ISSN:.....Print

Journal of Computing, Science &Technology

https://focjournal.unidel.edu.ng/
editorjcst@unidel.edu.ng

ISSN: ..... Online

Improving Customer Trust through Fraud Prevention E-Commerce Model

Sebastina Nkechi Okofu[1], Maureen Ifeanyi Akazue[2], Amanda Enaodona Oweimieotu[3],Rita Erhovwo Ako[4], Arnold Adimabua Ojugo[5], & Clive Asuai[6]

[1]Department of Marketing and Entrepreneurship, Faculty of Management Science, Delta State University, Abraka, Nigeria., [2,6]Department of Computer Science, Faculty of Science, Delta State University, Abraka, Nigeria., [3]Department of Mathematical Science, Faculty of Science, Edwin Clark University, Kiagbodo, Nigeria, [4,5]Department of Computer Science, College of Science, Federal University of Petroleum Resources, Effurun, Nigeria.

okofuseb@gmail.com[1], akazue@delsu.edu.ng[2], amandaoweimieotu@gmail.com[3], ochukorita2@gmail.com[4], Ojugo.arnold@fupre.edu.ng[5], Cliveebomagune@gmail.com[6]

Corresponding Author's Email: okofuseb@gmail.com

Article Info
Date Received: 02-03-2024
Date Accepted: 06-05-2024

Keywords:

Authentication; rule-Based techniques; Central Merchant Registration Retrieval (CMRR) System; Trust; Business to Consumer e-commerce

ABSTRACT

The advancement of E-commerce brings trust concerns in society, due to the lack of physical inspection of items by customers. Online fraud is badly menacing the customers and e-commerce boom in society because E-commerce has removed the barriers of physical contact between merchants and customers in the business environment thus making the online transaction to be vulnerable. This has brought some challenges and of most importance is customers' trust amidst fraudulent transactions. The problem of customer trust due to fraud has mandated greater cooperation between organizations and customers to enhance trust. In this paper, a Multi-Authentication E-commerce (MAE) system that uses rule-based methods and distinct checks to prevent fraud from false virtual stores, thus enhancing customers' trust, was designed using a Java card fraud detection framework, configured rules, customized filters, and tools, to achieve high rates of fraud prevention. This model uses a centralized merchant registration retrieval (CMRR) system to ensure efficiency, accuracy, and comprehensive customer fraud prevention and support. The MAE model was tested and evaluated using multiple regression analysis on the data generated on IBM SPSS 2.0. The result revealed that customer trust is guaranteed and enhanced in the MAE model because fraud is prevented when the merchant's location is verified. The CMRR component can guarantee merchant integrity. The evaluation of the parameters used in the data analysis of the structured questionnaire showed that customers' trust is dependent on fraud prevention and trust is enhanced through the use of CMRR for fraud prevention in online transactions. In future, another algorithm can be combined with rule-based technique to counter new fraudulent actions as it will enhance the efficiency of the CMRR.

2.0 INTRODUCTION

Computer technology has emerged as a valuable tool for addressing diverse human and organizational challenges. It has found application in various domains, including predicting health survival rates [1-4] enhancing security measures [5-9], tackling educational obstacles [10], and exploring trust in technology [11-15]. By leveraging advanced technologies, computer systems have significantly transformed the identification and prevention of fraudulent activities, particularly in e-commerce transactions. They have proved instrumental in detecting various forms of cyber-attacks and fraud, including identity theft, credit card fraud, account takeover, transactional fraud, and e-commerce fraud. The application of computers in e-commerce fraud detection has revolutionized the process, allowing for more accurate and effective identification and prevention of fraudulent activities in online transactions.

The increasing threat of fraud committed in e-commerce transactions is claiming attention in the society in which we live. Most countries utilize existing laws of society to combat fraud committed by customers and/or merchants in E-commerce transactions. In the society, legal protection is provided for victims of fraud. But, the presence of fraud in the transaction makes customer lose confidence or trust in the system. Moreover, the advancement of E-commerce brings along obvious trust concerns in society, due to the lack of physical inspection of items [16]. Thousands of online fraud attacks are perpetrated on customers and sellers that provide online transactions. Thus, online fraud is badly menacing the customers and e-commerce boom in society because E-commerce has removed the barriers of physical contact between merchants and customers in the business environment thus making the online transaction to be vulnerable. Also, available information from national authorities suggests that Business-to-consumer (B2C) e-commerce is expanding rapidly. However, its role remains relatively low when compared to traditional retail and Business-to-Business (B2B) e-commerce [17-20]. In the United States, for example, B2C e-commerce retail sales have grown by over USD133 billion since 2000. However, this growth is relatively limited as it accounts for less than 4% of total retail sales [21]. B2B, on the other hand, generates USD 3.1 trillion in sales which is over 27% of total B2B transactions [22].

There are four important stages involved in a B2C transaction flow. They include Bill and ship address, purchase information, online payment, and delivery. In any of these four stages, valuable information of the customer such as name, date of birth, address, credit card number, and other personal could be stolen. This could create opportunities for fraud which can affect customers' trust [23, 24].

2.0 RELATED WORKS

Over the years, there has been an increasing interest in research efforts to develop customer-merchant trust models that can mitigate fraud and invariably enhance trust [5,7,25-29]. Several types of online fraud are menacing the society economy. This fraud includes false web traders, fake payment companies, and undelivered goods and services [30]. Victims of Internet fraud or cybercrime often lose confidence and trust in e-commerce transactions thus affecting sales revenue and the country's economy [20,31].

In the Nigerian economy, for example, cybercrime has depressed the confidence of traders and investors. Cybercrime is capable of compromising the national security and the citizens' prosperity [18, 32].

Online auction is fast becoming popular overtaking traditional auction, example includes olx.com, and quickr.com. This advancement also brings along obvious trust concerns in society, due to the lack of physical inspection of the item under auction in an online environment which is present in traditional auction systems. Security and privacy are crucial considerations for a customer to feel confident when making an online transaction. [33][34] conducted research based on secondary data to examine the key components of trust in e-commerce, understanding customer trust, the parties to trust in electronic commerce, tactics to promote trust, and ways to increase customer trust in electronic commerce. The findings of the report indicate that consumers desire a seamless and hassle-free shopping experience where they can place orders without encountering any complications.[33] conducted a study focusing on consumer online trust in B2C e-commerce, specifically among consumers in Ekaterinburg, Russian Federation. Their research aimed to identify the key factors that influence trust in this context. The findings of the study revealed that perceived security was the most significant determinant of online trust among consumers in Ekaterinburg.

[35] addressed the problem of false reputation, which refers to the manipulation of ratings by unfair users. To tackle this issue, they proposed an algorithm that relies on the customer's confidence to establish a true reputation. The algorithm effectively identifies malicious users and mitigates their influence on the computation of trust scores. These malicious users may attempt to boost their reputation or undermine the reputation of their competitors. The study further demonstrated that the proposed algorithm enables the determination of individual dimensional scores for each product. This information facilitates self-improvement in areas where a product may be lacking, leading to overall enhancements in product quality.

In his study, [36] employed a mixed methods approach that included both quantitative and qualitative components to explore the effectiveness of computer-aided systems in detecting and preventing fraudulent transactions in e-commerce. The researcher conducted interviews with experts from fraud prevention companies to gain insights into the traditional methods employed in the e-commerce mail-order business for fraud prevention. Additionally, a dataset containing transactions from one of Europe's largest e-commerce firms was analyzed. As part of the study, Knuth developed a predictive model that aimed to identify fraudulent transactions.

2.1 Technology Enhanced Trust Models in e-commerce

The summary of the various technology-enhanced trust models in e-commerce as they relate to preventing fraud and enhancing trust are stated as follows:

As e-commerce websites continue to offer predictive analytics-based advice (PAA), such as forecasts on future price reductions, there are novel and distinct challenges in building consumer trust in these systems. [37] presented a novel approach to address the challenge of establishing consumer trust in predictive analytics-based advice (PAA) systems, particularly in the context of e-commerce websites. Their proposed system utilizes Toulmin's Argumentation Model to enhance trust in these advice-giving systems. The study provided evidence highlighting the importance of different types of statements in fostering trust and enhancing various trusting beliefs within PAA systems.

[5] highlighted how false virtual stores are distinguished from legitimate online stores. In their work, CMMR was an efficient e-commerce component that was used in identifying and confirming merchant locations. Also, a structured questionnaire was distributed to customers who buy online goods and services to evaluate the use of CMRR, a technology-enhanced system, in distinguishing false virtual stores and the result favored the use of CMMR tool to distinguish false virtual stores from legitimate online stores.

[38] addressed the challenges faced in price prediction within the e-commerce industry, particularly when constrained by Look-to-Book or Call-Limit bounds commonly used in the Travel industry. They emphasized the complexity arising from highly inconsistent pricing behavior, which encompasses a combination of trends and anomalies. To tackle this issue, the researchers proposed an Efficient Query-Optimal E-Commerce Pricing Model Discovery Using Active Learning, which aims to strike a balance between accurate price prediction and the cost

associated with collecting the data upon which the prediction model relies.

The enhancement of customers' trust in e-commerce through a secure payment model has been investigated with reliable results by several researchers. [40] highlighted how a centralized merchant registration retrieval (CMRR) component of the e-commerce model was used to serve as an advisory tool that identifies cloned payment pages in an e-commerce transaction. The authors did an online evaluation of the use of CMRR in identifying cloned payment pages and acting as an advisory tool to customers. Their analysis showed that CMRR can identify cloned payment pages by URL difference from the merchant's original URL address at the point of registration with the corporate affair of the country and that customers' confidence and trust in the purchase of online goods and services are enhanced by mitigating fake virtual stores fraud.

2.2 Problem Formulation:

Every e-commerce model has its capabilities and limitations. For instance: [40-44] focused on credit card fraud prevention in e-commerce transactions. In other words, their works focused on merchant (Seller) protection in e-commerce transactions as well as virtual shop protection. Their works did not discuss measures that will enhance customer's trust through the checking of merchant integrity which the CMRR does.

Furthermore, [45] conducted a study to examine the factors that influence e-customer trust and e-customer loyalty in the Business-to-Consumer (B2C) domain. The researchers employed exploratory factor analysis, confirmatory factor analysis, and structural equation modeling (SEM) to test their hypotheses.

[7,28,29] Models were adopted in this design and implementation. The MAE model proposes the use of a CMRR, which will consistently check virtual stores without involving the customer or the merchant, to authenticate and distinguish fraudulent virtual stores and enhance legitimate transactions.

There are numerous trust theories. Among these are the Organization theory [46], Economic theory [47], and Systems Theory [48] applied in this work.

This research paper proposed the use of a technology-enhanced fraud prevention e-commerce model known as the Multi Authentication e-commerce (MAE) transaction model to restore confidence and enhance trust in individuals involved in e-commerce transactions [7].

2.2 Evaluating the MAE fraud prevention/detection authentication model

3.0 METHODOLOGY

The detailed procedure and methodology for the practical design and implementation of the e-commerce system is:

- [7] discussed the extracted seven processes (Retail Services, Central Merchant Registration Retrieval Service (CMRRS) which obtains information from Local Merchant Registration Service (LMRS), List Service which houses customers complaints, Merchant Service, Switching Service, Shipping service and Reporting service) make up the components that were used at the implementation stage. Each process has its detailed activity as reported in [8]. These seven processes were used for implementation.
- Rule-based detection, customized filters, and intelligent tools used for fraud prevention were also applied in the implementation.
- Electronic Java Bean (EJB), which is a platform-independent and service-based oriented architecture, was used to build the application. MySQL was also used in the design of the e-commerce system database. The technology-enhanced MAE model was developed, tested, validated, and reviewed by the use of a questionnaire. The questionnaire process was used to capture data and the generated data was used to evaluate customer trust and fraud prevention by the MAE system.

3.1 Architecture of MAE-commerce model

The detailed interaction of the various components of the proposed MAE-commerce model was shown in [7]. The workflow of the MAE-commerce authentication model is shown in Figure 1. The model has seven components: Retail Services is the module where transactions occur and payment is made at the Merchant service module (banks). Shipping service module provides transportation means of purchased items. Reporting service is the module that handles the delivery report from shipping service module. The Central Merchant Registration Retrieval Service (CMRRS), our introduced module, obtains information from Local Merchant Registration Service (LMRS) and List Service (List customer complaint), to test and authenticate the integrity of the merchant virtual store and authenticate the payment webpage.

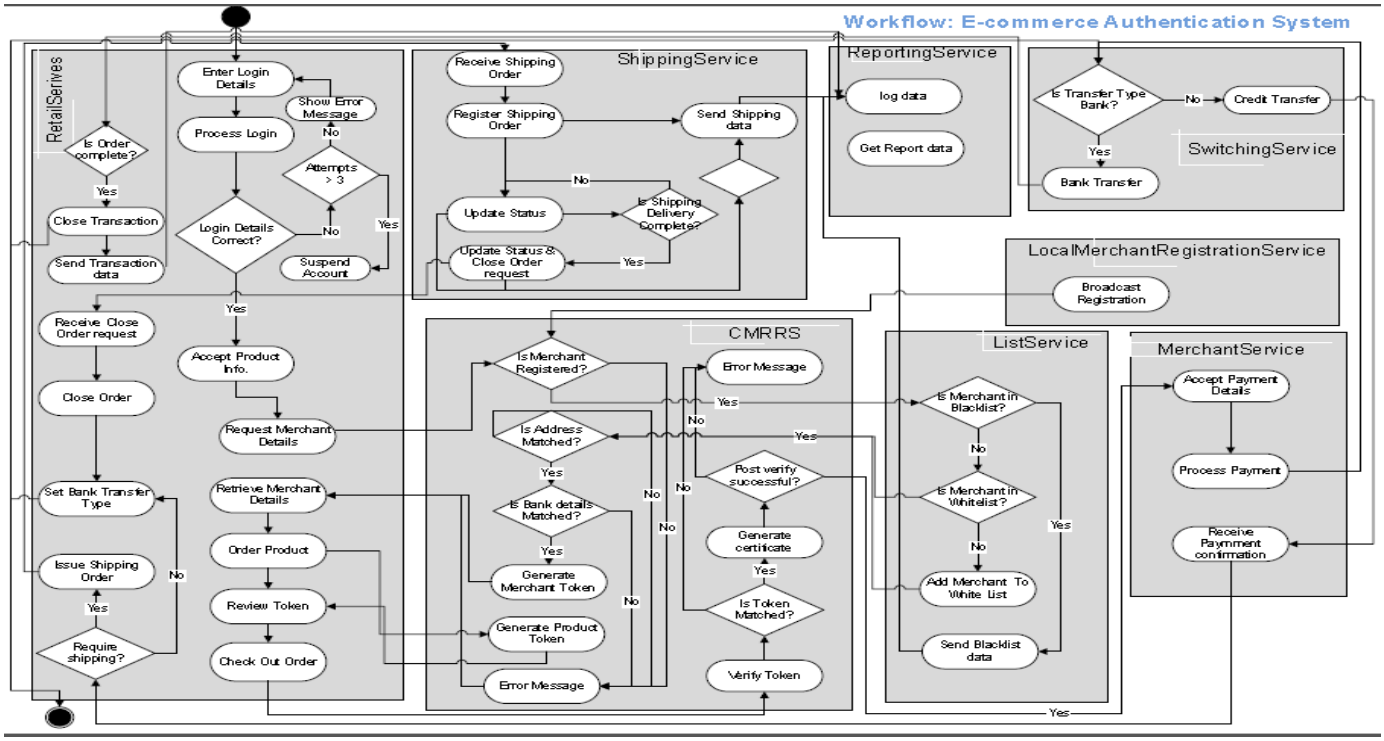

Figure 1: Workflow of Proposed e-commerce Authentication System

Quantifying trust enables us to express in numerical terms, the consumers' trust in the merchant in e-commerce transactions from [49]. We have Eq. (1);

$$C_T = f(M_I) = f(CM_{RS}) \quad (1)$$

Where Customer Trust (C_T) is a function of Merchant Integrity (M_I) which in turn is a function of a centralized merchant retrieval system (CM_{RS}). The study utilizes one (1) dependent variable and one (1) independent variable. The dependent variable which is C_T is measured by M_I and CM_{RS} on the e-commerce website. The M_I and CM_{RS} were the actual variables caused by the controlling influence of the independent variable; Merchant local address, Merchant local Bank details, merchant online address, and merchant online bank details. The notation for these variables is:M_{LA}, M_{LBD}, M_{OA}, and M_{OBD}.

The impact of the variables (factors) on customers' trust is determined by the use of regression theory Eq. (2).

A regression model relates Y to a function of **X** and **β**.

$$Y \approx f(\mathbf{X}, \boldsymbol{\beta}) \quad (2)$$

Where:

- The unknown parameters, denoted as β.
- The independent variables, X.

The dependent variable, Y.

2.3 The Research Instrument

Most questions were broad to give room for respondents to define the situation. The focus was on the influence of technology-enhanced CMRR components in e-commerce websites in enhancing customer trust by preventing fraud in e-commerce transactions. To test the MAE model online, some online customers were administered a set of questionnaires consisting of three sections. The questionnaire was used to elicit data on customer trust, and merchant integrity and to compare the results. Also, the questionnaire used a five-scale type to measure how the CMRR component checks merchants' integrity to prevent fraud which invariably enhances customers' trust. The respondents were asked to express their opinions on each question and each question was a 5-point Likert item from which respondents were to pick an option ranging from; Neutral, Strongly Agreed, Agreed, Disagree, and Strongly disagreed. The scaling of the options was done with a scale of 0-4, where Neutral = 0, Strongly Agreed = 4, Agreed = 3, Disagree = 2, and Strongly disagreed = 1. The scales are digital which is discrete because specific values are used.

2.4 Method Justification

Twenty-one users responded and the data obtained was analyzed using regression analysis. Regression analysis is one of the most commonly used statistical techniques that explore the relationship between a dependent variable and one or more independent variables (which are also called predictor or explanatory variables). In all cases, the estimation target is a function of the independent variables called the regression function. Regression analysis is used to understand which among the independent variables are related to the dependent variable and to explore the forms of these relationships [49].

Thus, Linear regression explores relationships that can be readily described by straight lines or their generalization to many dimensions and a large number of problems can be solved by linear regression.

Therefore, in multiple linear regression, there are several

independent variables or functions of independent variables. For instance, the equation of the Jumia commercial site is Eq. (3) while the MAE model is Eq. (4):

$$y_1 = \beta_O + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4 + \beta_5 x_5 + \in_i \text{ - - - (3)}$$

$$y_2 = \beta_O + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4 + \beta_5 x_5 + \in_i \text{ - - (4)}$$

Where,

y_1 : Customer's Trust in the Jumia Commercial Site

y_2 : Customer's Trust in the MAE Model

x_1 : Merchant Integrity in the Jumia Commercial Site

x_2 : Merchant Integrity in the MAE Model

x_3 : Other Commercial Site Rating to Customers' Trust

x_4 : MAE Model Rating to Customers' Trust

x_5 : Merchant Integrity determined by CMRR

β : Coefficient

$\in_i$: Error Terms

The numbers of variables are: 1,2,3,4 and 5. The five variables used to evaluate merchant integrity were based on the following determining factors: merchant's registration with the Country's corporate affair, Physical location address, bank details, Activity log in the ListService and availability of CMRR component. These factors were used to determine the reality of the merchant's shops online and these enhanced customers's confidence and trust. Cronbach's alpha in SPSS was used to check for the internal consistency of the scale used in evaluating customer trust. The result showed a good Cronbach's Alpha of 0.734 according to Table 1.

Table 1: Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No of Items
.734	.757	39

The detailed analysis of the scale used in the questionnaire is shown in Table 2

5.0 RESULTS AND DISCUSSION

Testing the designed MAE model

To test the MAE model online, online customers were administered a set of questionnaires consisting of three sections. The first section is on Jumia, an existing e-commerce transaction model, the second section is based on the MAE model and the third section is on CMRR, a technology-enhanced fraud prevention component. The questionnaire aimed to elicit data on customer trust, and merchant integrity. Then, compare the results. Twenty-one users responded and the data obtained was analyzed using regression analysis. In this analysis, two different regression models, which follow the general regression model, were used. The two models for the regression are stated in Eq (3) and Eq (4) respectively.

Table 2: Detail Reliabilitv Statistics of the scale used

Questions used to define the dependent and independent variables	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
1. Other ecommerce site Cus Trust payment page not hijacked or cloned	98.9048	57.753	-.142	.748
Other ecommerce site Cus Trust verified merchant	99.0952	55.003	.078	.740
2. Other ecommerce site Cus Trust payment page not compromised	98.7619	53.578	.214	.730
3. Other ecommerce site Cus Trust payment page Authenticity	98.4762	58.699	-.216	.755
4. Other ecommerce site Merchant Integrity based registered merchant	99.1429	56.216	-.002	.742
5. Other ecommerce site Merchant Integrity based on match physical address	98.9524	55.310	.113	.735
6. Other ecommerce site Merchant Integrity based on token from CMRR	99.1905	55.599	.088	.736
7. Other ecommerce site Merchant Integrity based on physical traced of merchant	99.1429	54.691	.193	.731
8. MAE site Cus Trust payment page not hijacked or cloned	97.5714	56.970	-.071	.747
9. MAE site Cus Trust verified merchant	97.5238	48.099	.605	.701
10. MAE site Cus Trust payment page not compromised	97.3810	55.835	.095	.734
11. MAE site Cus Trust payment page Authenticity	97.3810	52.410	.479	.717
12. MAE site Merchant Integrity based registered merchant	97.3333	50.446	.616	.708
13. MAE site Merchant Integrity based on match physical address	97.4286	54.270	.186	.731
14. MAE site Merchant Integrity based on token from CMRR	97.4286	50.695	.543	.710
15. MAE site Merchant Integrity based on physical traced of merchant	97.4286	53.070	.348	.723
16. CMRR Effective in detecting clone/hijack payment page	97.3333	54.096	.266	.727
17. CMRR is capable in verifying URL address of retailer from clone site if implemented	97.4286	53.320	.476	.720
18. CMRR necessary component to ensure merchant virtual stores have located physical address	97.0000	55.687	.123	.733
19. CMRR is a good advisory tool that check merchants so as to enhance consumer trust	97.0952	55.903	.081	.735
20. ease of use of Other Ecommerce	98.2381	54.328	.168	.733
21. Other Ecommerce Identify fraudulent virtual stores	99.5238	55.699	.148	.732
22. URL hijack tracking in Other Ecommerce	99.2381	52.978	.390	.721
23. Other Ecommerce ease in identifying Merchant physical address location	99.4286	56.420	.017	.737
24. Other Ecommerce Payment page authentication	99.0952	55.778	.053	.738
25. Other Ecommerce in Merchant Integrity authentication	99.2857	58.927	-.276	.752
26. Other Ecommerce in Credit card validation	98.6667	56.421	-.012	.741
27. ease of use of MAE	97.8571	53.066	.341	.723
28. MAE Identify fraudulent virtual stores	97.5714	53.820	.198	.731
29. URL hijack tracking in MAE	97.9524	51.035	.467	.714
30. MAE ease in identifying Merchant physical address location	97.4762	50.624	.566	.710
31. MAE Payment page authentication	97.4762	51.524	.380	.719
32. MAE in Merchant Integrity authentication	97.4762	53.799	.337	.724
33. MAE in Credit card validation	97.8571	53.391	.267	.727
34. Other ecommerce site has enhanced Cus Trust payment page	98.8095	55.862	.097	.734
35. Other ecommerce site has enhanced Merchant Integrity	99.1071	55.210	.222	.730
36. MAE site has enhanced Cus Trust payment page	97.4643	52.971	.630	.717
37. MAE site has enhanced Merchant Integrity based on physical traced of merchant	97.4048	51.897	.640	.713
38. CMRR is a good advisory tool that check merchants so as to enhance consumer trust	97.2143	54.558	.577	.724

The regression model Eq (3) was used to evaluate the JUMIA e-commerce model while the regression model Eq (4) was used to evaluate the MAE model. The regression analysis result of customers' trust using the JUMIA model is presented in Table 3. The dependable variable is

Table 3: Regression Result on the JUMIA Model (Dependent Variable: Y_1)

Variable	Coefficient â	Std. Error	t-Statistic	Prob.
C	2.241990	1.676858	1.337018	0.2025
X_5	0.174708	0.432069	0.404352	0.6921
X_4	-0.226526	0.224323	-1.009821	0.3297
X_2	-0.104118	0.216160	-0.481669	0.6375
X_3	-0.446409	0.335712	-1.329737	0.2049
X_1	0.490286	0.234563	2.090212	0.0553
R-squared	0.417212	Mean dependent var		1.875000
Adjusted R-squared	0.209074	S.D. dependent var		0.455233
S.E. of regression	0.404857	Akaike info criterion		1.272758
Sum squared resid	2.294726	Schwarz criterion		1.571478
Log-likelihood	-6.727583	F-statistic		2.004494
Durbin-Watson stat	1.158350	Prob(F-statistic)		0.140350

customers' trust in the Jumia commercial site (Y_1), while merchant integrity in the Jumia commercial site (X_1), merchant integrity in the MAE model (X_2), Jumia commercial site rating to customers' trust (X_3), MAE model rating to customers' trust (X_4) and merchant integrity determined by CMRR (X_5) are the independent variables.

The model's adjusted coefficient of determination(R^2) shows that only about 20.9% of the variations incustomers' trust in the JUMIA commercial site (Y_1)are explained by the combined influence of merchant integrity in the JUMIA commercial site (X_1), merchant integrity in the MAE model (X_2), JUMIA commercialsite rating to customers' trust (X_3), MAE model rating to customers' trust (X_4) and merchant integrity determined by C MRR (X_5).

The F-statistics value of 2.00 is highly insignificant at a 5% significant level. The 5% critical value for the analysis is 0.1403 of the JUMIA model. The insignificant of the F-Statistic tells us that no linear relationship exists between the dependent variable and its determinants.

Furthermore, with regards to the signs of the independent variables, it was observed from the results that merchant integrity in the JUMIA commercial site (X_1) and merchant integrity determined by CMRR (X_5) have positive signs. This indicates that these variables have a positive relationship with customer trust in the JUMIA commercial site (Y_1). Also, Merchant integrity in the MAE model (X_2), JUMIA commercial site rating to customers' trust (X_3), and MAE model rating to customers' trust (X_4) all have negative signs. This is a further indication that they all have a negative relationship with customers' trust in the JUMIA commercial site (Y_1) and none of the independent variables are significant at the 5% significance level.

Hence, this study reveals that the JUMIA commercial site has lesser customer trust, due to its drawbacks which include: vulnerability to hacking, lack of merchant verification capability, susceptibility of the payment page to cloning, and lack of merchant integrity verifying capability such as verifying if a merchant is duly registered with the cooperate affairs commission of the country where the business is located, traceability of merchant physical location, merchant information consistency checks, and availability and verifiability of CMMR token.

Table 4 represents the regression result of customers' trust using the MAE model. The dependable variable is customers trust in the MAE model (Y_2), while merchant integrity in the JUMIA commercial site (X_1), merchantintegrity in the MAE model (X_2), JUMIA commercial site rating to customers' trust (X_3), MAE model rating to customers' trust (X_4) and merchant integrity determined by CMRR (X_5) are the independent variables. The model's adjusted coefficient of determination (R^2) shows that only about 45.55% of the variations in customer trust in the MAE model (Y_2) are explained by the combined influence of merchant integrity in the JUMIAcommercial site(X_1),merchant integrity in the MAE model (X_2),
JUMIA commercial site rating to customers' trust(X_3), MAE model rating to customers' trust (X_4), and merchant integrity determined by CMRR (X_5).

In addition, The F-statistics value of 4.18 is highly significant at a 5% significant level. The 5% critical value for the analysis is 0.0156 of the proposed system. The significance of the F-Statistic shows that a linear relationship exists between the dependent variable and its determinants. The model is free of autocorrelation and this made the model very efficient and the test of regression coefficient very reliable; this can be interpreted from the Durbin-Watson statistics result which is 1.814.

Also, concerning the signs of the independent variables, it was observed from the results that merchant integrity in the MAE model (X_2), JUMIA commercial site rating to customers' trust (X_3), and MAE model rating to customers' trust (X_4), and merchant integrity determined by CMRR (X_5) have positive signs. This indicates that these variables have a positive relationship with customers' trust in the MAE model (Y_2). In addition, Merchant integrity in the JUMIA commercial site (X_1) has negative signs. This is an indication that it has a negative relationship with customers' trust in the MAE model (Y_2). Only merchant integrity in the MAE model (X_2) is significant at the 5% significance level. The other independent variables are not significant at the 5% significance level.

Therefore, this study reveals that customers' trust in the MAE model is greatly enhanced due to several advantages of the MAE model in mitigating fraud, amongst which include: the non-susceptibility of the site to hacking, none-susceptibility of payment page to cloning, customer and

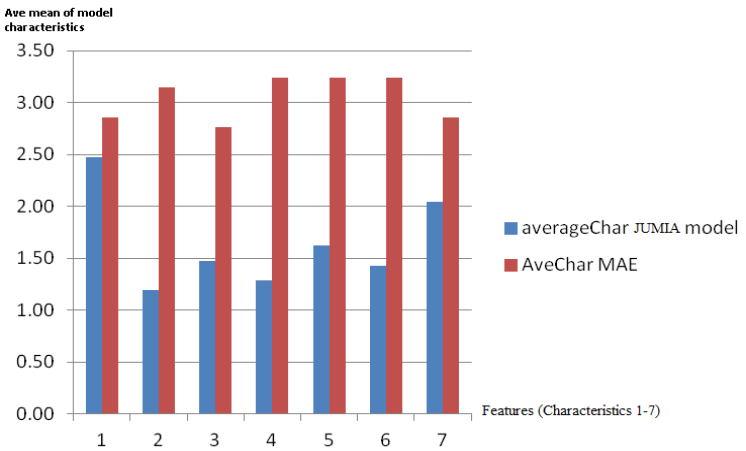

Figure 6: A comparative study of the features of the MAE model with JUMIA e-commerce models using a line chart

merchant are aware that the site cannot be hacked, goods can be verified, payment page cannot be compromised and the web site is trusted. Also, merchant integrity is guaranteed, because it can be verified if the merchant is registered with its corporate affairs commission, if its address is real, if the site has a token from CMRR and the information of every merchant can be traced or located.
From the generated result the MAE model was compared with JUMIA e-commerce models and the findings are tabulated in Table 5 and Table 6.

Table 5: A comparative study of the MAE model and JUMIA e-commerce models

Table 6: A comparative study of the MAE model and JUMIA e-commerce models using the average mean values

Characteristic	JUMIA model	MAE model	Existing model diff	MAE diff	% strength of MAE model
Ease of use	2.48	2.86	0.464419	0.535581	7.116105
Identify fraudulent virtual stores	1.19	3.14	0.274827	0.725173	45.03464
URL hijack tracking	1.48	2.76	0.349057	0.650943	30.18868
Ease in identifying Merchant Physical address location	1.29	3.24	0.284768	0.715232	43.04636
Payment page authentication	1.62	3.24	0.333333	0.666667	33.33333
Merchant integrity authentication	1.43	3.24	0.30621	0.69379	38.75803
Credit Card Validation	2.05	2.86	0.417515	0.582485	16.49695

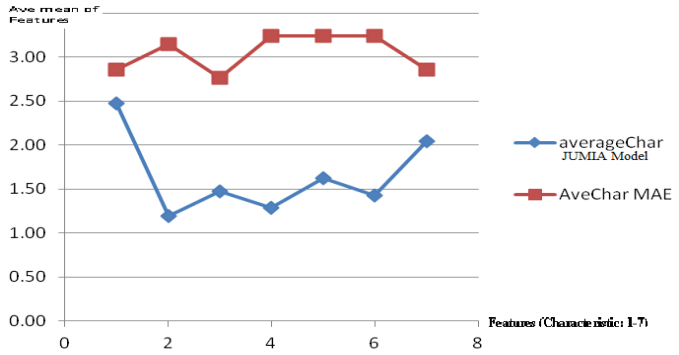

Figure 7: A comparative study of the features of the MAE model with JUMIA e-commerce models using a column chart

The customer's response on the Trusting MAE model (Table 7) with JUMIA e-commerce models (Table 8) using a line chart is shown in Figure 8. In the graphical representation, only9% (two respondents) said that there is no difference in trusting either of the models, while 91% (19 respondents) agreed that the MAE model has enhanced customer trust ine-commerce transactions.
The higher values signify better performances of the model in possessing the stated characteristics. In other words, when the average mean value of the users' response is lower than 2.0, it signifies that the model is not efficient in the stated characteristic.
The strength of the MAE model over existing models is shown by the percentage difference in the ability of the MAE model to; identify fraudulent virtual stores (45%), ease in identifying merchant physical address location (43%), merchant integrity authentication (39%), URL hijack tracking (30%), and payment page authentication (33%).
The graphical representations of the characteristics of the MAE model with JUMIA e-commerce models using the average mean values are shown in Figure 6 and Figure 7

Table 7: Customer trust on the MAE Model

The customer trusts the MAE				Average response on Customer Trust MAE
Q9	Q10	Q11	Q12	
4	3	4	4	3.75
3	2	4	3	3.00
3	4	3	4	3.50
4	4	3	3	3.50
3	3	3	3	3.00
4	3	4	3	3.50
3	4	3	4	3.50
3	4	3	3	3.25
2	4	3	4	3.25
1	4	3	4	3.00
3	3	3	4	3.25
4	2	3	2	2.75
3	2	3	3	2.75
3	4	3	3	3.25
4	3	4	4	3.75
3	1	3	3	2.50
2	2	3	3	2.50
4	4	4	3	3.75
3	3	4	3	3.25
4	4	3	3	3.50
3	4	4	4	3.75

Table 8: Customer trust in the JUMIA Model

Customers trust the JUMIA model				Average response on Customer Trust JUMIA
Q1	Q2	Q3	Q4	
1	2	2	1	1.50
2	0	2	4	2.00
2	1	1	2	1.50
1	1	1	1	1.00
2	2	1	2	1.75
1	2	2	2	1.75
2	1	2	2	1.75
2	1	2	3	2.00
1	3	3	2	2.25
1	3	4	2	2.50
2	1	2	2	1.75
3	3	2	3	2.75
3	2	3	3	2.75
2	2	2	2	2.00
2	2	3	1	2.00
2	2	1	3	2.00
2	2	2	2	2.00
1	1	2	2	1.50
2	0	1	2	1.25
1	1	1	3	1.50
3	2	2	3	2.50

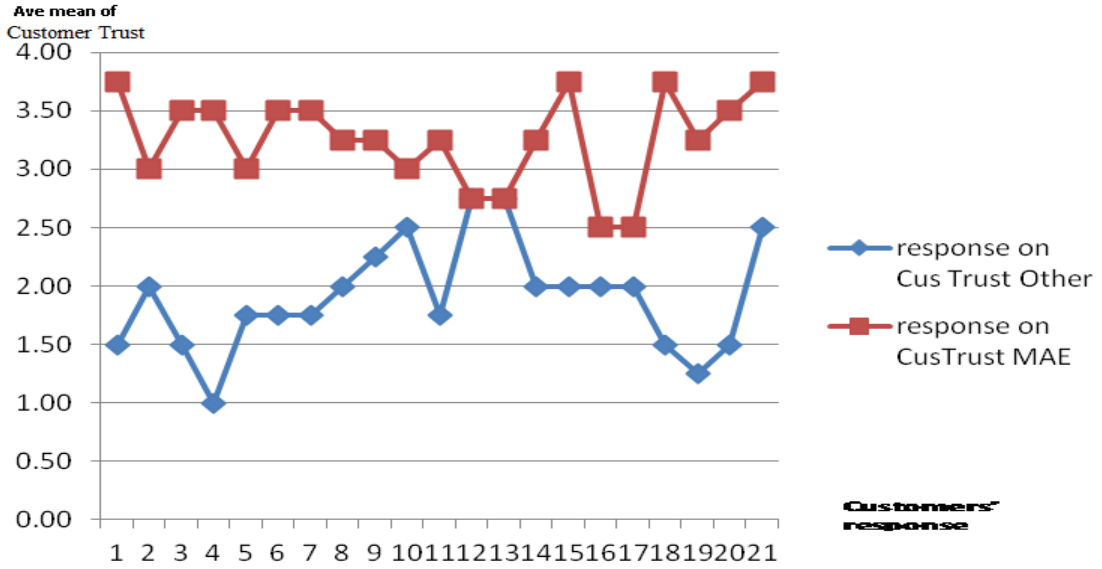

Figure 8: A Comparative Study Of Customers' Response to Trusting the MAE model with JUMIA e-commerce Models Using A Line Chart

Table 9: Merchant Integrity in MAE

[redacted]

Table 10: Merchant Integrity in JUMIA model

[redacted]

Also, the degree of customers believing in the integrity of merchants in the JUMIA model and MAE model is shown in table 9 and table 10 respectively.

The graphical representation in Figure 9 represents the customer's response on Trusting Merchant Integrity in the MAE model over JUMIA e-commerce models is enhanced by using a centralized merchant registration retrieval system.

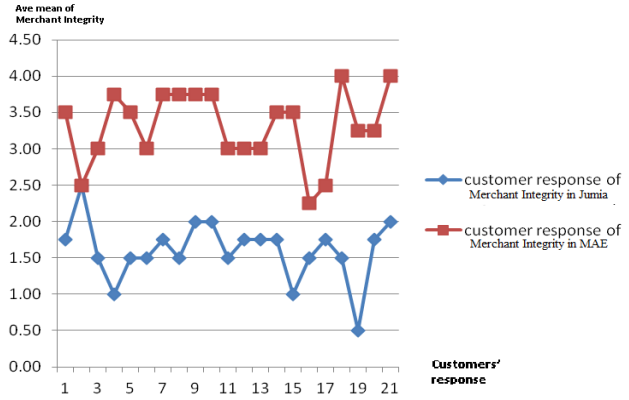

Figure 9: A comparative study of customers' responses on Trusting Merchant Integrity in the MAE model with JUMIA e-commerce models using a line chart

6.0 CONCLUSION

The analysis has demonstrated that MAE model increases customer trust in e-commerce transactions by the significance of the F-Statistic value of 4.18 at a 5% significant level. The 5% critical value for our MAE analysis is 0.0156 and from the analysis, only merchant integrity in the MAE model (X2) is significant at the 5% significance level.

The MAE commerce transaction model has addressed the This research provides a framework on which further research on customer trust against fraudulent merchants and fake virtual stores can be built. Other factors that will enhance merchant integrity, such as the legal aspect, can also be researched and incorporated.

Author's notes

All authors participated in the design of the study, and the critical review and revision of the article for important intellectual content about their specialties. All authors read and approved the final version of the article for publication.

Acknowledgments

We would like to extend our heartfelt thanks and deep appreciation to all the individuals and Tetfund Nigeria, who have played a vital role in the successful completion of this work.

REFERENCES

[1] I. Ajenaghughrure, P. Sujatha and M. Akazue (2017), Fuzzy based multi-fever symptom classifier diagnosis model, International Journal of Information Technology and Computer Science, 9(10):13-28. DOI: 10.5815/ijitcs.2017.10.02

[2] D. Ojie, M. Akazue and A. Imianvan,(2023), A Framework for Feature Selection using Data Value Metric and Genetic Algorithm, International Journal of Computer Applications, 184(43): 14-21. DOI: 10.5120/ijca2023922533.

[3] M. I. Akazue, R. E. Yoro, B.O. Malasowe, O. Nwankwo and A. A. Ojugo, (2023), Improved services traceability and management of a food value chain using block-chain network: A case of Nigeria, Indonesian Journal of Electrical Engineering and Computer Science, 29(3): 1623-1633.

[4] M. Akazue and N. F. Efozia, (2010), A Review of Biometric Technique for Securing Corporate Stored Data, Software Engineering and Intelligent Systems, 1, 329-342.

[5] M. Akazue and A. Aghaulor, (2015), Identification of Cloned Payment Page in Ecommerce Transaction, International Management Review, 11(2): 70-76.

[6] R. E. Yoro, F. O. Aghware, M. I. Akazue, A. E. Ibor and A. A. Ojugo, A. A. (2023), Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian, International Journal of Electrical and Computer Engineering, 13(2): 1943.

problem of false web merchants and how it results in fraud and thus makes the customer lose confidence and trust. The technology-driven model will enhance the trust of those individuals who are involved in e-commerce and thus boost the business economy. Findings from this paper can be used for future research work in the area of trust in B2C e-commerce and to address further the importance of fraud prevention management on the Internet.

6.1 Suggestion for further studies

[7] M. I. Akazue, (2015), A Survey of Ecommerce Transaction Fraud Prevention Models, In The Proceedings of the International Conference on Digital Information Processing, Data Mining, and Wireless Communications, Dubai, UAE.

[8] A. A. Ojugo, M. I. Akazue, P.O. Ejeh, C. C. Odiakaose and F.U. Emordi, (May, 2023). DeGATraMoNN: Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing. KongzhiyuJuece/Control and Decision, 38(01): ISSN: 1001-0920.

[9] M. I. Akazue and I.B. Ajenaghughrure, (2016), Virtual Examination Supervision System for Nigerian Universities, International Journal of Modern Education and Computer Science (IJMECS), 8(9): 43-50.

[10] M. I. Akazue, and C. O. Onyekweli, (2019), Awareness of the Knowledge, Perception, Impact and Usability of CAPTCHA Security Technology, Nigerian Journal of Science and Environment, 17: 9-25

[11] S. Okofu, E. K. Anazia, M. Akazue, C. Ogeh and I. B. Ajenaghughrure, (2023). The Interplay between Trust In Human-Like Technologies And Integral Emotions: Google Assistant, KongzhiyuJuece/Control and Decision, Volume 38, Issue 01, April 2023, ISSN: 1001-0920.

[12] M. Akazue, (2016), Enhanced Hotel Management Information System for Multiple Reservation Booking, Int. Manag. Rev., 12(1): 52.

[13] Akazue, M. I., Nwokolo, G. A., Ejaita, O. A., Ogeh, C. O., & Ufiofio, E. (2023a). Machine Learning Survival Analysis Model for Diabetes Mellitus. International Journal of Innovative Science and Research Technology, 8(4): 754-760.

[14] Ojie, D. V., Akazue, M., Omede, E. U., Oboh, E. O., &Imianvan, A. (2023). Survival Prediction of Cervical Cancer Patients using Genetic Algorithm-Based Data Value Metric and Recurrent Neural Network. International Journal of Soft Computing and Engineering (IJSCE), 13(2), May 2023. ISSN: 2231-2307.

[15] M. Akazue, A. Onovughe, E. Omede, and J.P.C. Hampo, (2023), Use of Adaptive Boosting Algorithm to Estimate Users Trust in the Utilization of Virtual Assistant Systems, International Journal of Innovative Science and Research Technology, 8(1): 502-7. Retrieved from

https://www.ijisrt.com/assets/upload/files/IJISRT23JAN727.pdf
[16] T.V. Vuuren, M. Roberts-Lombard and E. V. Tonder, (2012), Customer satisfaction, trust and commitment as predictors of customer loyalty within an optometric practice environment, Southern African Business Review, 6: 81-96
[17] C. Mei-Jane and H. Yann-Haur, (2009), Factors that affect consumer trust in online shopping in Taiwan, Journal of Global Business Management, 5: 14-20
[18] N. Ribadu, (2007), Cyber-crime and Commercial Fraud: A Nigerian Perspective, Presented at the Congress Celebrating the Fortieth Annual Session of the UNCITRAL (United Nations Commission On International Trade Law), Vienna, Austria. Retrieved from www.uncitral.org/pdf/english/congress/Ribadu_Ibrahim.pdf
[19] I. Bojang, (2017), Determinants of Trust in B2C E-commerce and their Relationship with Consumer Online Trust: A Case of Ekaterinburg, Russian Federation, Journal of Internet Banking and Commerce, 22(3): 1-10.
[20] R. M. Shettar, (2019), Customer Trust in Electronic Commerce: An Overview. IOSR Journal of Business and Management (IOSR-JBM), 21(2): 24-31, doi: 10.9790/487X-2102012431
[21] G. Mol, and S. John, (2017), A Trustworthy Model in E-Commerce by Mining Feedback Comments, International Research Journal of Engineering and Technology (IRJECT), 4(4):2027-32.
[22] T. Knuth, (2018), Fraud Prevention in the B2C E-commerce Mail Order Business: A Framework for an Economic Perspective on Data Mining (Unpublished doctoral dissertation), Edinburgh Napier University.
[23] E. Rubin and I. Benbasat, (2023), Using Toulmin's Argumentation Model to Enhance Trust in Analytics-Based Advice Giving Systems, ACM Transactions on Management Information Systems. Advance online publication. https://doi.org/10.1145/3580479
[24] S. Horovitz, A. Eze and D. Paz, (2021), Efficient Query-Optimal E-Commerce Pricing Model Discovery Using Active Learning, In 2020 2nd International Conference on E-Business and E-Commerce Engineering (EBEE 2020) :1-5, Association for Computing Machinery. https://doi.org/10.1145/3446922.3446923
[25] M.I. Akazue, A. Aghaulor and B. I. Ajenaghughrure, (2015), Customer's Protection in Ecommerce Transaction Through Identifying Fake Online Stores,The Proceedings of the 2015 World Congress in Computer Science, Computer Engineering, and Applied Computing, 52-54
[26] I. Sadgali, N. Sael and F. Benabbou, (2019), Fraud Detection in Credit Card Transaction Using Neural Networks, In Proceedings of the 4th International Conference on Smart City Applications (SCA '19) (Article No. 95). Association for Computing Machinery. https://doi.org/10.1145/3368756.3369082
[27] B. Y. Yuksel, S. Bahtiyar and A. Yilmazer, (2021), Credit Card Fraud Detection with NCA Dimensionality Reduction, In Proceedings of the 13th International Conference on Security of Information and Networks (SIN 2020) (Article No. 18), Association for Computing Machinery. https://doi.org/10.1145/3433174.3433178
[28] Y. Yang, C. Liu, N. Liu, (2020), Credit Card Fraud Detection Based on CSat-Related AdaBoost, In Proceedings of the 2019 8th International Conference on Computing and Pattern Recognition (ICCPR '19) :420-425. Association for Computing Machinery. https://doi.org/10.1145/3373509.3373548
[29] M. Chen, (2023), Credit Card Fraud Detection Based on Multiple Machine Learning Models, In Proceedings of the 2022 6th International Conference on Electronic Information Technology and Computer Engineering (EITCE '22) :1801-1805. Association for Computing Machinery. https://doi.org/10.1145/3573428.3573745
[30] J. Ahammad, N. Hossain M. S. Alam, (2020), Credit Card Fraud Detection Using Data Pre-Processing on Imbalanced Data - Both Oversampling and Undersampling, In Proceedings of the International Conference on Computing Advancements (ICCA 2020) (Article No. 68). Association for Computing Machinery. https://doi.org/10.1145/3377049.3377113
[31] W. Aslam, A. Hussain, K. Farhat and I. Arif, (2019), Underlying Factors Influencing Consumers' Trust and Loyalty in E-commerce, Business Perspectives and Research, 8(2). doi:10.1177/2278533719887451.
[32] S. Pittayachawan and M. Singh,(2004), Trust Models in the E-Commerce Environment, The Fourth International Conference on Electronic Business, Beijing, 901-907. Retrieved from http://iceb.nccu.edu.tw/proceedings/2004/Paper/EN182-paper.pdf.
[33] S. N. Okofu, (2018), Influence of Culture on Youths Buying Behavior, Journal of Social and Management Sciences, 13 (2): 75-82
[34] W. Lomerson and P. Tuten,(2005), Examining Evaluation Across The IT Value Chain, Proceedings of the South Association of Information Systems Conference.
[35] J. S. Armstrong,(2012), Illusions in Regression Analysis. International Journal of Forecasting, 28(3): 689. doi:10.1016/j.ijforecast.2012.02.00.
[36] Jithendra, D. (2006). Credit Card Security and E-payment, Enquiry into credit card fraud in E-

Payment. Masters project, Luleå University of Technology. Retrieved from http://epubl.ltu.se/1653-0187/2006/23/LTU-PB-EX-0623-SE.pdf

[37] A. A. Ojugo, M. I. Akazue, P. O. Ejeh, N. C. Ashioba, C. C. Odiakaose, R. E. Ako, and F. U. Emordi, (2023), Forging a User-Trust Hybrid Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study, Journal of Computing Theories and Applications, vol. 1 (2): 1-11

[38] U. ChiezeyandA. J. C. Onu, (2013), Impact of Fraud and Fraudulent Practices on the Performance of Banks in Nigeria, British Journal of Arts and Social Sciences, 15(1), ISSN: 2046-9578.

[39] M.I. Akazue, G. E. Izakpa, C. O. Ogeh E. Ufiofio, (2023), A secured computer-based test system with resumption capability module, KongzhiyuJuece/Control and Decision, ISSN: 1001-0920, 38(02): 893-904

[40] S. Y, Yousafzai, J. G. Pallister and G. R. Foxall, (2003), A proposed model of e-trust for electronic banking, Technovation, 23(11):847–860.http://dx.doi.org/10.1016/S0166-4972(03)00130-5

[41] M. Akazue, I. Nonum, E. Omedeand A. Edje (2023), Application of A Multi-Layered Optimal Classifier for Telecommunication Fraud Prediction System, International Journal of Trend in Research and Development,10(4): 225-231

[42] A. A. Ojugo and E. Ekurume, (2021), "Deep learning network anomaly-based intrusion detection ensemble for predictive intelligence to curb malicious connections: An empirical evidence," International Journal of Advanced Trends in Computer Science and Engineering,10 (3) :2090–2102

[43] A. A. Ojugo and D. O. Otakore, (2020), Intelligent cluster connectionist recommender system using implicit graph friendship algorithm for social networks, Int. Journal of Artificial Intelligence, 9(3): 497~506

[44] A. A. Ojugo, M. I. Akazue, P.O. Ejeh, C. C. Odiakaose and F.U. Emordi, (May, 2023), DeGATraMoNN: Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing, KongzhiyuJuece/Control and Decision, 38 (01) ISSN: 1001-0920

[45] A. Rehab, B. Shiraz, S. Malik, K. Hayat, K. Aihab and K. Memoona, K. (2010). Online credit card fraud prevention system for developing countries, International Journal of Reviews in Computing, 62-70.

[46] M. I. Akazue, I. A. Debekeme, A. E. Edje, C. Asuai, U. J. Osame (2023). UNMASKING FRAUDSTERS: Ensemble Features Selection to Enhance Random Forest Fraud Detection. Journal of Computing Theories and Applications, 1(2): 201-11

[46] S. N. Okofu, (2018), Users Service Quality Trust Perception of Online Hotel Room Reservati, SAU Journal of Management and Social Sciences, 3(1 & 2): 1-14

[47] X. Ding, T. Wei, C. Cao, (2022), Towards a Four-Dimensional Dynamic Trust Model in B2C Cross-Border E-Commerce, Proceedings of the 2022 13th International Conference on E-Education, E-Business, E-Management, and E-Learning (IC4E '22),414-418. Retrieved from https://doi.org/10.1145/3514262.3514299.

[48] M. Akazue, A. Clive, A. Edje, E. Omede and E. Ufiofio, (July 2023), CYBERSHIELD: Harnessing ensemble feature selection technique for robust distributed denial of service attacks detection, KongzhiyuJuece/Control and Decision, 38 (03): 1211- 24