Nigerian Journal of Technology (NIJOTECH)
Vol. 42, No. 1, March, 2023, pp.152 - 159
www.nijotech.com

Print ISSN: 0331-8443
Electronic ISSN: 2467-8821
https://doi.org/10.4314/njt.v42i1.19

A TRUST, PRIVACY AND SECURITY MODEL FOR E-COMMERCE IN NIGERIA

O. Akinola[*,1] and O. Asaolu[1]

[1]Department of Cybersecurity, School of Computing, Federal University of Technology. Akure

*corresponding author (Email: hisgracetoyin@gmail.com)

Article history: Received 23 May, 2022. Revised 19 July, 2022. Accepted 19 July, 2022

Abstract
Today, digital technologies has permeated every sector of human life from communication to medicine to education to transportation and most recently shopping.. The mode of buying and selling by Nigerians have moved from traditional to digital, whereby consumers buy and sell goods online. The online presence of commerce is known as Electronic commerce or E-commerce and it is an initiative amongst other emerging digital sectors in Nigeria that has witnessed substantive growth recently. However, the issues of security, privacy of data and the trust endeared by users on the initiative remains a challenging one. Presently in Nigeria, the solutions to combat security concerns of E-commerce are technically inclined and therefore do not sufficiently capture the solution paradigm. Due to a rise in these E-commerce's security-related concerns in Nigeria as discovered by taking random samples of the population used for the survey, this research proposes a Security, Trust and Privacy model for the survival of E-commerce in Nigeria.

Keywords: E-Commerce, Security, Privacy, Access Control, Perspective, Requirements.

1.0 INTRODUCTION

The Internet amongst its numerous potential offers a facility for buying and selling of goods and services virtually known as Electronic Commerce (E-commerce). In Nigeria, E-commerce has revamped the mode of exchange of goods and services from physical to virtual through a distributed computing method. Although the evolution of E-commerce has gained a rapid acceptance in Nigeria, Security and privacy of data remains unpredictable due to various factors. Through E-commerce, consumers are able to shop online at any point in time in Nigeria thereby transmitting volumes of data across the internet. Data such as credit card information, personal profiles, employment details and most recently health fitness status are requested from users when buying or selling goods online. Moreover, the Internet is the global network of non-executive directors and it has a lot of security risks [1].

Presently in Nigeria,,Security and privacy of E-commerce transactions is a vital area of research in Nigeria and it has become a high-profile concern due to the increasing number of merchants trying to spur commerce online and more importantly the advent of unforeseen events such as the recent epidemic outbreak. The most recent Covid 19 outbreak is one example of out of many that increased the dependence of consumers on E-commerce thereby giving room for a closer look at how to ensure the trust and Privacy of data of users on E-commerce platforms. There is also an undeniable rate of explosion in E-commerce related cyber incidents reported yearly thereby leading to fear and trust issues expressed by E-commerce players.

The focus of the research is to establish and estimate the security elements needed to provide privacy and trust on Electronic commerce. According to [2], the security and privacy policies put in place by owners of E-commerce platforms are often inadequate. Quite a number of people understand security as a means of protecting information assets, meanwhile, a system can have technological infrastructure to prevent data breaches whereas other elements such as man could provide a weaker link for incidents that could compromise security of E-commerce within its ecosystem. Security is described as a state of an entity or a system being free from acts, incidents or

influences that are inimical to the existence of the entity or its being in preferred prescribed state.

On the other hand, Privacy is a major issue in E-commerce because users are concerned about how to protect their personal data when buying or selling goods online. Thus, Privacy is described as having control over one's personal data. All the E-commerce players in Nigeria ranging from consumers to the service providers and the Government want to have some level of control over their data that is being transmitted on E-commerce sites. With a rise in cases of identity theft, phishing and social engineering, it has become more difficult for users to provide data on E-commerce sites without an assurance of privacy on such data.

Therefore, it is expedient to augment the existing Security technologies with a trust model that E-commerce stakeholders can leverage on and can be rest assured that their information is private. The use of hierarchical structure of layered technologies comprising of Access-based control and the prevalent digital signatures in E-commerce can be used to address privacy concerns on the part of the consumers. Not only that, the socio-technical aspect of addressing privacy and security concerns in E-commerce should be given attention through an awareness of the elements of E-commerce Security from the initial phase of making an order to the last stage of making payment online. The customer must be aware of the security elements required to transact businesses online. This in addition to hierarchical models of technology on E-commerce systems would succinctly address the issue of privacy of user's data.

1.1 E-Commerce and Security

A critical success factor of E-commerce as identified by researchers and stakeholders is how security measures can be established to foil the challenges of breaches and compromises on the privacy of user's data. As expressed by [3], the security of the transaction is the core and key issue in the development of E-commerce. E-commerce security provides the security of assets of E-commerce from illegal access, use, modification, or damage [4]. All the models of E-commerce from Business to Consumer, Consumer to Consumer , Government to consumer, Business to Business and M-commerce allows transaction of data between them. This data is vulnerable to attack vectors which extinct data breaches on information systems.

[5] argued that in as much that there is nothing called absolute security , system security in general and E-commerce security in particular is conceived of as a process rather than a one-time developed product. It is therefore important to understand the requirements of E-commerce security from both the consumer and the service provider's perspectives.

1.2 Security Features of E-Commerce

Today, the mode of commerce has moved from the traditional system to an Electronic one. Nevertheless, the pervasion of the E-commerce intiative into the Nigerian economy has brought some concerns just like the every other technological implementation. According to this survey, The most serious concern of users of online commerce in Nigeria is security. For E-commerce to thrive well or survive in Nigeria, the security issue must be tackled. The requirements of the security triad must be core to the implementation of E-commerce as well as other important security elements within the Nigeria"s commerce space.

The security features of an entity such as E-commerce defines the units of measuring elements that are necessary to transact business online in a secured manner. These features are paramount as almost every business have a form of online sales or the other. The websites used by these businesses must possess some elements of security such as the authentication of users, the authorization given to users , integrity of information given by such websites, Non-repudiation, confidentiality, privacy, Availability, usability, Information classification and Auditability.

[4] proposed this framework of security elements with six of such security elements while this research identifies ten of such elements. The ten security elements identified in this work are confidentiality, Integrity, availability, authentication, authorization, usability, non-repudiation, auditability, information classication and privacy.

i. **Integrity:** Integrity is about maintaining the value and the state of information in a system in a way that the information, is protected from unauthorized modification or alteration. The principle of integrity ensures that any information that customers shares online remains unalteredbecause Information only has value when we know that it is correct. A major objective of information security policies is thus to ensure that information is not modified or destroyed or subverted in any way.
ii. **Confidentiality:** Confidentiality is the protection or the keeping valuable information

only in the hands of those people who are intended to see it.
Confidentiality ensures that the data content cannot be understood by unauthorized entities.

iii. **Privacy:** Privacy is a confirmation that information is shared only between authorized organization and persons. A user must have control and non-disclosure right to transactional data on E-commerce sites .

iv. **Authorization**: Authorization is about ensuring that only the people who are authorized to have access to information are able to do so. This entails assigning administrative roles, privileges to access information resources physically or virtually. Users of E-commerce can be assigned roles using Role-based access control once their identity is approved by the server. This will restrict unauthorized access by hackers who intend to steal user's information on Electronic commerce websites.

v. **Authentication:** Authentication is a means of checking the identity of users on E-commerce platform. The buyer and seller should be who they say they are by prooving their identity. The most common means of authentication include password, OTPs, Biometric techniques and third party verification.

vi. **Availability**: Availability means ensuring that information is available and operational when they are needed. A major objective of security policies of E-commerce systems must be to ensure that information is always available to support critical business processing.

vii. **Non repudiation:** refers to an individual's intention to fulfill their obligations to a contract. E-commerce uses technology such as digital signatures and encryption to establish non-repudiation. (Revarthi,2015) described Non-repudiation as " prevention against one party from reneging on an agreement"

viii. **Usability**: An Information system such as an E-commerce system can only be considered secured when it is usable. A commerce website must be secured enough to allow users to use it at any point in time.

ix. **Information classification**: E-commerce websites must contain information that is classified into categories ranging from where to make an order to product categories to where to make payment. This will help in securing the platform as users are able to authorize to do one form of transaction per instant of time. That is, a buyer cannot make payment unless an order or purchase has been made.

x. **Auditability:** Information systems are evolving to become auditable. The history of events of any information system must be traceable. This feature of security will help E-Commerce platforms to maintain a log of events on their websites at all times. An audit log or trail can be of great value when there is an incident on security breach where the root cause of such failure can be trailed.

1.3 Objectives of the Study

The objectives of this research are:

a. To identify the security and privacy requirements of Electronic commerce(E-commerce) in Nigeria
b. To identify what these security and privacy requirements are, and how they are being addressed by consumers, organizations, Government and other stakeholders in E-commerce sector.
c. To design a model based on the security and privacy requirements identified in b above.

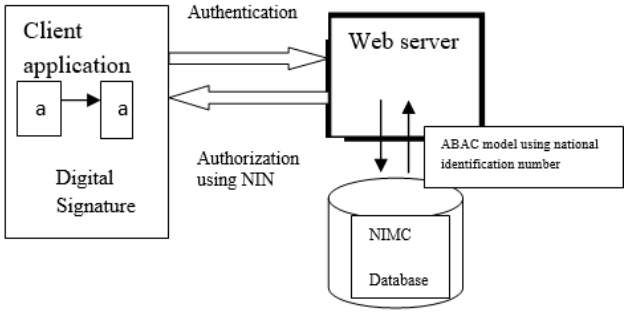

Figure 1: An Architecture of the privacy model using digital signature and Attribute-based access control.

1.4 Privacy Concerns

The issue of privacy in E-commerce is undetermined due to the fact that there is no common understanding between the E-commerce service providers, the Government and consumers or users on what information should be private and how to achieve privacy on E-commerce website. Privacy is a means of preventing any activity that will lead to the sharing of customer's data with unauthorized parties.

[6] explained that in order to reduce these privacy concerns and attract online customers, E-commerce organizations should address some factors that would affect customers 'trust such as privacy and security concerns. To address these concerns, we propose a

solution from a technical perspective by using a digital signature encryption for sending Information by a user on E-commerce platform meanwhile the platform would authorize the user based on a particular user attribute and the environment.

Attribute-based access control draws a set of attributes based on user's profile, environment or resources before it authorizes a user to execute a task. In this work, a user-based attribute using National Identification Number (NIN) of E-commerce users in Nigeria and their environment where they will be combined together to grant them access to information and operations on E-commerce platforms. From the social–technical perspective, a cyber-awareness notice containing the ethics of security on E-commerce platforms should be enforced by government on users and E-commerce service providers.

1.5 Related Work

In this section, the literature of related work on E-commerce security, trust and privacy is being discussed. [7] discussed the usability and security issues in the implementation of E-commerce website, according to him, the essential dimensions of e-commerce security are integrity, Non-repudiation, Authenticity, Confidentiality, Privacy and Availability. The work focused on both the technical and non-technical solutions in order to have a secured E-commerce.

Moreover, internet businesses like Electronic commerce (E-commerce) have brought large security issues as reported by International Journal of Security and its Applications. A systematic review of attacks that could occur on E-commerce systems was done by [8] with certain recommendations made on the proposed solutions. Availability, Authentication, Confidentiality, Integrity and Non-repudiation were higlighted as the dimensions of security that must be considered for a secured E-commerce. With the development of E- commerce, these security issues have obtained more and more attention [9].

Phishing, social engineering, hacking are all used by hackers and malicious users to gain access to E-commerce user's data. Therefore, the users of E-commerce sites are constantly exposed to privacy and security risks. [10] explained that if these privacy and security threats are not eliminated, users will never trust, visit or shop at an E-commerce site. According to [10], factors affecting E-commerce security are role of computer auditing, data protection and security, authenticity, data accuracy and data disclosure. These factors are considered only from a user's perspective and not from the other stakeholders point of view.

The requirement of E-commerce stretches beyond how to prevent data loss but on other salient factors. E-commerce security has its own particular nuances and it is one of the highest visible security components that affect the end user through their daily payment interaction with business sites as well as organizations. In his work, [11] used behavioral intention analysis to propose a preliminary model (privacy-security risk- trust model), that would consider customer's privacy concerns, security concerns, and how they can affect his/her perceived risk. The model captured confidentiality, integrity and availability as the elements of security. [12] in his research concluded that Citizen's income and Data Security are major factors impeding the growth of E-commerce in Nigeria. [13] did an analysis of E-Commerce Security System in Nigeria and he identified four elements governing the security framework of E-commerce in Nigeria. These elements are firewalls-programming and physical component, Open key infrastructure Encryption programming, Advanced endorsement, all derived from technological solutions.

The way the consumers use information on E-commerce websites can also pose a security threat to such systems. According to [2], Being aware that there are privacy and security risks associated with the internet naturally moderates a user's behavior while online. Also, it could be helpful to have, at least a form of basic knowledge of necessary security requirements that a web retailer is expected to put in place before customers transact business on their E-commerce platform. Consequently, Rajesh Kumar described e-commerce security as the fortification of web-based business resources from illegal access, use, modification or anihiliation.

[14] also stated that using the Internet as the underlying backbone network that does not support security sufficiently in E-commerce has led to security risks and concerns. Therefore, a wholistic solution to E-commerce security challenges must be beyond the technology that drives it but a means of getting consumer's aware about the associated risks and threats related to transacting business onlines. According to [15], without all these proper security methods in place, it is just like building a house without locks, any person can gain access.

Thus, there is a wider scope of human dependence on E-platforms especially E-commerce. As expressed by [16], E-commerce security elements needed to ensure security of data being transmitted in a network are the integrity of the information, the validity of the information, the authenticity of the transaction status and the reliability of the system. [17] in their research about the security issues of Ecommerce, they put forward solution strategies from two perspectives namely the technology and the system, similarly, [18] expressed the four areas of concerns.on E-commerce security as Privacy concerns, System security concerns, cyber crime concerns and transactional security concerns.

As stated by [19] in his work, Data privacy issue is a growing concern among businesses and organizations, he then identified the basic requirements for privacy-aware access control on E-commerce application. [20] elucidated Authentication, integrity, confidentiality and Non-repudiation as the only elements of security in E-commerce. The work explained how common criteria roadblock is being used to design a security framework for E-commerce systems. However, the model addressed the security issues in E-commerce from a technical perspective only.

2.0 METHODOLOGY

The study area of this research work includes some states in Nigeria where there is a large base of customers who buy and sell online. The first survey was conducted amongst users and non-users of E-commerce in Nigeria, while the other one was conducted among some selected organizations in Nigeria . A survey method using online and paper questionnaires was adopted and a total of 284 responses were obtained from both ends.

A summary of statistical estimation procedures were used to obtain the parameters of E-commerce security on data collected within a population sample from Nigeria. These include chi-square formula, independent T-test, Pearson Correlation:

For the purpose of this research work, we assume 5% as alpha level of significance, X= 5% level of significance, Pearson Correlation test where Alpha level of confidence is $-1 \leq r \leq 1$

Table 1: Demography of the participants

Variable	State	Frequency	Percentage (%)
Sex	Male	191	67.3
	Female	93	32.7
	Total	284	100.0
Age	18-35	145	51.1
	36-50	116	40.8
	51-60	22	7.7
	> 60	1	1.0
	Total	284	100.0
Employment	Employed	216	76.1
	Unemployed	68	23.9
	Total	284	100.0
Marital Status	Single	93	32.7
	Married	183	64.4
	Divorced	6	2.1
	Widowed	2	0.7
	Total	284	100.0

2.1 Research Hypothesis

H1.0. Does security concerns expressed by consumers affect their attitude towards E-commerce?
H1.1. Security concerns expressed by consumers does not affect their attitude towards E-commerce
H1.2. Security concerns expressed by consumers affects their attitude towards E-commerce
H2.0. Is the consumer's level of knowledge on security not positively related to E-commerce adoption?
H2.1. Consumer's level of knowledge on security is not positively related to E-commerce adoption.
H2.2: Consumer's level of knowledge on security is positively related to E-commerce adoption?.

3.0 DATA ANALYSIS

In this study, a total of 300 paper questionnaires were administered out of which 223 were completed and returned. The research was also done through a web survey URL where 57 entries were recorded on the database.

Both paper and online survey respondents are 284 in number and this formed the basis of data analysis for this research work.

Table 2: Customer Ranking of Security Features

S/N	Security Features	Very important	Important	Less important	Not important	Invalid	Total
1	Confidentiality	83.1	13.4	1.1	0	2.5	100
2	Integrity	77.7	19.4	0.7	0	1.1	100
3	Availability	60.6	35.6	2.8	0	1.1	100
4	Privacy	60.2	28.2	9.2	0.7	1.1	100
5	Non-Repudiation	49.3	25.4	18.0	2.5	2.5	100
6	Authentication	60.6	27.8	7.7	0.7	1.8	100
7	Authorization	59.9	30.3	6.7	1.4	0.4	100
8	Usability	44.0	39.9	12.4	2.1	0	100
9	Information Classification	52.1	37.7	4.2	2.1	2.5	100
10	Auditability	46.5	34.2	10.2	2.1	4.6	100

In addition, we used Statistical Package for the Social Sciences (SPSS) software for data analysis and Chi square was used to test our Hypotheses with α level of confidence taken as 0.05. From the data obtained from the questionnaire, a frequency distribution of the factors that are considered by consumers to engage in E-commerce such as security (48.2), Fast Delivery (28.5), reputation of merchants (11.3) , Web interface (25) and use of Authentication seal on websites(4). Amongst these factors, security ranked the highest with a cumulative percentile of 48.2%. This establishes the need for a secured E-commerce within the Nigerian context.

From the survey, it can be deduced that the security requirements needed to have a an enabling E-commerce environment in Nigeria are Confidentiality, Integrity, Availability, privacy, Non-repudiation, Authentication, Authorization, Usability, Information classification and Auditability. The results shown in the table reveals that none of these features was null for the "very important" category, thus we can infer that the elements required to enhance the security of E-commerce in Nigeria is beyond the usual elements of information security, that is the C-confidentiality, I-integrity, A-Availability triad.

3.1 Hypotheses Testing

For testing the Research hypotheses, mean values, independent T-test, chi square analysis, and correlations among other research dimensions were considered using Pearson's correlation coefficient . We used all responses from 284 participants in calculating these measures. We cross tabulated each variable in terms of factors considered by consumers to participate in E-commerce with the concern for a secured E-commerce, A chi- square analysis was done using Alpha level of confidence taken as 0.05 .

If any of them was correlated, then one of the first two hypotheses is supported. Similarly, we correlate each variable in security, namely; confidentiality, integrity, and availability, with the level of importance to security in E-commerce. Risk variable (i.e. Security Variable/level of importance)

The first hypothesis (H1.0) states that does the security concerns expressed by consumers not affect their attitude towards E-commerce?

The Chi square coefficient is 0.02 with the Alpha level of confidence taken as 0.05, Therefore, we reject the null Hypotheses H0 and accept the alternate Hypothesis H1: Security concerns expressed by consumers affects their attitude towards E-commerce

hypothesis (H1.0) states that Security concerns expressed by consumers does not affect their attitude towards E-commerce.

Table 3: Factors to consider for online purchase*participants are concerned about security of E-commerce

	Value	Df	Asymp. Sig
Pearson Chi-Square	17.175	4	0.02
N of Valid cases	275		

Hypothesis (H1.1) Security concerns expressed by consumers affects their attitude towards E-commerce.

With level of significance obtained as 0.02 less than Alpha level of confidence, we reject H1.0 and accept H1.1.

Table 4: Security strategy* Use of Internet for business transactions

	Value	Df	Asymp. Sig
Pearson Chi-Square	16.175	5	0.006
N of Valid cases	275		

For Hypothesis two, we correlate the knowledge of security awareness on E-commerce expressed by consumers to how they use the Internet for business transactions?

Hypothesis (H2.0) states that: Is the Consumer's level of knowledge on security awareness NOT positively related to E-commerce adoption?

Hypothesis (H2.1**)** states that : Is the Consumer's level of knowledge on security awareness positively related to E-commerce adoption?

Alpha level of confidence taken as 0.05, the result of the chi square 0.006 is lower, hence we reject H2.0 and accept H2.1. Level of Knowledge of consumers on security of E-commerce is positively related to its adoption.

The results show that a support for this hypothesis exists

3.2 The Proposed Model

E-commerce services have grown sporadically in recent years. In light of this, quite a number of

security challenges have also emerged. These security issues have plunged experts into the spiral of technological solutions and defense mechanisms being developed. Nonetheless, there seems to be lack of a single approach that can succinctly tackle problems in the area of security in E-commerce.

In this work, we adopt the use of privacy-trust behavioral intention model [21] and finite state automata as the basis of formulating our model for providing solution to the security state of E-commerce in Nigeria.

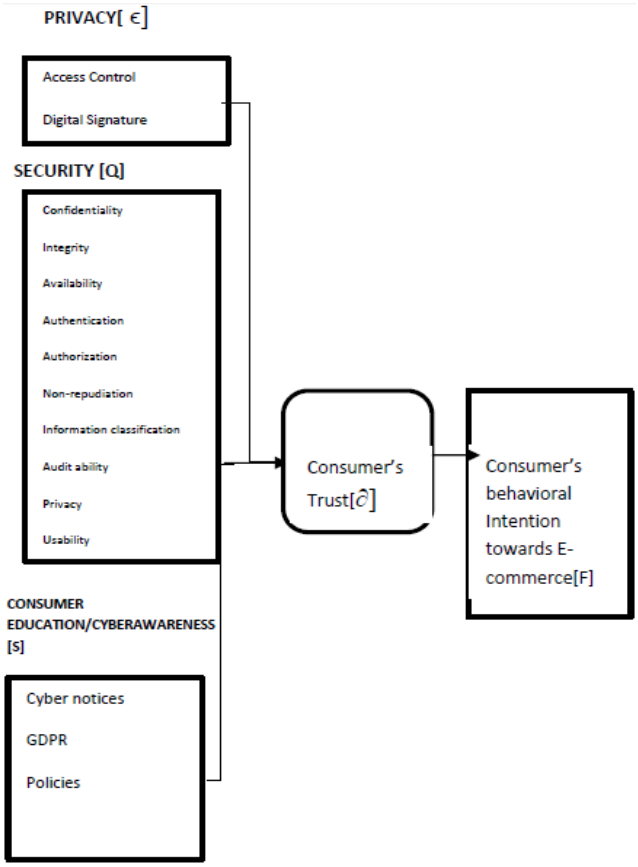

Figure 2: An Architecture of the proposed E-commerce trust and security model

The state of E-commerce security in Nigeria denoted by E can be represented by a set of 5-Tuple of a finite state machine. A finite state automata consisting of 5 features (Q, ϵ, ∂, S , F) . In the proposed E-commerce model, we represent the 10 elements of security by a finite set Q, ϵ is a finite set of E-commerce privacy measure and mechanisms consisting of digital signature and Access control. ∂ is the transition function to have a state of secured E-commerce in Nigeria and ∂ in this model is the trust that consumers or users have in the E-commerce initiative. S is the start state whereby consumers have considerable level of knowledge or awareness about the security of E-commerce in Nigeria. F is the final state of consumer's behavioral intention towards E-commerce in Nigeria which informs their decision to buy goods online or not.

E=[Q, ϵ ,∂ ,S, F), E=Q x ϵ an ordered pair to transit to a state of secured E-commerce denoted by ∂.
Q={ confidentiality, Integrity, Availability, Usability, Authorization, Authentication, Privacy, Auditability, Non-repudiation ,Information classification}
ϵ={ Access control, Digital signature}
∂= transition state of consumer's trust in E-commerce
S= start state where consumer's have the required level of security education
F= final state of E-commerce where behavioral intention of consumers towards E-commerce is positive.

The model suggested that Trust was an important intermediary variable that influences behavioral intention for online transactions. This work addresses how the security variables influences the trust and ultimate behavior of consumers towards online transactions.

4.0 CONCLUSION

Security as regards E- commerce is considered as the most important factor affecting its adoption. This survey examines some requirements for Trust, Privacy and the Security of E-commerce in order to provide a baseline for the buying and selling of goods online on a secured platform. The discussion is supported by the findings from two surveys which were conducted among both users and non-users (i.e. potential target consumers) of e-commerce and commercial businesses. These surveys considered both the attitudes to E-commerce in general and opinions relating to the associated security requirements. The results show that consumers behavior towards E-commerce is affected by their security concerns, mostly on the integrity, privacy, availability, confidentiality, authorization, authentication, non-repudiation, usability, information classification and auditability of the information used when they transact businesses online.

REFERENCES

[1] Ibrahim S. A. "Digital Signature in E-commerce security", *Middle East Journal for Scientific Publishing*, Vol 1, Issue 1, 2018.

[2] Osho F. Christoper I.O, Ugwu J. N. "E-Commerce in Nigeria: A Survey of Security Awareness of Customers and Factors that Influence Acceptance" .CoRI'16, Sept 7–9, 2016, Ibadan, Nigeria.

[3] Ladan M. I. "E-commerce security challeneges, A Taxonomy", *Journal of Economics, Business and Management*, Vol. 4, 2016.

[4] Pareek, N. "Design and Analysis of Access Control and Security Model in E-commerce System", *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 5, Issue 5, May 2016

[5] Kirti Saxena "E-commerce securirty,- A life cycle approach", *International Journal of Latest Trends in Engineering and Technology* (IJLTET), 2013.

[6] Gadheer, N., and Moammed A. P"rivacy, security, risk and trust concerns in E-commerce", conference paper, 2018; www.researcgate.com

[7] Pratap, K. K., Sashank, K., and Bires, K. "Usability and Security Issues in the implementation of E-commerce website", *International journal of scientific research in computer science, engineering and information technology* Vol 6, issue 3, 2020.

[8] Badotra, S., and Amit, S. "A Systematic review of security in Electronic commerce, threats and frameworks", *International Journal of applied science and Engineering* Vol 18, issue 3, 2021.

[9] Krishnan, S. "E-commerce Issues on Customer's Awareness in Malaysia" *Malaysia International Journal of Finance and Accounting* 2017.

[10] Muneer A*, Razzaq S and Farooq Z. Journal of accounting and marketing, Vol 7, issue 3, 2018.

[11] Revathi C, Shanthi K, Saranya, A.R . "A study on E-commerce security issues", 2015.

[12] Niranjanamurthy, M., and D. R. D. Chahar, D. R. D. "The study of E-Commerce Security Issues and Solutions," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, 2013.

[13] Amit M, Abdulrahman A, Josep E and Idris R "Analysis of E-Commerce Security System in Nigeria, International Journal of Scientific Research in Computer Science", *Engineering and Information Technolo*, Volume 2, 2017.

[14] Pradnya B. R. "Transaction Security for E-commerce Application", 2014.

[15] Rajesh K. "Security issues and guidelines for a successful E-commerce system", *International Journal for research and Analytical reviews* Vol 5, issue 2, 2018.

[16] Obafemi, M. "The challenges of globalization on ecommerce in Nigeria". Master's thesis, 2012, Ahmadu Bello University, Zaria, Nigeria.

[17] Wen, Y., and Zhou, C. "Research on e-commerce security issues," *International Seminar on Business and Information Management*, 2008.

[18] Kuruwitaarachi N, Abeyguna, P. K., Wardena, U. L,, Rupasingha, S. W., Wudara, I. *International Journal of Computer science and technology* Vol 9 Issue 1, 2019.

[19] Norjihan A. G, Harihodin, S. and Zailani M. S," "Analysis of Existing Privacy-Aware Access Control for Ecommerce", *Global journal of computer science and technology*, Volume 12 Issue 4 Version February 2012.

[20] Andeh, C., Amujo, O., Aliyu, O. International Journal of Advances in Scientific research and engineering, issue 9, 2019.

[21] Liu, C., Marchewka, J. T., Lu, J., and Yu, C. S., "Beyond Concern, A privacy-trust-behavioral intention model of electronic commerce". *Information & Management*, *42*(2), 2005.