International Journal of Information System and Engineering
Vol. 4 (No.2), November, 2016
ISSN: 2289-7615
DOI: 10.24924/ijise/2016.11/v4.iss2/09.27

IJISE
www.ftms.edu.my/journals/index.php/journals/ijise

A PROPOSED ONLINE SHOPPING AND PAYMENT FRAMEWORK WITH APPLICATION OF ENCRYPTION AND STEGANOGRAPHY FOR ENHANCED SECURITY

Babangida Zachariah
FTMS College Cyber Jaya, Malaysia
daddonyone@gmail.com

Mohamed Ismail Z.
Senior Lecturer, SOECS
FTMS College Cyber Jaya, Malaysia
ismail@ftms.edu.my

Abstract

Advances in technology has made online shopping such an interesting thing, providing online access and payment for products or services. However, security remains a concern. The use of sniffing tools, phishing and other social engineering techniques often prevail against the existing security systems. Therefore, this research proposes a framework that actively involves customers in the processes of online shopping and payment using Online Payment Alternative Solution (OPAS), a mobile application developed. To enhance the security of the proposed framework, Blowfish encryption of dynamic One Time Password (OTP) and One Time Password Encryption Key (OTPEK) generation algorithm are used. The encrypted OTP and OTPEK are then embedded in a captcha image using a Least Significant Bit (LSB) steganography; and then sent to the customer's OPAS for payment approval in near real time. The developed systems were tested and found to be working as accurately based on the generated test cases.

1.0 Introduction

The advances in technologies have greatly changed the way things are done, ranging from education, governance, manufacturing, shopping, etc. It has made sales and purchases (shopping) of goods and services from any part of the world such an easy task to accomplish through the use online merchant service (online stores) and online payment methods or some others such as Cash on Delivery (COD), Cheque/Check, Debit card, Direct Debit, Electronic Money, Gifts Card, Postal Money Order, Wireless Transfer/Delivery on Payment (DOP), Invoice, Bitcoins (Lopresti, 2007; Rao, 2010). These concepts are simply referred to as Online Shopping or e-tail.

In online shopping, customers assess, order and make payments for their order either online or on delivery. When payment is made online, the customer provides merchant with their Bank Card details such as card number, expiry month, expiry year, card holder name, card CVV and card pin. With these information, the merchant can request payment from customer's bank and withdrawals are made from the customer's bank.

Though this approach has made shopping faster and better, it has introduced security challenges. Hackers employ social engineering, phishing (Murugeswari, et al., 2015), sniffing, etc. to steal these

information from the customer for malicious purpose (More, et al., 2015). These forms of identity theft has a lot of financial implications. For example, in a report by Douglas (Douglas, 2010), 7% of all adults in the USA are victims of identity theft and on the average $3,500 is lost in each incidence. In another report of February 2014, titled "Third Report on Card Fraud", European Central Bank showed that of the 0.02% increase over the 2011 cases, One-Point-Thirty-Three billion Euros (€1.33 billion) was lost due to total fraudulent transactions in 2012, 60% was due to internet/telephone payments, 23% due to Point-of-Sale (POS) terminals, and 17% due to Automated Teller Machines (ATMs) (Bank, 2014). These imply that more security required of online shopping and payment systems. The rising concern in data communication such as this has led to the development of several security measures and techniques such as cryptography (Kahn, 1996) and steganography (Kefa, 2004). These security measures have enhanced security of the online payment systems, the required level of security is yet to be attained. The use of cryptography alone is not efficient; the use of steganography alone is not efficient. Thus, the two techniques are usually combined for enhanced security (Babangida, et al., 2016).

Though combining cryptography and steganography would enhance security to a great extent, it still stand the higher chance of being bridged. Once a cover media is suspected, steganalysis is used to retrieve the encrypted secret information and different attack techniques such as brute-force methods could be used to decrypt the retrieved encrypted information. This implies that more security is required especially in online payment systems where hackers have more interest. Therefore, this research proposes a new framework and tool which actively involves the user or customer in the payment process.

2.0 Literature Review

There are a lot of research in the area of online shopping and payment security which proposes the use of cryptography and/or steganography.

In the work of (Souvik & Venkateswaran, 2014) an online payment method was proposed which applies steganography and visual cryptography for enhancing security of payment process. The cryptography technique used took advantage of the inflexion, periphrases, and fixed word order when encrypting the payment details with enhanced flexibility. The steganography approach proposed is based on Vedic Numeric code and the stego image is also encrypted. The proposed payment method introduced a central Certified Authority (CA) through which the customer payment is verified.

Similarly, the works of (Murugeswari, et al., 2015) used Bit Plane Complexity Segmentation (BPCS) steganography; and (Chetan, et al., 2015) which used text-based steganography; and both used visual cryptography to implement a secure electronic payment system. The stego image containing the payment verification details is encrypted and forwarded to the CA and then to the Bank for transfer to made. The challenge with these is that since customers are redirected to CA portal for verification, fraudulent merchant could redirect a customer to its phishing portal that looks like the original CA portal.

In the work of (Khonde, et al., 2014), visual cryptography and Bit-Plane Complexity Segmentation (BPCS) steganography approach with the introduction of Certified Authority (CA) was used to encrypt and embed customer bank card details in an online shopping system. The visual cryptography component then creates two parts of the stego file, one for the customer and the other for the CA. The CA browses the customer share and retrieves the card details and then forward to the bank for payment to the merchant. Also, in (Murugeswari, et al., 2015), the same model was used but instead of image steganography, text-based steganography was used. These offered the security of card details against eavesdroppers but not against the merchants.

In the work of (Reddy & T., 2015), visual cryptography was used to encrypt data in an image and the image was also encrypted. The encrypted image is divided into two, one for the customer and the other for the CA. Just like the other previous studies, the CA retrieves the embedded data which are the secret

keys and forwards a payment request from the bank to the merchant's account. Like before, encrypting an image make it prone to malicious attacks.

In the work of (More, et al., 2015), a new framework for online shopping and payment was proposed. Instead of doing steganography at the merchant website like others, where the customer still has to submit Bank card details to the merchant, the Merchant registers with a bank just like a Customer. When a Customer checks out at the Merchants site, he submits only his account number, the Merchant use the account number to request payment from the bank. At the bank, a One-Time-Password (OTP) is generated through steganography, visual cryptography then splits the OTP into two shares and sent one to the merchant and the other to the client through Email, and then the communication between the customer and the merchant leads to the retrieval of the complete OTP which is then sent to the bank server by the client for verification, and payment is made according to the validity of the OTP. This offered the best security of all the approaches since the customer approves payment. Thus, customer's confidence in the security of his bank account balance is improved. However, using emails which are also prone to attacks makes the system inefficient.

Looking at the security loopholes present in the existing systems, the need for a more robust and secure approach to online shopping and payment becomes a necessity. Such a system should not only improve the security of the process but should be such that customers are directly involved in payments so that their confidence in the process would also be improved. Therefore, the purpose of this research work is to propose a framework, and apply a steganography and cryptography algorithm to the implementation of systems based on the framework.

3.0 Research Design and Methodology

For the purpose of this research, the opinions of users was acquired and analyzed using questionnaire. The questionnaire was developed using google forms and the link was posted on social media such as Facebook, and WhatsApp groups, also, personal messages to people on Facebook were sent containing the link and a request for them to fill the questionnaire. The responses submitted were Ninety-One (91). The responses based on questions are presented below.

Result and Analysis of Questionnaire Responses

Question One: Do you have any idea about Steganography? * (Hiding messages within innocent looking files)

Options	Responses	Percentages
No	28	30.77%
Partially	24	26.37%
Yes	39	42.86%
Total	**91**	**100%**

Table 3.1: Respondents' Familiarity with Steganography.

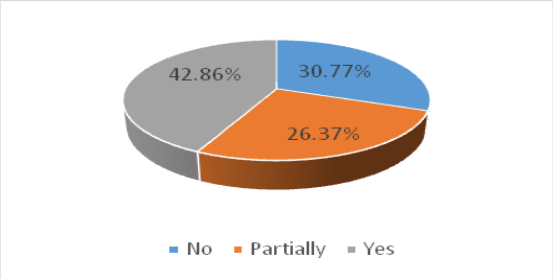


Chart 3.1: Respondents' Familiarity with Steganography.

Question one sought to find out the familiarity of the respondents on the concept of steganography irrespective of how and where they have used the concept. The result shown in Table 1 and depicted in Chart 1 shows that most respondents have a definite idea of the concept, more have some idea, and the rest have no idea at all. The implication of this could be that most of the respondents might have used or read about steganography before.

Question Two: Do you have any idea about Encryption and Decryption? *

Options	Responses	Percentages
No	12	13.19%
Partially	17	18.68%
Yes	62	68.13%
Total	**91**	**100%**

Table 3.2: Respondents' Familiarity with Encryption.

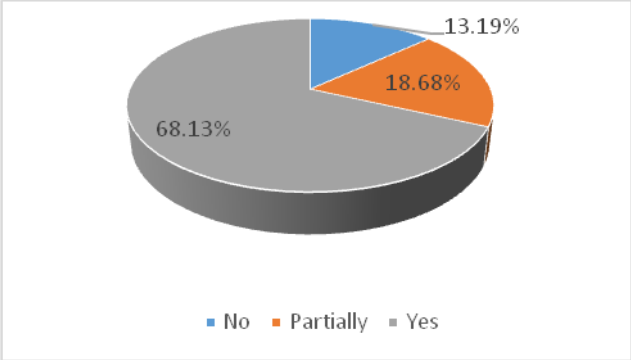


Chart 3.2: Respondents' Familiarity with Encryption.

Question two sought to find out the respondents' knowledge of the concept of Encryption and Decryption irrespective of where and how they might have to use the concept. The result shown in Table 2 and depicted in Chart 2 shows that most of the respondents have definite knowledge of the concept, some have partial knowledge and the rest with no knowledge at all. Also, like in question one, the implication might be that most respondents have used or read about Encryption and Decryption somehow.

Question Three: Have you ever transmitted any secret message before? *

Options	Responses	Percentages
Never transmitted any before.	53	58.24%
Transmitted once (one time).	10	10.99%
Transmitted more than once, like five times.	6	6.59%
More than five times, but not often.	11	12.09%
Often transmit secret messages.	11	12.09%
Total	**91**	**100%**

*Table 3.**Error! No text of specified style in document.**: Respondents' Use of Steganography.*

ISSN: 2289-7615

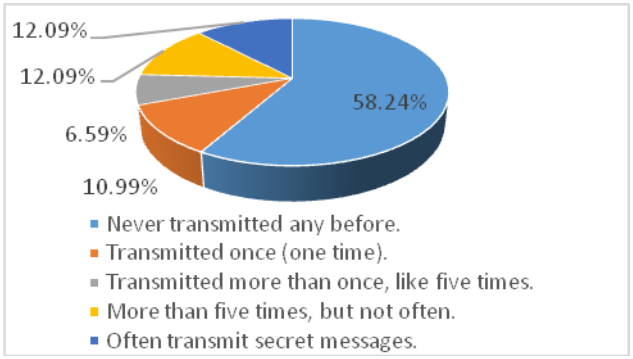


*Chart 3.**Error! No text of specified style in document.**: Respondents' Use of Steganography.*

Question Three sought to find out the use of Steganography by the respondents. Results shown in Table 3 and depicted in Chart 3 shows that most of the respondents have never applied Steganography consciously, a number of them have actually applied the concept either once or more times. Though 58.24% have not transmitted secret messages, it can be implied from Question one and on the results of Question two that more people with definite knowledge of steganography have transmitted secret message at least once.

Question Four: Have you ever made an online payment? *

Options	Responses	Percentages
Never transmitted any before.	53	58.24%
Transmitted once (one time).	10	10.99%
Transmitted more than once, like five times.	6	6.59%
More than five times, but not often.	11	12.09%
Often transmit secret messages.	11	12.09%
Total	**91**	**100%**

Table 3.4: Respondents' Use of Online Payment Systems.

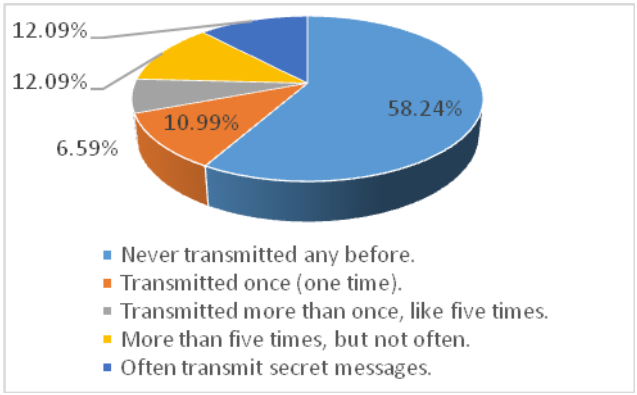


Chart 3.2: Respondents' Use of Online Payment Systems.

The objective of Question four was to find out if respondent has ever used the online payment system such as during online shopping. The results shown in Table 4 and depicted in Chart 4 shows about 10.99% have used online payment system at least once, 6.59% have use between one and five times, 12.09% have use more than five times, and another 12.09% often use the online payment system. This sums up to 41.76% of the respondents who have actually used the online payment systems at least once. The implication of this could be that the respondents do not trust the security of payment systems (afraid of online scams) or they just do not have a need for anything online. However, looking at the modern day

ISSN: 2289-7615

world where businesses have gone online, there should be more users of online systems than the result suggest.

Question Five: What do you think about the security of Bankcard (Master/Visa/...) details submitted to the merchants? *

Options	Responses	Percentages
Not Secured	11	12.09%
Partially Secured	64	70.33%
Secured	16	17.58%
Total	**91**	**100%**

Table 3.5: Respondents' Opinions on Security of Card Details and Merchants.

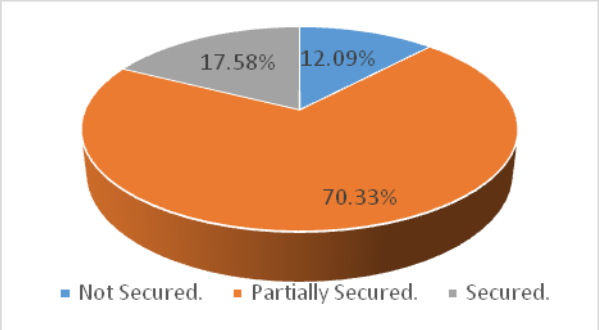


Chart 3.3: Respondents' Opinions on Security of Card Details and Merchants.

Question five sought to find out what the respondents think of security when purchasing and making online as it regards submission of their Bank Card details to Merchants. The results as shown in Table 5 and Chart 5 suggest that only a few (17.58%) of the respondents trust the security of the process, more, *70.33%* partially trust the security of the process, and 12.09% do not trust the process.

Question Six: Do you feel concerned giving your Bank card (Master/Visa/...) details to online stores/merchants for payments purpose? *

Options	Responses	Percentages
No	24	26.37%
Partially	19	20.88%
Yes	48	52.75%
Total	**91**	**100%**

Table 3.6: Respondents' State of Mind Submitting Card Details to Merchants.

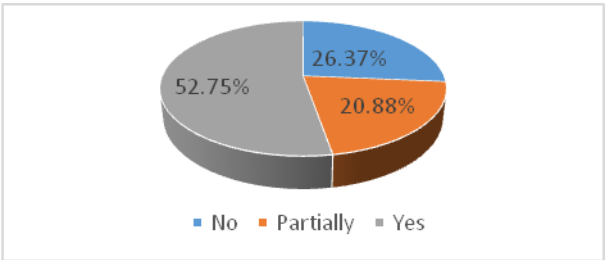


Chart 3.4: Respondents' State of Mind Submitting Card Details to Merchants.

ISSN: 2289-7615

To be able to confirm the result of Question five, the researcher included Question six which sought to find out explicitly if the respondents have any concerns relating to submission of their Bank Card details to online stores. The results are shown above in Table 6 and depicted in Chart 6 shows that 26.37% definitely have concerns submitting their payment card details, 20.88% are partially concerned, and 52.75% are never concerned. This concerns most likely are related to security and possibility of online scams such as phishing, eavesdropping, and/or identity theft; and this must be the confirmation of the results of Question five.

Question Seven: Have you ever being a victim of identity theft online? *

Options	Responses	Percentages
No	77	84.62%
Yes	14	15.38%
Total	**91**	**100%**

Table 3.7: Respondents as Victims Online Identity Theft.

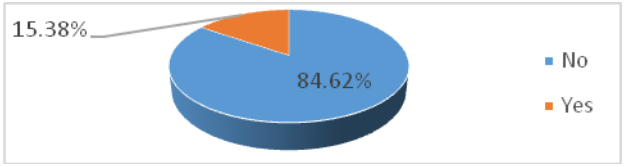


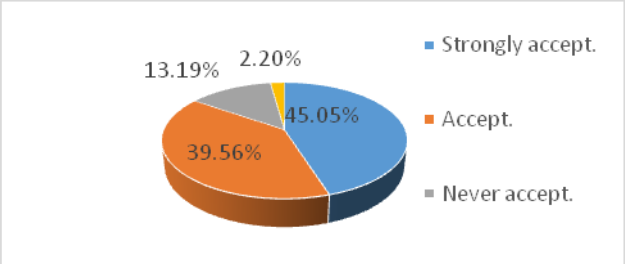
Chart 3.5: Respondents as Victims Online Identity Theft.

Question seven sought to find out how many of the respondents have at any point in time being victims of identity theft online. The results as shown in Table 7 and depicted in Chart 7 suggest a few (15.38%) have actually been victims of online identity theft. However, comparing the number of victims (14) in this result of Question seven to the number (38) of those who have at least for once used the online payment systems as in Question four, it shows that a significant number of those respondents who have used online payment systems have being victims. The implication of this result suggests that there is high risk of falling a victim.

Question Eight: Would you like and accept a system where you make payments to any merchants/store directly from your bank without having to give your card details to the merchant? *

Options	Responses	Percentages
Strongly Accept	41	45.05%
Accept	36	39.56%
Never Accept	12	13.19%
None of the Above	2	2.20%
Total	**91**	**100%**

Table 3.8: Respondents' Acceptance of a New Secured System.



ISSN: 2289-7615

Chart 3.6: Respondents' Acceptance of a New Secured System.

Having assessed the feelings of the current state of the processes of online payment, the researcher sought to find out if users would accept a new approach to online payment. Question Eight sought to find the degree of acceptability of the system based on the concept the research would propose and found that many users (39.56%) have a strong will to accept the proposed system, and more without too strong will also accept the system. However, a few (about 13.19%) would not; while 2.20% are indifferent. The implication of this result suggests that users actually need more security on payment systems than the current systems provide.

Question Nine: Do you think Steganography and Encryption can be implemented in online payments to improve security? *

Options	Responses	Percentages
Strongly Agree	31	34.07%
Agree	54	59.34%
Disagree	1	1.10%
Strongly Disagree	0	0.0%
None of the Above	5	5.49%
Total	**91**	**100%**

Table 3.9: Respondents' Perception on Steganography, Encryption, and Security Systems.

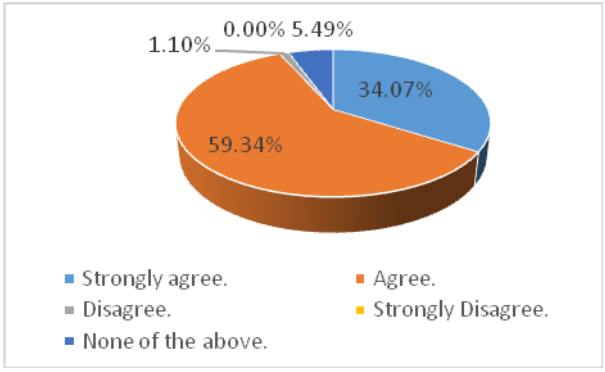


Chart 3.7: Respondents' Perception on Steganography, Encryption, and Security Systems.

Question nine sought to find out the potential of the acceptability of the application of Steganography and Cryptography to the security payment system to be proposed by the researcher. The result in Table 9 and depicted in Chart 9 suggest high acceptability.

ISSN: 2289-7615

Question Ten: Steganography and/or Encryption is a threat to individuals or organizations? *

Options	Responses	Percentages
Strongly Agree	9	9.89%
Agree	21	23.08%
Disagree	46	50.55%
Strongly Disagree	8	8.79%
None of the Above	7	7.69%
Total	**91**	**100%**

Table 3.10: Respondents' Perception on Steganography, Encryption, and Individuals/Organizations.

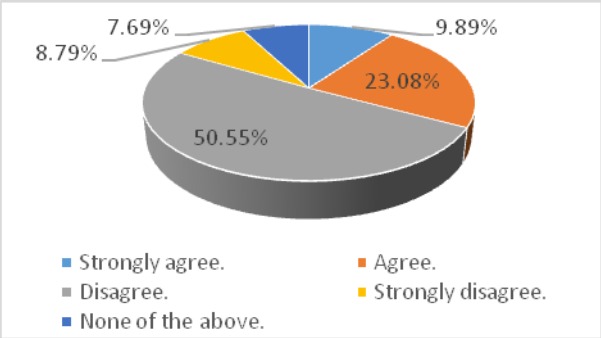


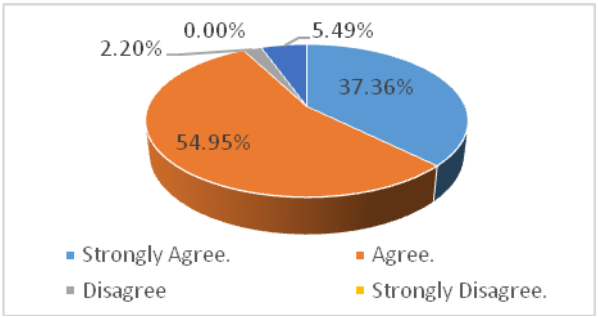
Chart3.8 : Respondents' Perception on Steganography, Encryption, and Individuals/Organizations.

Question ten sought to find out the perception of the respondents on the application and implication of steganography on the security of communications as it relates to individuals and/or organizations. Results shown in Table 10 and depicted in Chart 10 suggest that more than 50% do not see steganography as a threat to individuals nor organizations. However, a significant number show that they perceive steganography and cryptography as a threat. The implication of this result is that more awareness might be required on the concepts.

Question Eleven: Do you think Steganography and Encryption are worth investing on for security of online payments?*

Options	Responses	Percentages
Strongly Agree	34	37.36%
Agree	50	54.95%
Disagree	2	2.20%
Strongly Disagree	0	0.00%
None of the Above	5	5.49%
Total	**91**	**100%**

Table 3.11: Respondents' Will to Invest on Steganography and Encryption for Security.



ISSN: 2289-7615

Chart 3.9: Respondents' Will to Invest on Steganography and Encryption for Security.

Question eleven sought to find out the willingness of users to invest in the application of the concepts of Steganography and Cryptography on the security of online payment systems processes. Results shown in Table 11 and depicted in Chart 11 suggest the will of users to invest. This implies that if there be more awareness and research on the concepts it has the potential of gaining more acceptability.

Question Twelve: Do you find Steganography as a safe means of protecting privacy and important information in the nearest future? *

Options	Responses	Percentages
No	2	2.20%
Partially	18	19.78%
Yes	71	78.02%
Total	**91**	**100%**

Table 3.12: Respondents' Perception on the Future of Steganography and Encryption.

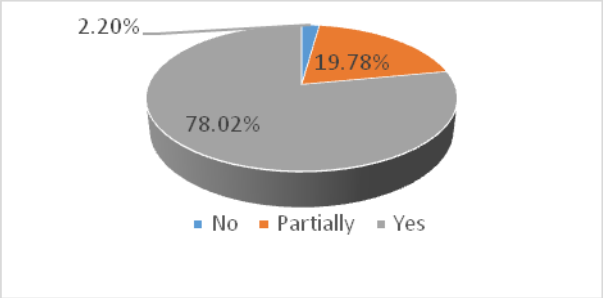


Chart 3.10: Respondents' Perception on the Future of Steganography and Encryption.

Question twelve also sought to find out the possibility of the respondents accepting Steganography as means of protecting privacy in the future. Results in Table 12 and depicted in Chart 12 shows that respondents have many expectations on the more use of Steganography.

ISSN: 2289-7615

Question Thirteen: Given the opportunity would you help to create awareness of Steganography to others? *

Options	Responses	Percentages
No	2	2.20%
Partially	10	10.99%
Yes	79	86.81%
Total	**91**	**100%**

Table 3.13: Respondents' Willingness to Create Awareness on Steganography and Encryption.

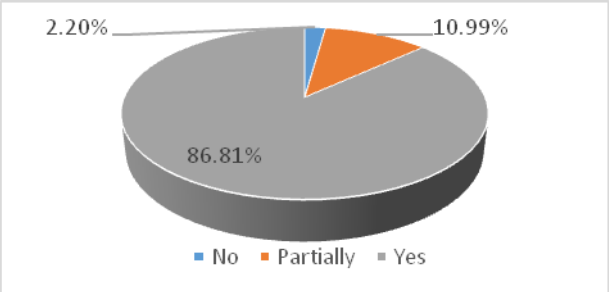


Chart 3.11: Respondents' Willingness to Create Awareness on Steganography and Encryption.

This question sought to find out the willingness of the respondents to create awareness on the concept of steganography and Cryptography as means of providing security to systems especially online payment systems. Results in Table 13 and depicted in Chart 13 suggest higher will. The implication is that should there be mechanisms to create this awareness, it has the potential of being done with less stress and cost.

From the data collected from respondents and analyzed by the researchers, it can be summarized that respondent has a high expectation on the security of online payment systems. Their knowledge and willingness to create awareness and to accept a system based on the use of Steganography and Cryptography as security measures in online payment systems and others suggest that this research is timely and required, and has the potential of turning the game (processes) of online payment systems over.

Design of the Proposed Systems

The design of the proposed systems is the next phase of the analysis of an existing system. Therefore, here, the design of our proposed system is presented.

Our system modifies the preceding framework and is presented in Figure 3.1. The proposed framework does not use emails to ensure real-time processing.

ISSN: 2289-7615

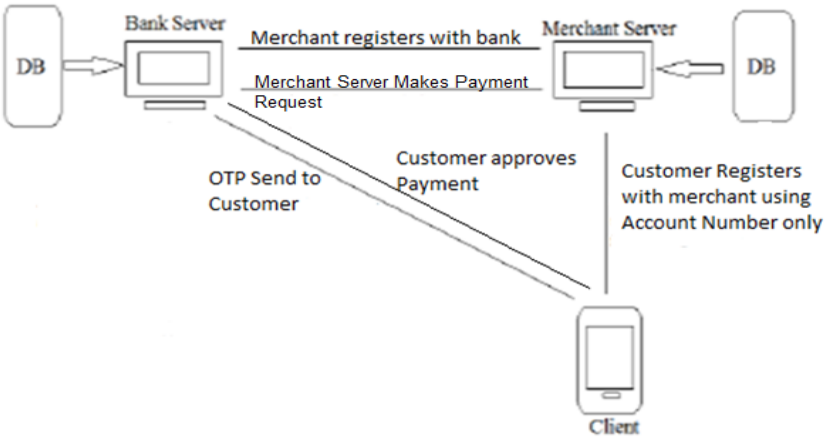


Figure 3.1: Proposed System Framework

Like the proposed framework of More et. al., our proposed framework also requires Customers (clients) to register with the Bank Server using the standard mobile application developed by supplying their Bank Card Details for Verification. The Merchant also would register with the Bank Server for verification purpose to ensure that payment request originates from a legitimate Merchant Server.

From Figure 1, the Merchant Server is any online store and stores products information and displays such for the customers. Customers may choose to register with the Merchant Server to have regular login accounts with the Merchant Server, but should never submit anything other than their Account Numbers. The customer access the Merchant Server for their desired products, add items to their online shopping cart, and checkout.

At the checkout, the customer instead of providing Bank Card details, they just provide their Bank and valid Account Number they wish to use to make the transaction.

The Merchant Server on receipt of the order along with the Customer Account Number, makes a web service call to the Customer Bank requesting payment from such an account.

The Bank Server on receipt of such request, validates the Merchant server making the call, if a registered Merchant Server, the Bank Server generates and OTP, and OTPEK; use the OTPEK to encrypt the OTP. Then generates a captcha image, using a LSB steganography embeds the encrypted OTP into the captcha, divides the OTPEK into two parts of the sequence, embeds one part of the sequence into the captcha image along with the encrypted OTP, the other half is then store in the Bank Server and associated with the transaction. The stego captcha image is then divided into two halves called Share-One and Share-Two. Share-Two is sent to the Merchant Server and Share-One is stored temporarily in the Bank Server until Customer logs on their approved mobile application. The Bank Server sends a notification to the Customer notifying him of such payment request from the Merchant Server.

On successful completion of the task by Bank Server, the Merchant Server is notified, and the Merchant Server can display a prompt to the customer to log on their approved mobile Application to approve payment.

The Customer logs on their approved mobile application by supplying their login details. On successful login, they access the pending transactions and then when they are to make payment, the application makes calls to the Bank Server and Merchant Server for the halves of the stego captcha image, combines the captcha image, retrieved the embedded encrypted OTP and the part of the OTPEK and then depending on the captcha image the Customer inputs the captcha text and another to the bank server is made for the remaining part of the OTPEK and it is combined and the encrypted OTP is decrypted. And

then the decrypted OTP is sent back to the Bank Server for validation and completion of the transaction after the verification of the OTP.

4.0 Implementation and Result Discussion

To achieve the everywhere anytime shopping and payment just like it is the present approach to shopping where customer submit card details to the merchant for payment, a mobile application called OPAS (Online Payment Alternative Solution) was developed. This would allow customers to be directly involved in any payment to be made from the customer's Bank Account and would be done with their approval. That way the customer would be less likely to fall victims of fraud where stolen card details are misused as though the customer is.

OPAS was developed for Android Platform using CIMB bank and Lazada as case study. It allows Customers to approve payment in real time with their mobile phones. Therefore, when Customers make purchases at the Merchant Server and submit their Bank Account Number and the request is made to their Bank, with their mobile phones and OPAS installed, they can process and approve payment.

When Merchant Server makes a make request to the Customer's Bank, the Customer is notified of the request as shown in Figure 4.2. This functionality was implemented using Google Cloud Message (GCM) which allows notifications to be sent to mobile phones.
On starting OPAS or on receipt of payment request notification and user seeks to attend to the notification, OPAS starts and displays the login interface as shown in Figure 4.1, which is a single session login authentication.

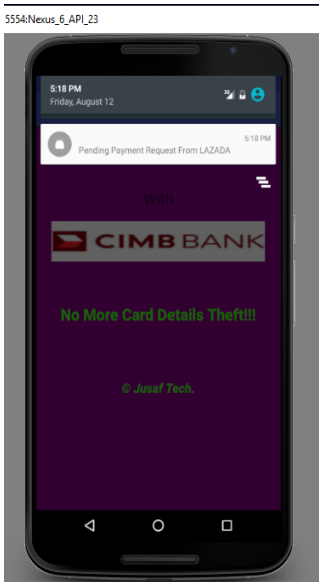


Figure 4.1: Payment Request Notification Received by OPAS.

ISSN: 2289-7615

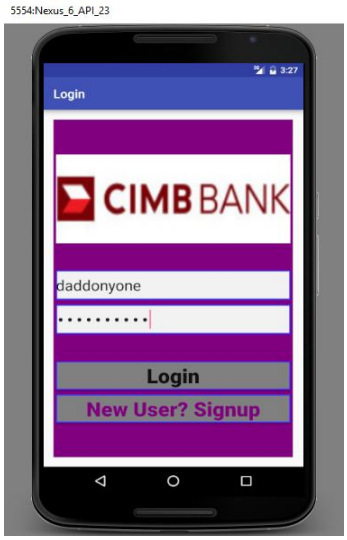


Figure 4.2: OPAS Login Interface.

The Customer login by providing username and password or fresh users may Register New Account. The interface for creating new accounts is as shown in Figure 4.2

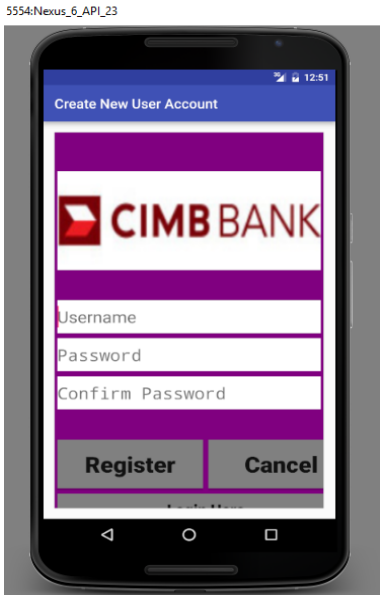


Figure 4.3: OPAS New User Account Creation

From the New User Account Creation, a user chooses a unique username validated at the Bank Server and a password. The user may also from this interface return to Login interface. When successfully logged in, User can then register their Bank Card Details so as to associate the Bank Card to their mobile phone using OPAS and the Bank Server. The essence is to allow Customers to a multiple numbers of cards if they so wish and also to validate that Customer has the rights to perform transactions on the account. The registration is done using the interface shown in Figure 4.4.

ISSN: 2289-7615

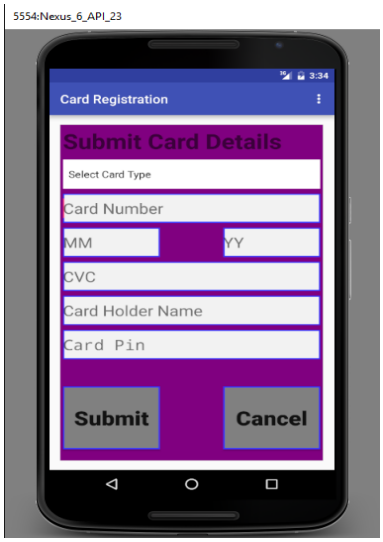


Figure 4.4: OPAS Bank Card Registration.

The user can view and attend to "Pending Transactions" which Merchant Server has requested for payment. The may also view transactions for which they have approved payment for. To attend to pending transactions, the user is to tap/press the menu button and selects "Pending Transactions" and the pending transactions from the different Merchants is then displayed as shown in Figure 4.6. In the same manner, "Paid Transactions" can be accessed and the list is shown in Figure 4.5

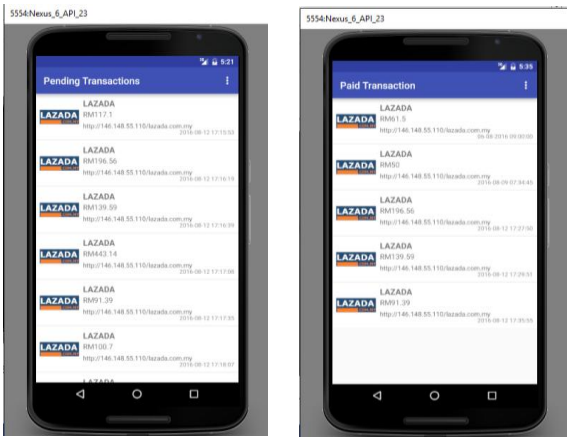


Figure 4.5: List of Paid Transactions.

To approve payment or view details of any pending transaction, the user simply taps on the transaction and the complete details of the transaction is displayed. The details of a transaction are displayed as shown in Figure 4.6.

When the user clicks the "Pay" button to approve payment, a request is made to the server to get the stego image share of the customer associated with the transaction and another request to the merchant server is made to get the merchant share of the stego image. The two shares are merged (combined) together, displayed for the user, and the user inputs the captcha text on the stego captcha images press submit button. A request is then sent to the server and the captcha text is validated and the remaining share of the encryption key is sent by the Bank Server to the Customer's copy of OPAS; then OPAS retrieves the embedded encrypted OTP and the other part of the encryption key decrypt the OTP and again sent back to the Bank Server which again validate the OTP and makes payment to the Merchant Account. This process is as shown in Figure 4.7.

*Figure 4.**Error! No text of specified style in document.**: Transaction Details.*

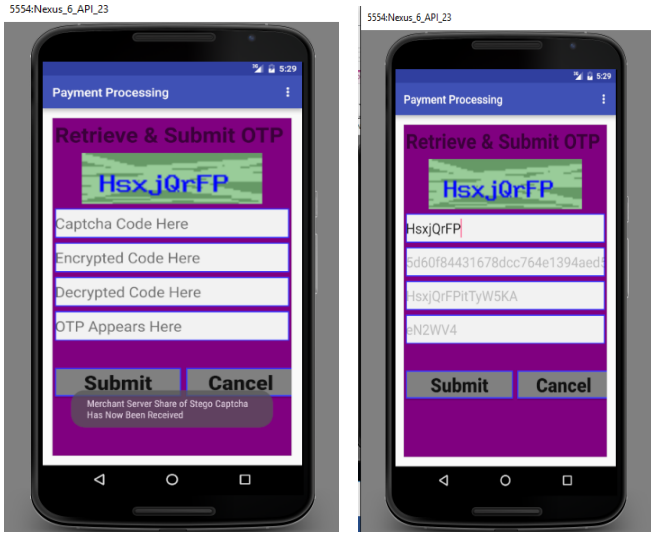


Figure 4.7: OPAS - OTP Processing.

For the purpose of the Customer information, OPAS provide the functionality to allow the user view approved Merchant List which is provided by the Bank Server in real time. This is shown Figure 4.8.

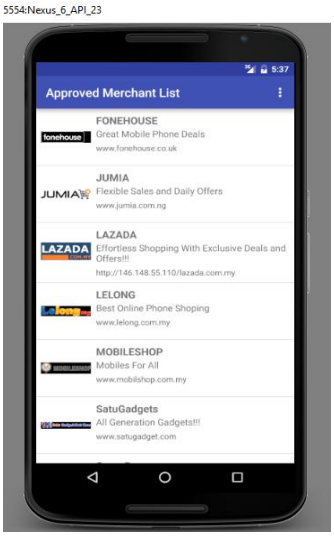


Figure 4.81: OPAS – View of Approved Merchant List.

Having made payment for items, a customer can request for generation of receipt of payment at any given time and have it download to the device being used. The generated receipt is a Portable Document Format (pdf) as shown in Appendix I. To make a request for payment receipt, the user opens paid transactions from the menu and then taps on the particular transaction for which receipt is required and on the transaction details interface, the receipt button is clicked. See Figure 4.9.

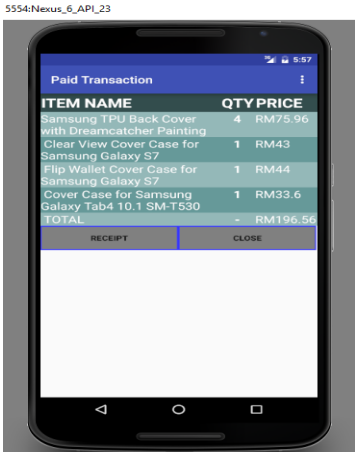


Figure 4.9: Receipts Generation Request with OPAS

Also, during the implementation, we foresaw the scenario of abandoned transactions. Transactions payment is not made for a long period of time. In such cases, a Cron Job task was implemented to check for such transactions and to notify users of such pending transactions before their deletion from the database. For the purpose of testing, we set the time between when a payment request is considered an abandoned transaction to be five (5) minutes and due to deletion after Ten (10) minutes. The notification sent to user after five minutes is as shown in Figure 4.10.

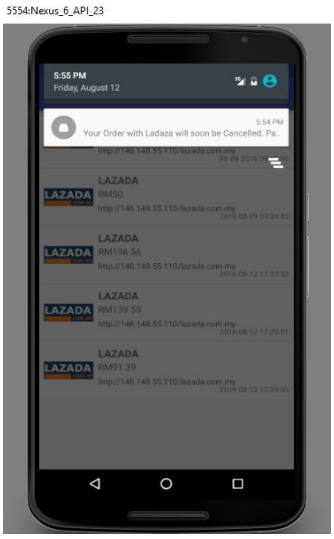


Figure 4.10: Abandoned Transaction Notification.

5.0 Conclusion

In this research, online shopping and payment systems were implemented based on the proposed framework, Blowfish encryption and LSB steganography were used to enhance the security of payment details sent over the internet during payment approval. This approach actively involves customer and thus should give the customer more confidence in the security framework. Also, the implication of the proposed framework is that Bank cards are used just between the customer and the Bank and not the merchant. This implies less chance of falling a victim of phishing.

However, we still see other opportunity to enhance this research as a future work. For example, an advanced encryption and steganography algorithm could be developed and applied to the framework to further enhance the security thereof. Also, the performance of the system should be assessed in terms of heavy load where many users are assessing the system at the system time so that better understanding of how to improve on our implementation approach could be determined.

References

Babangida, Z., Ndang, P. Y. & Bernard, E., 2016. Application of Steganography and Cryptography for Secured Data Communication – A Review. *International Journal of Engineering Research & Technology (IJERT),* 5(4), pp. 186 - 190.

Bank, E. C., 2014. *Third Report on Card Fraud,* Germany: ECB.

Chetan, P., Harsha, R., Sujit, L. & Sonal, R., 2015. Secured Data Transmission for Online Payment System Using Steganography and Visual Cryptography. *International Journal of Computer Science & Communication Networks,Vol 5(5),* pp. 303-307.

Douglas, R., 2010. *Identity Theft Victim Statistics,* USA: Identity Theft and Scam Prevention Services.
Kahn, D., 1996. *The Codebreakers: A Comprehensive History of Secret Communication from Ancient Times to the Internet..* New York: The Macmillan Company.

Kefa, R., 2004. Steganography-The Art of Hiding Data. *Information Technology Journal* , Vol.3(Issue.3), pp. 245-269.

Khonde, S. R., Agarwal, D. & Deshmukh, S., 2014. Online Payment System using BPCS Steganography and Visual Cryptography. *International Journal of Science and Research (IJSR) Volume 3 Issue 11,* pp. 2336 - 2339.

Lopresti, M., 2007. *Bill-2-Phone Lets Customers Add Online Purchases to Their Phone Bill.* [Online] Available at: https://www.allbusiness.com/media-telecommunications/8910400-1.html

More, P., Pooja, T., Leena, W. & Kumar, V., 2015. Online Payment System using Steganography and Visual Cryptography. *International Journal of Latest Technology in Engineering, Volume 4, Issue 10.,* pp. 94 - 96.

Murugeswari, D., Sangeetha, K. N. & Srivani, M., 2015. SECURE E-PAY USING TEXT BASED STEGANOS AND VISUAL CRYPTOGRAPHY. *International Journal of Engineering Research and General Science Volume 3, Issue 1,* pp. 1133 - 1144.

Rao, L., 2010. *Mopay Now Allows You To Bill Mobile Payments To A Landline Accoun.* [Online] Available at: https://techcrunch.com/2010/07/19/mopay-now-allows-you-to-bill-mobile-payments-to-a-land-line-account/

Reddy, V. L. & T., A., 2015. Combine Use of Steganography and Visual Cryptography for Online Payment System. *International Journal of Computer Applications. Vol.124, No.6,* pp. 7 - 11.

Souvik, R. & Venkateswaran, P., 2014. *Online Payment System using Steganography and Visual Cryptography.* s.l., IEEE.