International Journal of Advanced Multidisciplinary Research
ISSN: 2393-8870
www.ijarm.com
(A Peer Reviewed, Referred, Indexed and Open Access Journal)
DOI: 10.22192/ijamr Volume 10, Issue 6 -2023

Research Article

DOI: http://dx.doi.org/10.22192/ijamr.2023.10.06.001

Neuro-fuzzy and Boosted Regression Ensemble Model for Estimation of M-Payment Systems Security

Mohammed Bulama [1]
Abubakar Tatari Ali Polytechnic, Department of Computer Science, Nigeria, Bauchi-State,
Jos Road 0094, Nigeria. E-mail: *mbgiade@gmail.com*

Dr. Yakubu Bala Mohammed [2*]
Abubakar Tatari Ali Polytechnic, Department of Computer Science, Nigeria, Bauchi-State,
Jos Road 0094, Nigeria. E-mail: *mohammedbala0079@gmail.com*

Mahmood Saidu Badara [3]
Abubakar Tatari Ali Polytechnic, Department of Computer Science, Nigeria, Bauchi-State,
Jos Road 0094, Nigeria. E-mail: *Mahmood_saidu@yahoo.com*

Keywords

Artificial intelligence, M-payment platforms, Security, Risk.

Abstract

Recent advancements in remote payment systems and internet innovation have begun to provide people with more interesting, flexible, and affordable services in the form of m-payment services, and the system (m-payment) is expected to have a sunnier future. However, security threats and other targeted attacks still remain an issue that affect the development of m-payment platforms not only in evolving digital markets but also in developed markets. Therefore, the main aim of this research is to inspect the effects of protection, risk, and targeted attacks on m-payment platforms continual usage using two different “artificial intelligence (AI) based techniques; “Boosted regression tree” (BRT) and “Adaptive neuro-fuzzy inference system” (ANFIS) for estimation of security effects on the m-payments. A total of 579 datasets were obtained and used in training and testing the study models. Findings of the study shows that all the models estimate the effects of security on m-payment with higher accuracy NSE > 0.97. Also, the results of the study indicate that security and risk were the main factors affecting m-payment platforms growth in the research area. Interestingly, the findings of the study will assist remote payment stakeholders in understanding issues affecting m-payment platforms.

1. Introduction

Global spread of internet technologies and proliferation of mobile devices such as iPhones, tablets, and smartphones has led to the emergence of awide-range of services, one of themost popular among them is “electronic commerce(e-commerce)” (Kim et al., 2010; Park et al., 2019). As m-commerce is gradually becoming popular and part of peoples live, mobile payment (m-payment) platforms such as; electronic banking (e-banking), mobile banking (m-banking), and other forms of internet banking will no definitely comfort virtual transactions amongst payment organizations and individuals(Agarwal et al., 2007; Cavus et al., 2021). Thus, for the purpose of this study, m-payment is defined as all kinds of payments made for the payments of purchased goods, and/or rendered services via mobile devices(Lee et al., 2016; Moghavvemi et al., 2021; Zhou et al., 2020).

A typical m-payment platforms comprises of at least five key actors; the “financial service provider” (FSP) that is responsible for the execution of the backend processing required for seamless transactions between the parties involved, the “payment service provider” (PSP) that facilitates communication between the payer/payee and the financial service provider by offering the user interfaces and the payment software, “mobile network operator” (MNO) that offers the necessary infrastructures needed for the wireless service, the “payer and payee” (PP) who makes and receive payments, and regulatory agencies (i.e., government bodies) who are responsible for monitoring all transactions in order to ensure compliance with the laid down rules and regulation that govern m-payments. (Agarwal et al., 2007; Kim et al., 2010).

In the past few years, the global financial sector had witnessed a tremendous growth, especially during the Covid-19 lockdown due to the restriction of movement imposed by majority of countries globally. Thus, forcing people to utilized the various m-payment platforms for their financial dealings as the system (m-payment system) allows individuals to send and received payments irrespective of time and place via the internet. However, despite these benefits and government insistence on a cashless society, security still remains an issue that negatively affects m-payment platforms, especially in developing nations (Cavus et al., 2021; Malaquias & Hwang, 2016)(Alkhowaiter, 2020; Kamdjoug et al., 2021). Therefore, the need to have a better understanding of the security issues involved in m-payment systems using different approaches such as artificial intelligence (AI) based techniques. Thus, the purpose of this present study is to examine the effects of security on m-payment platforms using two AI-based techniques; “Adaptive neuro-fuzzy inference system” (ANFIS), and “Boosted regression tree” (BRT) in order to obtained precise predictions. AI-based methods have “proven to have better performance due to their estimation ability compared to conventional models such as technology acceptance models (TAM)” (Nourani, 2017). The study presents an interesting result regarding the effects of security on m-payment systems in developing states, specifically Nigeria, and highlights the precision ability of AI methods above the conventional methods e.g., TAM usually employed by prior m-payment studies. The study results will assist various m-payment stakeholders in understanding the dimensions and complexity of the security issues involved in m-payment platforms so that better and secured m-payment services can be delivered to the customers.

2. Literature Review

In this section, innovations used in m-payment platforms, stages of m-payment, and security challenges were discussed.

2.1 Innovation used in m-payment systems

To conduct a thorough analysis of m-payment systems security, one must understand the necessary technologies used, procedures, standards, and platforms employed. The most popular standards employed in m-payment processes are; “Code Division Multiple Access” (CDMA), and “Global System for Mobile Communications” (GSM). For the CDMA process, the subscription keys are usually kept or stored in the device (i.e., mobile devices) itself, and “short messaging services” (SMS) is the most common innovation used in m-payment services. The service is considered to be an alternative to usual calls making due to its ease of usage and lowcost (Johnson et al., 2018). Furthermore, remote payments via SMS are of two kinds; i) payment that requires a “change in device infrastructure (SIM card) e.g., SMS-Credit, and ii) Payments that do not require any changes in the infrastructure e.g., PayPal” (Prakash, 2015). While in the second process (i.e., GSM), a “subscriber identification module” (SIM) card that contains owners’ subscription numbers is used to identify the real owner of the cardso that it allows the user to initiate, process, and approved various transactions(Guo & Bouwman, 2016).

2.2 M-payment security challenges

Affordance and expedient were the main differences between remote payments such as m-payment and traditional payment systems e.g., cheque and other physical payment methods. However, despite these benefits security threats remain the main factor affecting m-payment acceptance and general growth, especially in developing nations (Kasiyanto, 2016). Vulnerability of remote payment e.g., m-payment platforms depend on at least two important factors; the infrastructure that facilitates the payment (i.e., the GSM), and other employed technology (e.g., Bluetooth). However, prior m-payment studies often overlooked the security susceptibility involved in these fundamental innovations while examining m-payment security. Thus, to have a better understanding of the security challenges confronting m-payment platforms, a rounded view of the susceptibilities of each of the security dimensions instead of focusing on a single dimension e.g., m-payment platforms or certain procedures involved (Agarwal et al., 2007).

Cavus et al. (2021) in their study found security and confidentiality to be the main reason majority of customers decline to use m-payment systems in developing nations. The authors argued that “customers fears’ of transactions not reaching its destination, information and data theft, and financial loses” were the main factors affecting m-payment growth in Nigeria and other African nations. In another research conducted by Wong and Mo (2019) discovered “customers perceptions of remote payments security, risk, and trust were the main issues affecting customers intention to accept and use various m-payment platforms in Hong Kong. Thus, affecting the systems general growth in the country.

3. Methodology

The main purpose of this present study is to inspect the different dimensions and effects of security on m-payment platforms in the research area using two different AI approaches i.e., ANFIS and BRT.

3.1 Research design

The research data gathering tool involves four inputs (i.e., security, risk, secrecy, and attempted attacks), and one output i.e., m-payment platform usage. Section “A” contains the respondent’s personal information such as; age, academic qualification, gender, and security knowledge. While the “B” part contains opinions regarding security issues affecting m-payment platforms progress.

3.2 Method of analysis

Two methods of data examination were employed; “i.e., structural equation modelling, and AI-based approach”. Respondent personal data were analyzed using SPSS (i.e., “structural equation modelling”), while data regarding the security issues of m-payment were simulated using MATLAB 2023a (i.e., the AI-based approach) in order to get prediction regarding the effects of security on m-payment platforms in the study area.

3.3 AI-based techniques

AI based methods such as; “Artificial neural network” (ANN), “Boosted regression tree” (BRT), “Support vector regression” (SVR), “Adaptive neuro-fuzzy inference system” (ANFIS), and “Convolutional neural network” (CNN) have demonstrated to have a better prediction skill compared to classical approaches such as TAM and D&M methods(Nourani et al., 2020; Wang & Srinivasan, 2017). Therefore, this research hired 2 AI methods ANFIS and BRT to modelled the study data so that accurate and reliable results (prediction) can be obtained regarding the effects of security on m-payment platforms in the research area.

3.3.1 ANFIS

Studies have shown that ANFIS is considered as one of the techniques with higher precision skills due to its fuzzifying ability (Karaboga & Kaya, 2019; Rezakazemi et al., 2017). The approach has been “effectively and widely used in different domain such as engineering, computer science, economics, medical, and other business domains. Algorithm of the research propose ANFIS approach is presented in **Figure 1**, consisting of 5 layers; the implication layer, fuzzifying layer, normalizing layer, aggregation layer, and defuzzifying layer all which perform certain functions in training, validation, and testing of the study dataset as shown **Figure 1**.

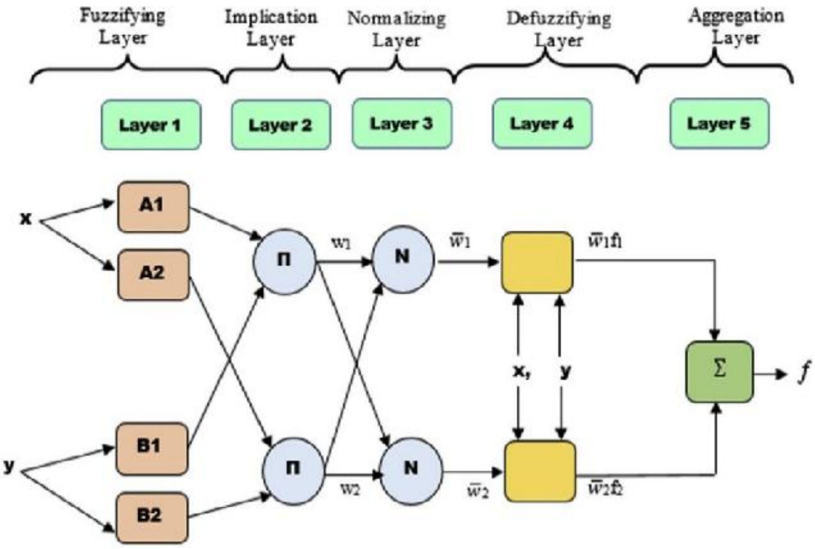

Figure 1. The Study Propose ANFIS Algorithm

3.3.2 BRT

Just like the ANFIS approach, the BRT method is one best AI techniques in terms of forecasting skills (Shaziayani et al., 2021). Thus, employed by this study to estimate the effects of security on m-payment platforms. The research propose BRT algorithm consists of 3 layers; i.e., input, normalization, and output layers as shown in **Figure 2**.

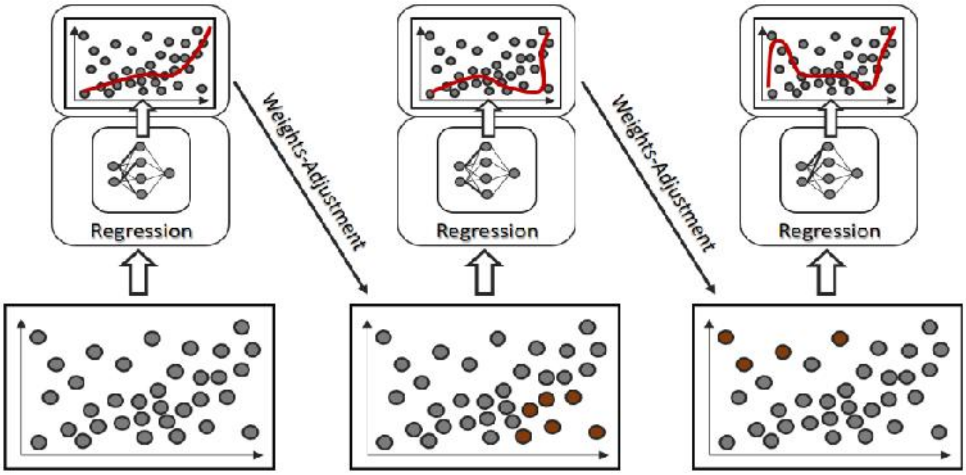

Fig. 2. Algorithm of the Study Propose BRT Approach

3.4 Evaluation and performance assessments criteria

There are different types of evaluation and performance assessment criteria. However, for the purpose of this study, the cross-validation method was used using 4 mathematical directories; “Nash-Sutcliffe efficiency (NSE), Mean absolute percentage error (MAPE), Root mean square error (RMSE), and Mean absolute error” (MAE). The 4 directories were explained using equations 1 – 4.

$$NSE = 1 - \frac{\sum_{i=1}^{n}\left(N_{obs_i} - N_{pre_i}\right)^2}{\sum_{i=1}^{n}\left(N_{obs_i} - \overline{N_{obs_i}}\right)^2} \tag{1}$$

$$\text{MAPE} = \frac{100\%}{n}\sum_{i=1}^{n}\frac{\left|N_{obs_i} - N_{pre_i}\right|}{N_{obs_i}} \tag{2}$$

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}\left(N_{obs_i} - N_{pre_i}\right)^2}{n}} \tag{3}$$

$$\text{MAE} = \frac{\sum_{i=1}^{n}\left|N_{obs_i} - N_{pre_i}\right|}{n} \tag{4}$$

The study proposed methodology is presented in **Figure 3** below.

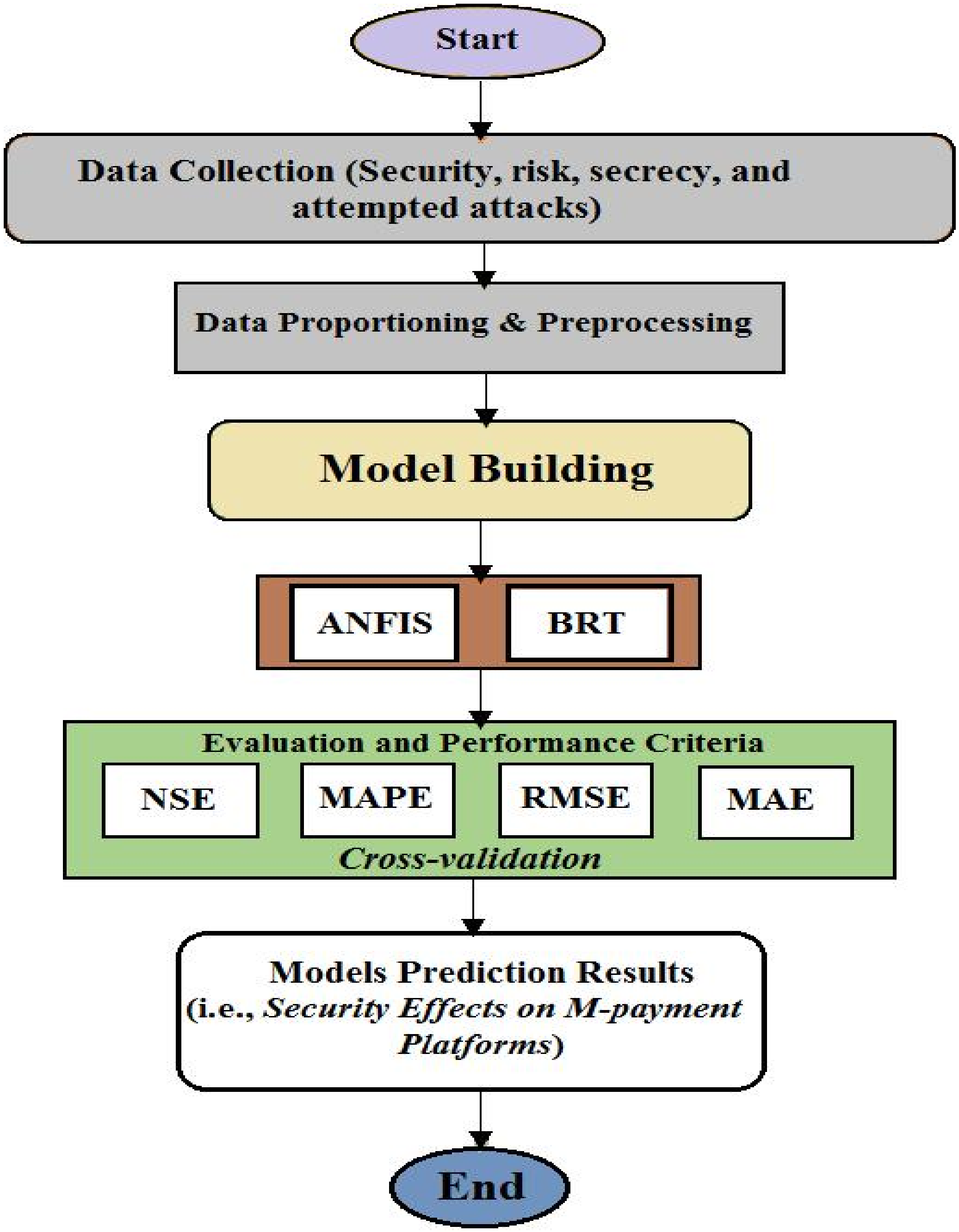
Start
Data Collection (Security, risk, secrecy, and attempted attacks)
Data Proportioning & Preprocessing
Model Building
ANFIS
BRT
Evaluation and Performance Criteria
NSE
MAPE
RMSE
MAE
Cross-validation
Models Prediction Results (i.e., Security Effects on M-payment Platforms)
End

Figure 3.Flow diagram of the study proposed AI-based methodology

4. Results and discussions

Results regarding the significance of each of the study inputs (sensitivity analysis results) on m-payment platforms, and models' estimation results were offered in the following subsections.

4.1. Parameters Sensitivity Results

In AI-based methods, choice and inclusion of relevant inputs is crucial as the inclusion of irrelevant parameters affects models concert vice versa. Therefore, the study inputs were ranked in order to determine the sensitivity of each on the study output i.e., m-payment platforms. Relevancy of each of the inputs was examined using equation 5 i.e., coefficient of determination (DC).

$$DC = 1 - \frac{\sum_{i=1}^{n}(N_{obsi} - Nprei)2}{\sum_{i=1}^{n}(N_{obsi} - N_{obsi})2} \quad (9).$$

Ns represent mean values for the inputs, n stands for the observations sum, and Nobs stands for the observed effects of the inputs, while Npre represents the estimated effects of the research inputs on the output.

Table 1: Inputs sensitivity results

Input parameters	DC values	Rank
Security	0.9761	1
Risk	0.9586	2
Attempted attacks	0.9188	3
Secrecy	0.9063	4

As shown in **Table 1**, clients concern for security and risk are the most significant factors affecting m-payment platforms in the research location as the two inputs have the uppermost DC values 0.9761 and 0.9586, thus ranked first and second. While attempted attacks and secrecy have lesser effects on the research output as they were ranked third and fourth with DC values of 0.9188 and 0.9063 respectively.

4.2. Models' prediction results

In this present research, two AI based approaches; ANFIS and BRT were used to modelled the effects of the research inputs on the study output i.e., m-payment platforms. Performance of the employed AI models (ANFIS and BRT) in both "training and testing were evaluated using cross-validation techniques" with 4arithmetic directories; MAE, NSE, RMSE, and MAPE. Results regarding the models' performance is presented in **Table 2**. The valuation metrics used involved "computing the fitness level and prediction error of the models as both are crucial in evaluating models' effectiveness". As shown in **Table 2**, both models performed well. However, the ANFIS model surpass the BRT model in both testing and training phases as the model has an NSE value of 0.9786 and 0.9681 in testing and training respectively signifying the model prediction skills. Also, suitability of the models regarding estimation accuracy was further examined using "scatter plots" as shown in **Figure 4 (**i.e., testing phase). ANFIS has a better fitness level compared to BRT as the models' experimental data are closer to the "bisector diagonal" than the other models (ANFIS and BRT). The models' performance results in offered in **Table 2**.

Table 2: AI models performance metrics

TRAINING					**TESTING**			
MODELS					**NSE**	**RMSE**	**MAE**	**MAPE**
	NSE	**RMSE**	**MAE**	**MAPE**				
ANFIS								
	0.9681	0.0836	0.0536	13.0162	0.9786	0.0432	0.0320	11.0321
BRT								
	0.9326	0.0811	0.0299	16.2332	0.9399	0.0634	0.0636	13.0897

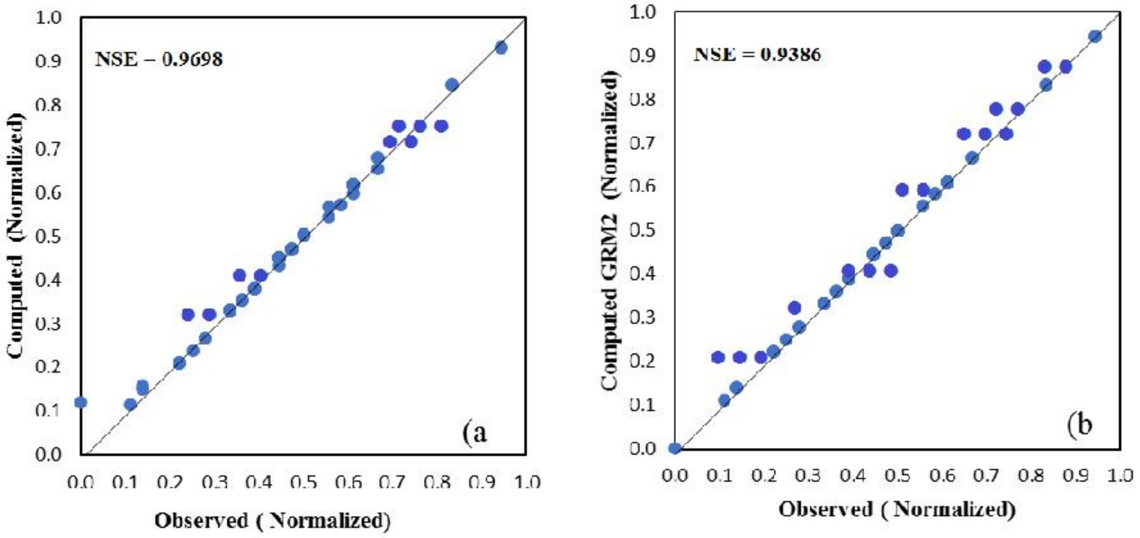

Figure 4: Testing scatter plots between computed and observed inputs effects on m-payment platforms by a) ANFIS, and b) BRT.

Based on the models' estimation results, security and risk were the two most significant factors affecting m-payment development in the research area followed by attempted attacks and secrecy. As seen in **Table 2** and **Figure 4**,the predictions made by all the models clearly shows that customers fear of security breach and risk associated with remote payments were the key issues affecting "m-payment systems adoption and continual usage" in Nigeria. The finding is supported by the result of Moghavvemi et al. (2021) who argued that "security and risk are the most likely factors affecting m-payment systems advancement not only in developing states but also in developed nations, thus signifying the correlation between the factors and m-payment platforms". For attempted and secrecy, the results shows that the factors came second and third in terms of effects on the study output indicating that secrecy and attempted attacks have lesser effects compared to the first two variables i.e., "security and risk". This result is strengthened by the findings of Zhou et al. (2021) and Rahman et al. (2021) who stressed that "secrecy and number of attempted attacks against persons account may likely have adverse effects on all forms of remote payment systems" usage. Thus, the need for stakeholders to do more in the areas of safety, secrecy, and risk.

5. Conclusion

In this study, two AI models i.e., BRT, and ANFIS were used to simulate and modelled the effects of security on m-payment platforms advancement in the research area (Nigeria). findings of the study shows that both models performed well in both testing and training, and forecast the effects of security on m-payment platforms with higher precisions as both models have an NSE values > .93 which indicates a strong relationship between the output and input variables. Also, the study sensitivity results found all the inputs to have significant effects on the study output as they all have DC values < 0.8 signifying the inputs relevance with regard to m-payment usage in the study area. Furthermore, the study results highlight the estimation ability of "AI-based techniques" compared to other conventional methods such as "TAM and D&M methods". Although, all the proposed AI models estimated the effects of security with higher accuracy, but the research is limited to the data collected and used, the area where the study is conducted, and the method hired. Therefore, impending studies should use a combination of classical approaches and other AI techniques e.g., CNN and GBDTto further inspect the effects of security on "m-payment platforms" in both advanced and developing nations.

References

Agarwal, S., Khapra, M., Menezes, B., & Uchat, N. (2007). Security issues in mobile payment systems. *Proceedings of ICEG*, 142-152.

Alkhowaiter, W. A. (2020). Digital payment and banking adoption research in Gulf countries: A systematic literature review. *International Journal of Information Management*, *53*, 102102.

Cavus, N., Mohammed, Y. B., & Yakubu, M. N. (2021). An Artificial Intelligence-Based Model for Prediction of Parameters Affecting Sustainable Growth of Mobile Banking Apps. *Sustainability, 13*(11), 6206.

Guo, J., & Bouwman, H. (2016). An analytical framework for an m-payment ecosystem: A merchants′ perspective. *Telecommunications Policy, 40*(2-3), 147-167.

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Computers in human behavior*, *79*, 111-122.

Kamdjoug, J. R. K., Wamba-Taguimdje, S.-L., Wamba, S. F., & Kake, I. B. e. (2021). Determining factors and impacts of the intention to adopt mobile banking app in Cameroon: Case of SARA by afriland First Bank. *Journal of Retailing and Consumer Services*, *61*, 102509.

Karaboga, D., & Kaya, E. (2019). Adaptive network based fuzzy inference system (ANFIS) training approaches: a comprehensive survey. *Artificial Intelligence Review*, *52*, 2263-2293.

Kasiyanto, S. (2016). Security issues of new innovative payments and their regulatory challenges. *Bitcoin and Mobile Payments: Constructing a European Union Framework*, 145-179.

Kim, C., Mirusmonov, M., & Lee, I. (2010). An empirical examination of factors influencing the intention to use mobile payment. *Computers in human behavior, 26*(3), 310-322.

Lee, S.-J., Rho, M. J., Yook, I. H., Park, S.-H., Jang, K.-S., Park, B.-J., Lee, O., Lee, D. K., Kim, D.-J., & Choi, I. Y. (2016). Design, development and implementation of a smartphone overdependence management system for the self-control of smart devices. *Applied Sciences*, *6*(12), 440.

Malaquias, R. F., & Hwang, Y. (2016). An empirical study on trust in mobile banking: A developing country perspective. *Computers in human behavior*, *54*, 453-461.

Moghavvemi, S., Mei, T. X., Phoong, S. W., & Phoong, S. Y. (2021). Drivers and barriers of mobile payment adoption: Malaysian merchants' perspective. *Journal of Retailing and Consumer Services, 59*, 102364.

Nourani, V. (2017). An emotional ANN (EANN) approach to modeling rainfall-runoff process. *Journal of hydrology, 544*, 267-277.

Nourani, V., Gökçekuş, H., & Umar, I. K. (2020). Artificial intelligence based ensemble model for prediction of vehicular traffic noise. *Environmental research, 180*, 108852.

Park, J., Amendah, E., Lee, Y., & Hyun, H. (2019). M-payment service: Interplay of perceived risk, benefit, and trust in service adoption. *Human Factors and Ergonomics in Manufacturing & Service Industries*, *29*(1), 31-43.

Prakash, K. (2015). Security issues and challenges in mobile Computing and m-commerce. *International Journal of Computer Science and Engineering Survey*, *6*(2), 29.

Rahman, T., Noh, M., Kim, Y. S., & Lee, C. K. (2021). Effect of word of mouth on m-payment service adoption: a developing country case study. *Information Development*, 0266666921999702.

Rezakazemi, M., Dashti, A., Asghari, M., & Shirazian, S. (2017). H2-selective mixed matrix membranes modeling using

ANFIS, PSO-ANFIS, GA-ANFIS. *International Journal of Hydrogen Energy*, *42*(22), 15211-15225.

Shaziayani, W. N., Ul-Saufie, A. Z., Ahmat, H., & Al-Jumeily, D. (2021). Coupling of quantile regression into boosted regression trees (BRT) technique in forecasting emission model of PM10 concentration. *Air Quality, Atmosphere & Health*, *14*(10), 1647-1663.

Wang, Z., & Srinivasan, R. S. (2017). A review of artificial intelligence based building energy use prediction: Contrasting the capabilities of single and ensemble prediction models. *Renewable and Sustainable Energy Reviews*, *75*, 796-808.

Wong, W. H., & Mo, W. Y. (2019). A study of consumer intention of mobile payment in Hong Kong, based on perceived risk, perceived trust, perceived security and Technological Acceptance Model. *Journal of Advanced Management Science Vol*, *7*(2), 33-38.

Zhou, L., Gozgor, G., Huang, M., & Lau, M. C. K. (2020). The impact of geopolitical risks on financial development: evidence from emerging markets. *Journal of Competitiveness*, *12*(1), 93.

Zhou, Q., Lim, F. J., Yu, H., Xu, G., Ren, X., Liu, D., Wang, X., Mai, X., & Xu, H. (2021). A study on factors affecting service quality and loyalty intention in mobile banking. *Journal of Retailing and Consumer Services*, *60*, 102424.

Access this Article in Online	
Quick Response Code	Website: www.ijarm.com
	Subject: Information Technology
DOI:10.22192/ijamr.2023.10.06.001	

How to cite this article:
Mohammed Bulama, Yakubu Bala Mohammed, Mahmood Saidu Badara. (2023). Neuro-fuzzy and Boosted Regression Ensemble Model for Estimation of M-Payment Systems Security. Int. J. Adv. Multidiscip. Res. 10(6): 1-10.
DOI: http://dx.doi.org/10.22192/ijamr.2023.10.06.001