.2001.991544

Li, Y., 2008. The design of the secure electronic payment system based on the SET. Proceedings of the International Conference on Computer Science and Information Technology, Aug. 29-Sept. 2, IEEE Xplore Press, Singapore.
DOI: 10.1109/ICCSIT.2008.175

Luhach, A.K., S.K. Dwivedi and C.K. Jha, 2014. Designing a logical security framework for E-commerce system based on SOA. Int. J. Soft Comput.

Nedjah, N., R.S. Wyant, L.M. Mourelle and B.B. Gupta, 2019. Efficient fingerprint matching on smart cards for high security and privacy in smart systems. Inform. Sci., 479: 622-639.
DOI: 10.1016/J.INS.2017.12.038

Owusu, N.B., M. Asante and I.K. Nti, 2017, Implementation of advanced encryption standard algorithm with key length of 256 bits for preventing data loss in an organization. Int. J. Sci. Eng. Applic.

Roy Laurens, C. and C. Zou, 2016. Using credit/debit card dynamic soft descriptor as fraud prevention system for merchant. Proceedings of the Global Communications Conference, Dec. 4-8, IEEE Xplore Press, Washington, DC, USA, pp: 1-7. DOI: 10.1109/GLOCOM.2016.7842369

Shrivastava, M., 2012. A multifactor authentication security protocol to prevent risks posed by phishing, for internet based online payment system.

Shu, W. and C.Y. Cheng, 2012. How to improve consumer attitudes toward using credit cards online: An experimental study. Electro. Commerce Res. Applic., 11: 335-345.
DOI: 10.1016/j.elerap.2012.01.003

Sriramya, P. and R.A. Karthika, 2015. Providing password security by salted password hashing using bcrypt algorithm. ARPN J. Eng. Applied Sci.

Strategy, J., 2017. https://www.javelinstrategy.com/

Takyi, A. and P.O. Gyaase, 2012. Enhancing security of online payments: A conceptual model for a robust e-payment protocol for e-commerce. Proceddings of th International Conference on E-business Technology and Strategy, (ETS' 12), Springer, Berlin, Heidelberg, pp: 232-239.
DOI: 10.1007/978-3-642-34447-3_21

Turban, E., J.K. Lee, D. King, T.P. Liang and D. Turban, 2010. Electronic Commerce: Managerial Perspective. 1st Edn., Prentice Hall.

Van Bavel, R., N.R. Priego, J. Vila and P. Briggs, 2019. Using protection motivation theory in the design of nudges to improve online security behavior. Int. J. Human-Comput. Stud., 123: 29-39. DOI: 10.1016/J.IJHCS.2018.11.003.

Xiao, H., B. Christianson and Y. Zhang, 2008. A purchase protocol with live cardholder authentication for online credit card payment. Proceedings of the 4th International Conference on Information Assurance and Security, Sept. 8-10. IEEE Xplore Press, Naples, Italy. DOI: 10.1109/IAS.2008.44

Yang, W., J. Li, Y. Zhang and D. Gu, 2019. Security analysis of third-party in-app payment in mobile applications. J. Inform. Security Applic., 48: 102358-102358. DOI: 10.1016/J.JISA.2019.102358.