*Applied Computer Science, vol. 16, no. 3, pp. 30–41*
*doi:10.23743/acs-2020-19*

*Submitted: 2020-08-11*
*Revised: 2020-09-04*
*Accepted: 2020-09-07*

*e-Commerce, AES, NDS,*

*Raphael Olufemi AKINYEDE* [0000-0002-5544-8529]*,
*Sulaiman Omolade ADEGBENRO* [0000-0002-3432-0198]**,
*Babatola Moses OMILODI* [0000-0001-6999-7425]***

# A SECURITY MODEL FOR PREVENTING E-COMMERCE RELATED CRIMES

**Abstract**

*The major challenge being faced by the financial related institutions, such as e-Commerce has been insecurity. Therefore, there is urgent need to develop a scheme to protect transmitted financial information or messages from getting to the third party, intruder and/or unauthorized person(s). Such scheme will be based on Advanced Encryption Standard (AES) and Neural Data Security (NDS) Model. Based on this background, an AES using Time-based Dynamic Key Generation coupled with NDS model will be used to develop security model for preventing e-commerce related crimes. While AES will secure users' details in the database server and ensures login authentications, NDS model will fragment or partition sensitive data into High and Low levels of confidentiality. The sensitivity of the data will determine, which category of confidentiality the data will fall into. The fragmented data are saved into two different databases, on two different servers and on the same datacenter. In addition, an exploratory survey was carried out using different performance metrics with different classifications of algorithms. Out of the four algorithms considered, Naive Bayes performs better as it shows, out of a total of 105 instances that were observed, 85.71% were correctly classified while 14.29% were misclassified.*

* The Federal University of Technology, School of Computing, Department of Computer Science, FUTA Rd, Akure, Nigeria, roakinyede@futa.edu.ng
** The Federal University of Technology, School of Computing, Department of Computer Science, FUTA Rd, Akure, Nigeria, adegbenrosulaiman@gmail.com
*** The Federal University of Technology, School of Computing, Department of Computer Science, FUTA Rd, Akure, Nigeria, omiloditola25@yahoo.com

## 1. INTRODUCTION

In recent times, our society is increasingly relying on the Internet and other Information Technology tools to engage in personal, public communication and conduct business activities among other several benefits (Berchane & Berchane, 2018). The cyber space creates boundless opportunities for commercial, business, economic, social and educational activities as well as a haven for societal miscreants to perpetrate their indiscriminate acts. Since the outbreak of coronavirus 2019 (COVID-19), Nigerian government, private sectors and mostly other establishment are increasingly depending on Internet to conduct business, manage industrial activities, and engage in personal communication among other numerous benefits within the reach of the country. While these developments allow for enormous gain in productivity, efficiency and communication that have changed the way in which data is managed, accessed and used commercially, they also create a loophole that criminals may take advantage of to destroy organization's image and reputation.

The Internet is a global network, which means, it contains several networks. Connecting a business to the Internet implies that such business can be reach globally. In other words, a company can reach anyone who has an access to the Internet such as customers, suppliers, on-line banks etc (Taroub, 2015). At the same time, the company can be reached by anyone both near and far. As mentioned above, the Internet creates vast opportunities for businesses, but at the same time poses some threats, which if they are not taken care of properly can lead to data thefts, diversion of funds and destroy businesses (Almunawar, 2012).

In Maitanmi *et al*. (2013) e-crime was defined as a type of crime committed by criminals who make use of computers through the Internet connections to perpetrate evils, such as illegal downloading of music files and films, piracy, spam mailing, data theft and the likes. E-crime evolves from the wrong application or abuse of Internet services. The core activities of e-commerce are business transactions between two parties or possibly mediated by a third party. In fact, the practice conducted by company before the term e-commerce appears is electronic data interchange (EDI), which is basically electronic transaction via computer networks (Yakasai, 2017). The major concern of electronic transactions is how to protect transactions from eavesdroppers (which can steal and modify the information in the transactions) and how to make sure those transactions are authenticated.

## 2. RELATED WORKS

In Hamilton and Gabriel (2012), a management system for dimensions of fraud in Nigeria selected firms was presented. The research was motivated by the need to examine the management of financial fraud in some selected companies in Nigeria. It involves the use of simple percentages and frequency distribution Tables. The purpose of the research is to provide a platform for the management of financial fraud in those companies and also minimize fraud through better internal control systems. The research work contributed a deep knowledge on the effect of fraud on business organizations and fraud reduction strategies. The method adopted is inappropriate and cannot be relied upon in combating cybercrimes because few firms were selected out of numerous companies facing same challenges.

In Jarupunphol & Buathong (2013), a secure electronic transactions (SET): a case of secure system project failures was presented. The research work was motivated by the need to enhance a security protocol for an electronic payment system that uses PKI to address e-commerce security and privacy concerns. It was designed to address security problems in e-payment systems and this involves the use of PKI for the architectural base of SET. Since the main purpose of securing e-commerce is to build a dependable system that addresses security requirements, as a result, this work appeared to be the most appropriate solution for it. The use of PKI for SET makes e-commerce end-users to reject SET because it has several usability issues. For example, e-commerce end-users are forced to comply with SET security requirements and this is unpleasant to them.

In Ogwueleka and Ocheme (2014), an RSA encryption/decryption algorithm for combating cybercrime using a case study of developing countries was presented. The research was to tackle cybercrime as anti-viruses and firewalls have been proved to be inadequate in minimizing the menace of cybercrime in cyber space. It provides a broader and specific approach for tackling cybercrime. It also involves the use of RSA encryption algorithm because hackers find it difficult to factor the large integers and this makes its deployment to be more secured. This research work established the efficiency of RSA encryption method which believed can never be cracked because it is computationally infeasible to permutated but is bound to be ineffective because RSA is vulnerable to Chosen Ciphertext Attack (CCA).

In Chinedu (2015), an e-commerce security using RSA cryptosystem was developed. This research was motivated by lack of adequate security on e-commerce information sent through the computer network and Internet. There is need for a security system that will protect e-commerce information transmitted via the Internet and computer networks. The developed system uses RSA Cryptosystem to secure e-commerce information sent. However, RSA encryption and decryption algorithm needs a lot of calculation and this slows down the speed of the system.

In Chauhan *et al.* (2015), an hybrid technique to secure e-commerce transaction was implemented. The developed system adopt parallel processing and multithreading on AES algorithm and steganography in Image. The system achieved time reduction in encryption and decryption with the use of multithreading and parallel processing. However, the use of steganography can aid illegitimate uses the system, such as in terrorism, pornography and data theft.

Rajeshree and Kirti (2018) developed a secured online transactions using biometrics in mobile phone. The research was motivated by the need to focus on the feature extraction from the runtime fingerprint image on an Android mobile and send to the server for authentication of an individual. The aim is to unravel the main security issues in online transaction with much safe, secure and very easy to use, also need not to remember passwords and secret codes system. The method adopted the use of a generic fingerprint authentication system which comprises of two parts: enrolment and verification. In enrolment, the raw fingerprint image is collected, pre-processed, and the features are extracted and stored. In verification the enrolled fingerprint features are compared with the features computed from the input fingerprint to find similarities between them. The limitation of the research work is based on the model used for fingerprint scanning embedded in a mobile phone that makes e-transactions very cost effective. In addition, the fingerprint scanner does not take into consideration users' finger that might change in either size or form/pattern over time.

## 3. SYSTEM ANALYSIS AND DESIGN

The proposed AES and NDS model for e-Commerce extracted and adapted some of the features of RasmiP and Paul (2011); Hamilton and Gabriel (2012); Akash and Bhonge (2013); Ogwueleka and Ocheme (2014); Kuppuswamy & Al-Khalidi (2014); and Rajeshree and Kirti (2018). From such systems, we can formally describe the security model for e-Commerce as a system that comprises of three modules, which are the customer side, server side and payment channel modules as shown in Figure 1.

The customer software is the front-end via web browser through which users can view, register and interact with the application. The web server (Apache) is the back-end that processes incoming network requests that are coming from customers to the merchant sites. MySQL is the database that works behind the scene to store data and deliver information to the users. The payment channel module includes functions designed to support ordinary types of payment services, the most common being credit/debit cards and mobile payments. Payment gateway such as Paypal, Stripe can be used.

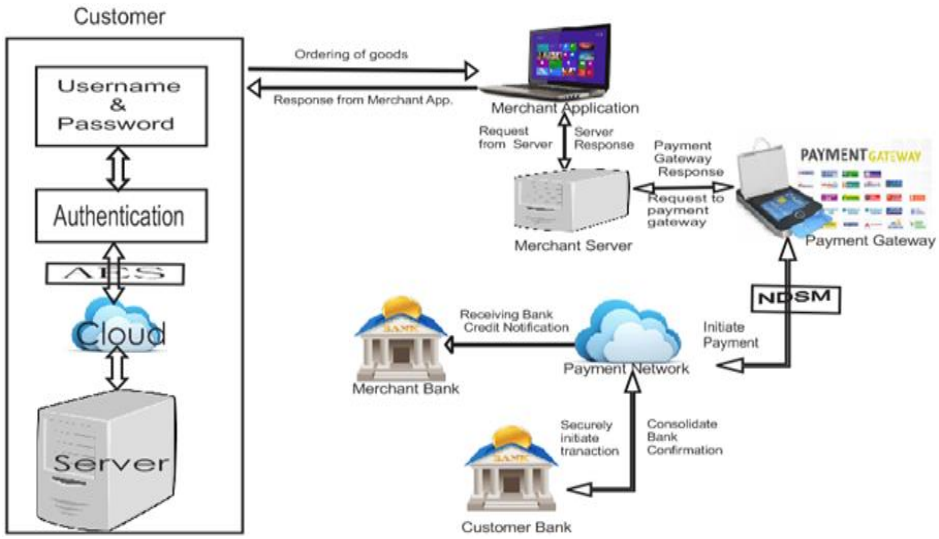


**Fig. 1. Architectural design of the proposed System**

Proposed algorithm execution steps are as follows:

A. Signup by entering details:
   - Securing of users credentials and credit card details using AES,
   - Login,
   - Input Credentials using Username and Password,
   - Authentication using AES.

B. Selection of desired products.

C. Payment with Credit Cards:
   - Securing of credit card details using NDS model.

D. Logout.

### 3.1. E-commerce performance metrics

For this analysis, performance metrics such as Confusion Matrix, Accuracy, and Kappa will be considered using some of the commonly used classification algorithm. The algorithms are Random Forest, J48, Naive Bayes Classifier, and Random Tree.

#### 3.1.1. Confusion Matrix

Confusion Matrix, also referred to as Table of confusion, is made up of two rows and columns that project the number of True Positive (TP), False Positive (FP), False Negative (FN), and True Negative (TN). Table 1 shows the cross section of both Predicted and Actual Values which indicate whether the developed system is good for use or not, especially based on the number of True Positive Values.

**Tab. 1. Confusion Matrix**

| | | Predicted Class: Yes | Predicted Class: No |
|---|---|---|---|
| Actual Class | Yes | TP | FN |
| | No | FP | TN |

I. **Accuracy:** This is the proportion of the total number of predictions that are corrected. The level of accuracy of each algorithm used are in Table 2:

$$Accuracy = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \quad (1)$$

II. **Recall:** This is the proportion of Positive cases that were identified correctly. High Recall indicates the class is correctly recognized (small number of FN). The Recall values for each of the algorithm used is as shown in Table 3:

$$Recall = \frac{\text{TP}}{\text{TP+FN}} \quad (2)$$

III. **F-Measure:** This is the harmonic mean of both precision and recall of the test. Since we have two measures (Precision and Recall) it helps to have a measurement that represents both of them. Values for each of the algorithm used can also be seen on Table 4:

$$F.Measure = 2 * \frac{\text{Precision*Recall}}{\text{Precision+Recall}} \quad (3)$$

IV. **Kappa Statistics**: The difference between the Observed Accuracy and the Expected Accuracy:

$$Kappa = \frac{O_A - E_A}{1 - E_A} \quad (4)$$

The value ranges from 0 to 1, the $Kappa$ value of 0 (zero) represents poor performance while value closer to 1 (one) represents good performance.

## 4. SYSTEM IMPLEMENTATION AND PERFORMANCE ANALYSIS

### 4.1. System Implementation

The layout of the user interface application is designed to be as user friendly as possible. When the user opens the system, e-Commerce Interface and Account Creation Page will appear as shown in Figures 2 and 3.

Click on anywhere on the Screen, then a User Sign-in Page form will appear. This will allow the registration of both the customer and merchant so that they can Login into the system. This is the first step for customer registration. The customer clicks on register new user and supplies his details including the payment information. System would process customer details for registration and send confirmation in form of cipher text. If the registration fails, an error messages would be displayed; and the system would prompt the customer to go through the process again. Then, CA checks that the credit card is valid and releases the signature certificate for customer who stores it for future use. All this information (such as credit card details) must be protected, but in case of merchant, he does not supply any credit card details as his form does not request for it. After that, when an OK button is clicked, a user sign-in page form will appear (Figure 4).

The user will log-in and the system will decrypt the encrypted user name and password from the http request and matches the details of user from database (e.g. validation). If authentication is successful, the system will display a message box with user session that informs the user that he can use the system. Otherwise, the system will display a message box that informs the user to go through the process again. Login authentication method of Akinyede *et al*. (2014) was adapted.

*Login authentication*.

When user $(U)$, which can either be the customer or merchant wants to access the $CA$, he carries out the following steps.

a. $U$ submits the computed $ID$, $yId$ and $Id$ and generates random number $a$, such that $a \in [1, n-1]$.
b. Calculates $Q_i = q_i P$ and then $p_i = h(Q_i)$, $X = q_i K_{pub\_ib}$ and $g = h(ID||Id||p_i||T_i)$.
c. Select random number $a$, calculates $Q_i = q_i P$ and then $p_i = h(Q_i)$, $X = q_i K_{pub\_ib}$ and $= h(ID||Id||p_i||T_i)$.
d. $U$ computes the hashed password $Y = yId$, dynamic identity $dID = p_i H(ID_i)$ encrypted and sends message to $CA$ server.
e. Decrypt $p_i H(ID_i)$.
f. Verify both certificate & signature.


**Fig. 2. E-commerce Interface**

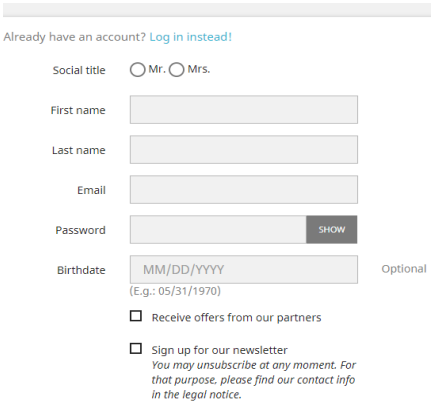


**Fig. 3. Account Creation Page**

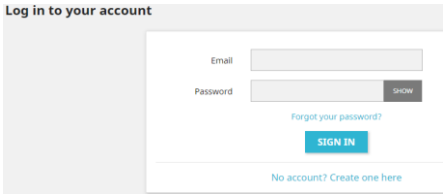


**Fig. 4. User Sign-in Page**


**Fig. 5. List of Products**

The system comprises of the merchant and customer interface. The merchant uses his interface to upload and display available items for shopping, while the customer chooses the desired merchant, the items that are available in his store at the customer's interface. Then, the customer can select the needed items from the list of products (Figure 5) and add them to the cart as shown in Figure 6. Having completed the ordering process, customers can checkout as shown in Figure 7. Shipping and payment can follows as shown in Figures 8 and 9: Here is the payment protocol.

*Verify PIN*

IF PIN is correct THEN

$$\{mp \;\; \text{A:} \left[[\text{PI}, \text{signed}], \text{C}\; ID\right]\}$$

ELSE $terminate$

$$\text{C} \rightarrow \text{M:}\; \{\{Ordered\ Items, Tr.ID, M_{ID}\}K^{-1}\}K^{secret}$$

$$\text{M} \rightarrow \text{C:}\; \{Item, M_{ID}, Tr.ID\ , ID_{\text{CA}}\}K^{secret}$$

$$\text{C} \rightarrow \text{M:}\; \{\{PaymentOrder, Tr.ID, M_{ID}\}K^{-1}\}K^{secret}$$

*Merchant* processes the order and starts the payment phase by forwarding the payment instructions to *payment Transaction Host*. Note that the *Transaction Host* will obtain transaction data via the network and processes the payment

transaction on behalf of a financial institution that holds the account of the customer for the payment method selected. This will be possible in the payment gateway (Figure 10).


**Fig. 6. Shopping Cart**

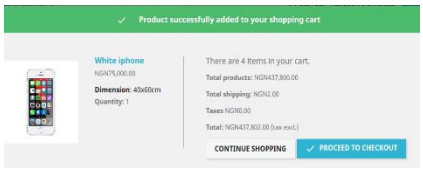


**Fig. 7. Checkout**

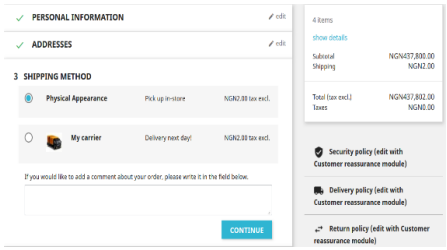


**Fig. 8. Shipping Method**

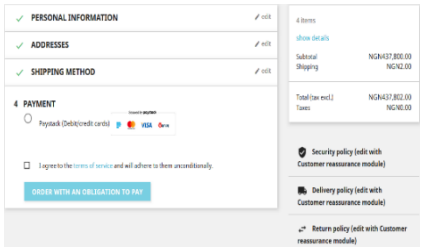


**Fig. 9. Payment Method**

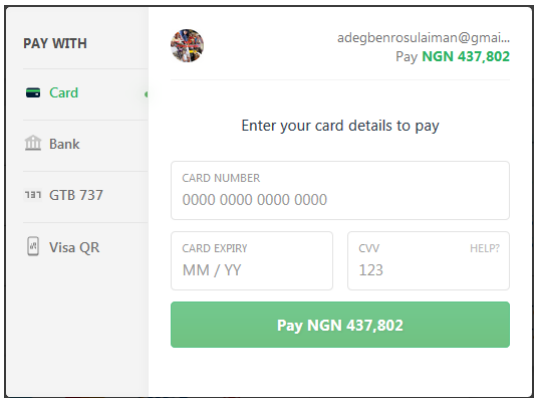


**Fig. 10. Payment Gateway**

## 4.2. Performance analysis using 10-fold cross validation technique

In order to investigate the performance of the classifiers, a 10-Fold cross validation was used to evaluate the classifiers. A 10-Fold cross validation is a technique to predictive models by partitioning the original sample into a training set to train the model, and a test set to evaluate it. Table 2 shows the performance analysis based on accuracy while Table 3 shows the results of both correct and incorrect classified data using different algorithms.

**Tab. 2. Performance Result Based on Accuracy**

| Algorithm | TP Rate | FP Rate | Precision | Recall | F-Measure | RoC |
|---|---|---|---|---|---|---|
| **Random Forest** | 0.838 | 0.244 | 0.853 | 0.838 | 0.830 | 0.909 |
| **J48** | 0.829 | 0.250 | 0.839 | 0.829 | 0.821 | 0.751 |
| **NaiveBayes** | 0.857 | 0.184 | 0.857 | 0.857 | 0.855 | 0.903 |
| **Random Tree** | 0.676 | 0.488 | 0.687 | 0.677 | 0.625 | 0.650 |

**Tab. 3. Performance Result**

| | Random Forest | J48 | NaiveBayes | Random Tree |
|---|---|---|---|---|
| **Kappa** | 0.22 | 0.61 | 0.69 | 0.63 |
| **Correctly Classified (%)** | 67.62 | 82.86 | 85.71 | 83.81 |
| **Incorrectly Classified (%)** | 32.38 | 17.14 | 14.29 | 16.19 |
| **MAE** | 0.41 | 0.25 | 0.14 | 0.39 |
| **RAE(%)** | 5.75 | 77.96 | 69.87 | 82.41 |

**Tab. 4. Confusion Matrix**

| | Random Forest | | J48 | | NaiveBayes | | Random Tree | |
|---|---|---|---|---|---|---|---|---|
| **Class** | **A** | **B** | **A** | **B** | **A** | **B** | **A** | **B** |
| **CLASS A** | 62 | 2 | 62 | 3 | 60 | 5 | 61 | 4 |
| **CLASS B** | 15 | 25 | 15 | 25 | 10 | 30 | 30 | 10 |

Tables 2 to 4 gives all the details of the individual algorithm used. It shows the Accuracy Performance of each algorithm. Out of the four (4) algorithms, Naive Bayes seems to perform better but with little margin as against other algorithms. Explaining Naive Bayes performance result from Table 3, a total of 105 instances were observed out of which 85.71% were correctly classified while 14.29% were misclassified.

With Kappa value of 0.690 shows good performance classification of fraudulent and non-fraudulent cases of transaction.

Table 2 shows the TP, FP, Precision, Recall, F-Measure and RoC of the four algorithms used. The ranges from 0.676 to 0.857 signifies good performance index for the classifier.

As shown in Figure 11, it can be concluded that using AES and NDS Model improves the prevention of e-Commerce related crimes.

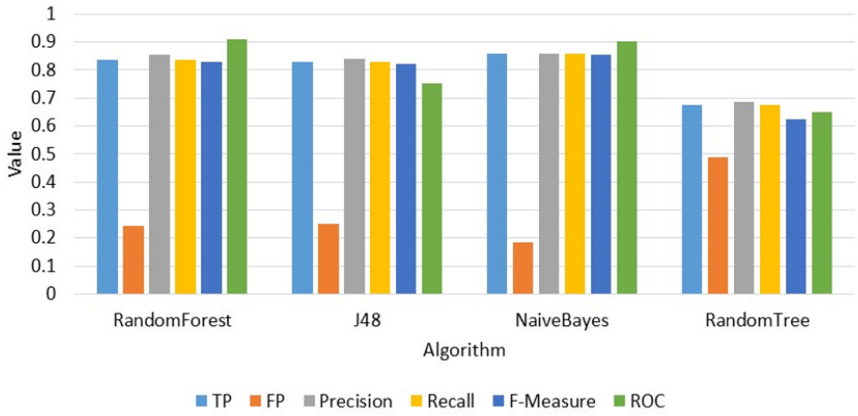


**Fig. 11. Performance Result Based on Accuracy**

## 5. CONCLUSIONS AND RECOMMENDATION

Despite the numbers of a security model for preventing e-commerce related crimes that have been proposed in the past, not many of them are practicable or implementable. As a result, in this work, an exploratory survey was carried out using different performance metrics with different classifications of algorithms. All the Tables show the Accuracy Performance of each algorithm. Out of the four algorithms, Naive Bayes seems to perform better but with little margin as against other algorithms. The scheme adopted the use of AES Dynamic key Generation for user authentication during login process and NDS model for fragmentation of customer's credit card detail into two different servers on the same data center. This paper also explained the user authentication and secured customers card details. User authentication provides the assurance that customer's details are secured and privacy is maintained. Merchant website provides vast security, thereby assuring the customers that the transaction is carried out without iota of doubt or fear of insecurity and also integrity, privacy and confidentiality is maintained.

## REFERENCES


Akash, V. M., & Bhonge, S. P. (2013). Secure Information Transmission Based on Cryptography Fused with Steganography by using Metamorphic Video Encryption. *International Journal of Science and Research (IJSR)*, *4*(4), 16041503.

Akinyede, R. O., Alese, B. K, & Adewale, O. S. (2014). Building a Secure Environment for Client-Side Ecommerce Payment System Using Encryption System. *Proceedings of the World Congress on Engineering* (vol. 1). London.

Almunawar, M. N. (2012). *Securing electronic transactions to support e-commerce*. Arxiv.org. www.arxiv.org/ftp/arxiv/papers/1207/1207.4292.pdf

Berchane, N., & Berchane, N. (2018, March 21). Impacts of information technology (IT). Master Intelligence Economique et Stratégies Compétitives. https://master-iesc-angers.com/impacts-of-information-technology-it/

Chauhan, E. S., Datta, U., & Pratap, M. (2015). A Hybrid Technique to Secure E commerce Transaction with the Help of AES Encryption and Stenography in Image. *International Journal of Hybrid Information Technology*, *8*, 271–278.

Chinedu, J. N. (2015). Design and Development of an E-Commerce Security. *International Journal of Innovative Research in Information Security (IJIRIS)*, *6*(2), 5–17.

Hamilton, D. I., & Gabriel, J. M. (2012). Dimensions of fraud in Nigeria quoted firms. *American Journal of Social and Management Sciences*, *3*(3), 112–120. http://doi.org/10.5251/ajsms.2012.3.3.112.120

Jarupunphol, P., & Buathong, W. (2013). Secure Electronic Transactions (SET): A Case of Secure System Project Failures. *International Journal of Engineering and Technology*, *5*(2), 278–282. http://doi.org/10.7763/IJET.2013.V5.558

Kuppuswamy, P., & Al-Khalidi, S. Q. (2014). Securing E-Commerce Business Using Hybrid Combination Based on New Symmetric Key and RSA Algorithm. *MIS Rev. Int. J.*, *20*(1), 59–71.

Maitanmi, O., Ogunlere, S., & Ayinde, S. (2013). Impact of Cyber Crimes on Nigerian Economy. *The International Journal of Engineering and Science*, 2(4), 45–51.

Ogwueleka, F., & Ocheme, I. (2014). Review of RSA Algorithm Encryption for Combating Cybercrime: A Case Study of Developing Country. *International Journal of Emerging Technology and Advanced Engineering*, *4*(9), 538–548.

Rajeshree, S. T., & Kirti, K., (2018). Securing Online Transactions Using Biometrics in Mobile Phone. *International Research Journal of Engineering and Technology (IRJET)*, *5*(6), 848–851.

RasmiP, S., & Paul, V. (2011). A Hybrid Crypto System based on a new Circle- Symmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Applications. *IJCA Proceedings on International Conference on VLSI, Communications and Instrumentation (ICVCI)*, *9*, 14–18.

Taroub, A. M. S. (2015). Privacy and Protection in Electronic Transaction: A Review of the e-Commerce Security Protocols. *The 7th International Conference on Information Technology* (pp. 421–429). http://doi.org/10.15849/icit.2015.0079

Yakasai, A. M. (2017). The Relevance of E-Commerce in Nigeria. In *Northwest Business and Entrepreneurship Development Review* (pp. 103–135). Faculty of Social and Management Sciences.