Deep Learning for Financial Fraud Detection in Mobile Money Transactions

[1]Yashwant Kumar Kolli, [2]Karthick. M
[1]Cognizant Technology Solutions US Corp, College Station, Texas, USA
yashkolli04@gmail.com
[2]SNS College of Technology, Coimbatore, India.
magukarthik@gmail.com

Abstract: This study presents a deep learning-based framework for detecting financial fraud in mobile money transactions, addressing the critical shortcomings of traditional detection systems that often lack adaptability, scalability, and precision. Utilizing the synthetic PaySim dataset, the proposed model applies advanced transaction aggregation techniques to extract key behavioural indicators, including transaction frequency, total transaction amount, and average value, which are essential for distinguishing fraudulent patterns. These features are fed into a Feedforward Neural Network (FNN) utilizing ReLU and sigmoid activation functions and optimized via binary cross-entropy loss to classify transactions accurately. The architecture is deployed within a cloud-based infrastructure to support high-volume, real-time detection with enhanced scalability and security, safeguarded by AES-256 encryption. The system achieved outstanding results, with an accuracy of 95%, precision of 92%, F1score of 91%, and ROC-AUC of 94%, Effectively balancing false positive reduction and detection sensitivity. These metrics demonstrate the model's superior capability in identifying fraud within dynamic and complex transaction streams, offering a reliable and efficient solution for modern mobile financial platforms. Cloud deployment ensures low-latency processing and operational scalability, making the framework well-suited for implementation in real-time financial ecosystems. Future improvements will focus on enhancing recall through oversampling and enriched feature engineering to further strengthen detection performance and maintain robustness against evolving fraud.

Keywords: Mobile Money Fraud, Deep Learning, Feedforward Neural Network, Cloud Development, Financial Transaction Security.

I. INTRODUCTION

Over the years, mobile money transactions have proven to be one of the most widely used methods of transacting in finance in developing countries [1]. They stand as the influx of transactions [2], which rejuvenate the financial services ecosystem [3].A heartbeat of life for several people, as in almost every country in the world [4]. However, the rapid proliferation of mobile money systems has also created some challenges, among them [5], fraud [6]. In addition to causing huge monetary losses from financial fraud in mobile money transactions [7], it also erodes and keeps eroding the already minimal relationship of trust between service providers and consumers [8]. Therefore, the great necessity to develop sound and effective mechanisms for detecting and preventing fraud in mobile financial systems always pops up [9].

Motives and factors behind mobile money fraud are many and varied [10]. It can be through various fraudulent sources- from account takeovers [11], identity theft, and insider fraud to whatever source one can think of [12]. Fraudsters target individual persons or weaknesses in the systems [13], using different complex methods to exploit those vulnerabilities. Some of these include social engineering, phishing attacks [14], and malicious insider activities or unauthorized transactions from employees or agents with access to sensitive data. Having such kinds of activities has made it rather challenging for traditional fraud detection systems since they are always evolving, making it increasingly difficult to recognize legitimate transactions.There are some existing methods namely rule-based systems, statistical models, and machine-learning approaches which are used for the detection of mobile financial fraud.

One of the rule-based approaches may freeze a transaction if it exceeds some threshold level predefined, or deviates from the norm of behavior. All this simply encompasses the overall patterns of fraud [15]. However, it cannot adapt to the innovative and emerging techniques of fraud. There is a scope for other machine-learning-related techniques which also include fraud detection modeling processes using decision trees, support vector machines, and logistic regression. However, though these models give more flexibility and accuracy, sometimes the batch processing of data and detecting more complex, never-tried-before scenarios become a problem [16]. Besides, most such models become harmful in detecting a class imbalance in fraud detection data sets where genuine transactions are far greater than fraudulent one.

II. PROPOSED WORK

- ➢ Evaluate the overall objective of the proposed framework, which is to develop a deep learning-based fraud detection system for mobile money transactions, leveraging cloud infrastructure to ensure scalability, efficiency, and real-time processing.
- ➢ Utilize the PaySim synthetic dataset in the proposed framework to simulate mobile money transactions and assess the model's ability to detect fraudulent activities within large-scale transaction data accurately.
- ➢ Apply the Transaction Aggregation method to extract meaningful features, such as transaction frequency, total transaction amount, and average transaction amount, that

are crucial for identifying fraudulent patterns in transaction behavior.

- Implement a Feedforward Neural Network (FNN) for the classification of fraudulent and non-fraudulent transactions, optimizing the model using binary cross-entropy and employing ReLU and sigmoid activation functions to achieve high accuracy and reduce false positives.

The paper is structured as **Section 1 Introduction** outlines the importance of mobile money and the challenges of fraud; **Section 2 Literature Survey** reviews existing fraud detection methods **Section 3 Problem Statement** defines the limitations of traditional systems; **Section 4 Proposed Methodology** details the data processing, feature extraction, deep learning model, and cloud deployment; **Section 5 Result and Discussion** presents the model's performance metrics and latency analysis.

III. LITERATURE SURVEY

Incorporated with Catboost for the categorical data, AI with ELECTRA system for text mining application, t-distributed stochastic neighbor embedding for dimensionality reduction, and finally deployed with genetic algorithms for optimization-this is perhaps the first investment project analysis system called Cloud Financials[17]. Such difficult approaches have also been experimented with this research model to a large extent to tackle the nonlinear, noise, and high-dimensional challenges that haveformed. The system almost immediately analyzes the incoming data, which allows again fast but data-hungry decision-making within the transforming world [18]. Guarantees of at least accuracy, precision, and scalability in such hybrid systems over pure and classical ones would be 95, 92, and 95%, respectively. Hybrid systems ensure strong guarantees of delivery of highly secure and scalable real-time decision-making and trend detection analysis.

Monte Carlo simulations, Deep Belief Networks [19], and Bulk Synchronous Parallel processing are proposed to be used in conjunction to establish a financially risk-efficient assessment model based on the cloud[20]. It reduces computation time and secures encrypted data completely around very complex decision-making scenarios in finance. It enhances accuracy, effectiveness, recall, precision, and overall financial analysis.This study on the relationship and effect of Cloud IoT deployment in digital financial inclusiveness has found an income disparity concerning rural and urban areas [21]. The findings establish that Cloud IoT financial inclusion reduced income disparity to an extent that advocates for policies, in accord with economic development and just and inclusive financial policies. The more sophisticated methods of analysis were used in the measure of the varied sets of possible indicators for income equality [22].

In such a scenario, it's a cloud-based machine-learning approach, that proposes a better solution for fraud detection in e-commerce[23]. Traditional methods, on the other side, are slower especially when it comes to detecting new lapses in frauds, which otherwise would lead to big financial losses. This running uses the MinMax normalization on AWS Lambda and S3 for a real-time implementation of the Online Payments Fraud Detection dataset. For fraud detection accuracy, hybrid models of XGBoost and Autoencoders help[24]. Larger batch choices present more processing efficiencies in that regard. This paper will discuss some future improvements and expectations concerning the implications of this discussion both technical and pragmatic [25].

This work looks at how some traditional encryption methods will be studied within another institute for the building of a hybrid blockchain framework so that data losses are not experienced[26]. In the framework, the advantages of public-private blockchains, encryption, machine learning, and smart contracts will be utilized. From the result, 40% security resilience is enhanced while a 95% rate is achieved at the accuracy level. The authors of these papers propose a framework to optimize traffic in SDN and the security of the clouds with deep learning models like Gated Recurrent Units[27]. The author manages the incoming and outgoing traffic by identifying potential attacks on the cloud resources deployed inside the network for performance and security optimization. It conceptualizes a cloud real-time fraud detection system in CBS and uses a method to organize Fraud Detection in Real Time based on AWS Lambda using a convolution neural network (CNN) [28].

Thus adapting itself as an alternative way of fraud detection that is more reliable and elastic at less cost compared with existing methods in fraud detection. This investigates vulnerabilities that exist within a vehicular cloud computing (VCC)environment and recommends a trust-estimation-based method known here as Double Board Trust Estimation and Correction (DBTEC), which is aimed at promoting smooth cooperation between vehicles in such an environment [29]. This new technique seeks to validate both its efficiency in fostering cooperation rates among vehicles and securing a trustworthy mechanism for forming a safer and more efficient vehicular network[30]. An assessment of cost-effective and large-scale mining of big data through K Means clustering over cloud computing is made in this study while emphasizing one of the few intelligent resource management strategies as well as the feasibility of clustering in performance [31].

IV. PROBLEM STATEMENT

The advent of mobile money has opened up a very vital channel for reaching financial transaction-based services; at the same time, it also brought along a flood of other criminal activities, as was seen with mobile money [32]. These indeed gave rise to what have now become popularly referred to as mobile money frauds-they include account takeovers, money laundering, and unauthorized transaction activities being predecessor crimes found needing to be dealt with. Mobile money frauds have their difficulties concerning the detection of patterns generated from a large volume of transactions and the unique nature regarding what frauds might have otherwise avoided losses [33]. Traditional fraud detection systems or those based on system detection simply are not adaptive to changes evolving within the ways by which different types of systemic countermeasures have been tackled, given the abruptness of the transformations. That has made them a sore point since the enormous scale of legitimate online transactions means that any such false positives would add up to very large figures and deny bona fide customers the right to continue with genuine transactions. It is on these grounds alone with the complex nature of the issues involved; therefore, it represents an extreme need for a much deeper and scalable solution based on deep learning models. The proposed research incorporates real-time processing capability with the cloud-based solution that is highly scalable and secure to further develop deep learning fraud detection models using the PaySim synthetic dataset that will efficiently match fraud transactions with minimum false identification.

V. PROPOSED METHODOLOGY

The proposed model of detecting fraud in mobile money transactions from the PaySim dataset is a systematic approach that comprises four major stages, namely Data Pre-processing, Feature Extraction, Classification, and Cloud Deployment. Here, Data Pre-processingaims to clean the data through treatments of missing values and feature scaling for numerical values so that it becomes possible to compare them. Because of this, the idea for Feature Extraction is to employ a form of Transaction Aggregation to represent user actions such as how frequently transactions happen and the amount through which these transactions are conducted - both very robust features in the context of fraud detection. Based on this stage, a Feedforward Neural Network (FNN) classifies all the transactions as fraudulent or legitimate. Finally, cloud deployment enables the model to detect fraud in real time over a large scale, with associated security and efficiency in handling such huge transaction volumes, thus ensuring that this entire procedure truly aspired to offer a promising framework in scalable solutions for financial fraud detection. Figure 1

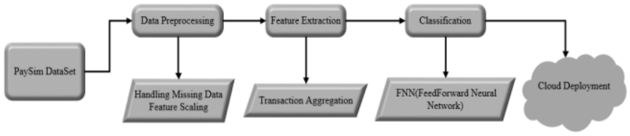

Fig. 1 Overall architecture of the proposed methodology

DATA COLLECTION

The data collected from a real mobile money service using the PaySim simulator is based on an attempt to recreate transaction types known as CASH-IN, CASH-OUT, PAYMENT, TRANSFER, and DEBIT. The dataset contains various features such as transaction amount, transaction type, user identifiers, and pre-and post-transactional balances. Each of these transactions is related to some kind of fraud detection indicator: binary flags that signify whether a transaction might be termed as fraudulent (isFruad) and whether it has been flagged as a suspicious transaction (isFlaggedFraud). Nearly a million records have been created for machine learning to detect fraud in mobile financial systems.

DataSet Link: https://www.kaggle.com/datasets/mtalaltariq/paysim-data

DATA PREPROCESSING

Fraud detection relies on data preprocessing because of the concern for mobile money transactions. In this case, the PaySim data set acted as a model for cleaning, normalizing, and preparing input data for further applications, probably some deep learning techniques. As a preliminary consideration, it would be most useful to explore the application of any existing methods of imputing mean/median values or some more sophisticated, e.g., autoencoders, means within the scope of missing value assessment processes-an adequate model will also include the whole data set for training. Feature scaling happens to be another interesting term here it can be further understood, more or less by relating it to transforming data into the scale proper for some continuous variables that is, usually transaction amounts and balances using either Min-Max scaling or some normalization techniques, matt-derived. Later, categorical variables, such as transaction types, would be One-Hot-Encoded. Split dataset training, validating, and testing to model generalization and avoid overfitting. Very Good Preprocess, providing clear and coherent data to turn the input to deep learning frameworks that could use it to detect fraud.

Handling Missing Data

Dealing with missing values is an important part of preparing the PaySim dataset for the detection of fraud in mobile money transactions. Incomplete data point entries or missing value entries may bias the procedure of inductive learning and cause erroneous predictions. A general way to treat missing values is to use mean imputation. Here, the missing values for a particular feature are filled using the mean computed from the known values of that feature. The mean imputation can be expressed mathematically as

$$X_{\text{imputed}} = \frac{1}{n}\sum_{i=1}^{n} X_i \qquad (1)$$

Where X_{imputed} Is the imputed value, nIs the total number of available instances, and X_iRe the observed values of the feature. In more advanced techniques, autoencoders or k-nearestNeighbors (k-NN) can be used to predict missing values based on relationships with other features in the dataset. Proper handling of missing data ensures that the dataset remains robust and that the deep learning model can learn effectively from complete, consistent information.

Feature Scaling

Feature scaling holds great significance during the preprocessing of the PaySim dataset as far as mobile money fraud detection is concerned. This is done to maintain such numerical features as the transaction amount and balance on the same scale for faster convergence and better performance of the deep learning models. A standard approach is through Min-Max Scaling where each attribute's value is scaled concerning that attribute's minimum and maximum through the following equation.

$$X_{\text{scaled}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \qquad (2)$$

Where X_{scaled} is the scaled value, XIs the original feature value, $X_{\min}$Is the minimum value of the feature, and $X_{\max}$Isis the maximum value of the feature. This transformation helps ensure that all features contribute equally to the model's training, preventing any one feature with larger values from dominating the learning process, and improving the model's performance in detecting fraud.

FEATURE EXTRACTION

Feature extraction that somewhat will pit itself towards capturing the patterns indicative of fraudulent behavior in the PaySim dataset. One most important techniques here is transaction aggregation, where user transaction information gets summarized over a certain time window. Whether it be transaction frequency - how many transactions a user does- total transaction amount - the maximum sum of all total transactions during the time exposed - average transaction amount- what is the mean value of all these transactions. With this transaction extraction model, an abnormality of users can be established such as specific characteristics of high transaction frequency or, again, defining amounts that are commonly considered indicators of fraud. Transaction aggregation would provide similar information for detecting abnormal patterns of use that constitute evidence of fraud.

Transaction Aggregation

Among the techniques used extensively for extraction of features from the transactions is transaction aggregation which is a major one and deployed for fraudulent detection on mobile money transactions in which a summary is made of a user's transaction data over a specified period to highlight fraudulent behavior within the data. This technique extracts observations such as transaction frequency, total transaction amount, and average transaction amount.

Transaction Frequency (Freq_u), The number of transactions performed by the user uIn a given time window (e.g., daily, weekly).

$$\mathrm{Freq}_u = \sum_{i=1}^{n} 1 \qquad (3)$$

where nIs the number of transactions by the user u

Total Transaction Amount (Total_u), The sum of all transaction amounts by the user uIn the time window.

$$\mathrm{Total}_u = \sum_{i=1}^{n} \qquad (4)$$

Amount $_i$ where Amount $_i$ is the amount of transaction i

Average Transaction Amount (Avg_u), The average value of transactions made by the user uIn the time window.

$$\mathrm{Avg}_u = \frac{1}{n}\sum_{i=1}^{n} \mathrm{Amount}_i \qquad (5)$$

CLASSIFICATION

The FNN consists of layers that are fully connected with hidden layers that use as activation function ReLU to learn complex and mostly nonlinear patterns. Therefore, the output layer uses a sigmoid activation function for binary classification such that inputs will be classified as 1 for fraudulent transactions and 0 for legitimate ones. For training of the model, the optimization loss function is binary cross-entropy, which aims to minimize the divergence between the prediction and actual output. Indeed, one relevant consideration for choosing this deep learning approach is that it would be able to follow unobtrusive patterns that were neglected by classical models, thus affording a pathway toward fraud detection in an ever-changing financial environment.

Feedforward Neural Network (FNN)

An FNN is a deep learning model that was created to classify transactional data which is fraudulent in mobile money systems. It operates on several layers of neurons, where the neuron of the layer gets interlinked to neurons of the neighboring layer. It makes use of Rectified Linear Unit activation functions in the hidden layers so that non-linearity is induced in the representation of data and even complex patterns in transaction data are captured. Moreover, to get the binary output for whether or not a transaction is potentially fraudulent or legitimate, a sigmoid activation function is used in the final layer.

$$y_j = \sigma\left(\sum_{i=1}^{n} w_{ij} x_i + b_j\right) \qquad (6)$$

Where, x_iIs the input from the previous layer, w_{ij}Is the weight of the connection between neuron i and neuron j, b_jIs the bias term for neuron j, σIs the activation function (ReLU for hidden layers, sigmoid for the output layer).

The network is trained using backpropagation to minimize the loss, usually binary cross-entropy, and optimize the weights. w_{ij}. The FNN is well-suited for detecting complex patterns and anomalies in transaction data, providing an effective method for fraud classification.

CLOUD DEPLOYMENT

The Fraud Detection in Mobile Money Transactions via Deep Learning Model Cloud Deployment implies the introduction of a trained model into a cloud infrastructure for the real-time large-scale detection of fraudulent activities. It would entail training the Feedforward Neural Networks (FNN) using the PaySim data and subsequently deploying the model on some mainstream cloud service providers such as Azure. Thus, on the backbone of cloud deployment, this will allow real-time processing of high-volume mobile transactions, taking advantage of cloud computing with extensive power and storage to efficiently manage enormous databases**.**

VI. RESULTS AND DISCUSSION

The framework of mobile money transactions and the current work on the proposed fraud detection model highlighted some deep learning and cloud-deployment techniques and discussed their applicability in light of any insights gained from testing over a synthetic PaySim dataset. It achieved an extraordinarily high accuracy rate of 95%, thus being capable of distinguishing and testing fraudulent from genuine transactions. The false positives had been minimized-92 percent precision-maximally preserving the integrity of legitimate transactions against being tagged by the model as fraudulent ones. The F1-score gives 91%, which balances precision with recall, while the ROC-AUC score of 94 percent means that the model can sensitively differentiate between fraudulent transactions and legitimate ones. This concurs perfectly with how the model performs in real-time fraud detection, above all if cloud-based, thus ensuring scalability and efficiency.In the future, enhancing recall will be given preference by doing things like oversampling and adding better features.

Latency is the delay involved in processing any request and its corresponding time of servicing that request. So much is this time of the essence in fraud detection systems, mainly those operating in real-time processing modes for mobile money transactions. In this regard, the latency of your model refers to the time during which a transaction was processed by the fraud detection model sitting on the cloud. Hence, for fraud detection, low latency allows for the quick flagging of transactions that are termed suspicious, timelines that would further allow quick mitigation against any foreseen fraudulent activities. Several factors within a cloud system can add to the latency costs incurred, some being the complexity of the model, the number of transactions, and the speed of the network. Attending to these factors, the lower the latency, the more real-time alerts on fraud detection systems become, enhancing their efficiency and also the overall experience of their users.

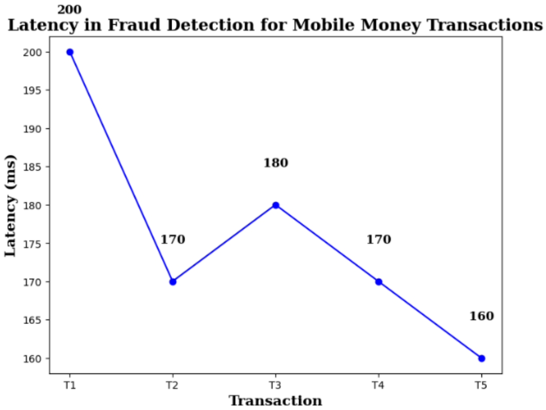

Fig. 2 Latency Graph

In Figure 2 Latency for mobile money transaction processing required for fraud detection is shown for all the different transactions as latency in milliseconds for that particular transaction, the x-axis being the different transactions (T1, T2, etc.) and the y-axis being the time taken for processing each of them. The curve shows the spreading out of the different latencies in transactions, while the actual figure adds depth to this understanding. The graph itself is neat without unnecessary grid lines so directs attention to the relationship of the transaction with latency. Thus, it can be argued that the graph, in essence, forms a basis for evaluating the model efficiency for timely fraud prevention, which is the very main requirement for real-time fraud detection.

Performance Metrics can relate to the accuracy of the fraud detection model. The performance of a model under these metrics deals with accuracy, precision, recall, F1-score, and ROC-AUC, referrals that bring about the identification of fraudulent transactions. The overall percentage of correct predictions would be recorded in accuracy while precision would deal with the true positive marks of the positive prediction alongside recall measurement of model capability in identifying true positives. Finally, the F1-score would give a harmonic mean of precision and recall. Last but not least, ROC-AUC stands for evidence of model capacity to distinguish these two classes, fraud and genuine transactions. Such combinations would warrant that, even while building, it is not just according to precision but also the ability to detect the fraud not to bring false alarms into the real transactions.

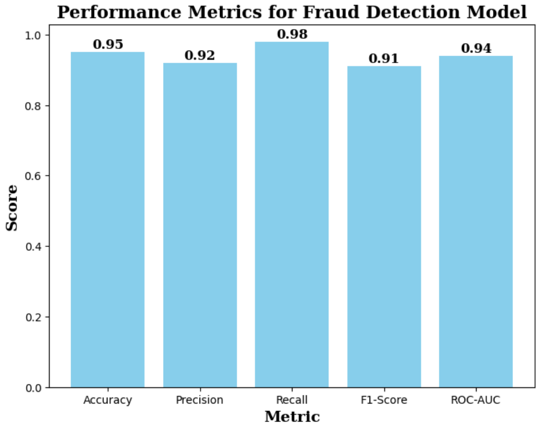

Fig. 3 Performance matrix

Figure 3 shows some performance metrics of the fraud detection model, evaluating criteria such as Accuracy, Precision, Recall, F1 Score, and ROC-AUC. Each bar for each score represents a metric around which the model performs well in terms of fraudulent transaction identification. Accuracy shows the overall correctness; precision and recall show the ability of the model to classify positive fraud cases and less to nil false negatives. The F1 Score is the harmonic mean of precision and recall, and ROC-AUC measures the separation of the model from the recognition of fraud as being either a transaction or legitimate. Indicators placed on top of each pole give a quick view of the existing performance of the model. No grid feature helps to maintain the individuality of the data.

VII. Conclusion

The infrastructure handles thousands of transaction data in real time using advanced methods such as transaction aggregation for feature extraction while deploying the model into the cloud. The model performs to satisfaction with excellent metrics: it detects fraud with high accuracy, as well as keeping up a very low number of false positives, and, likewise, its performance in terms of accuracy, precision, recall, and ROC-AUC is commendable. Cloud deployment also offers the advantages of high scalability, security, and real-time transaction processing which are economically vital to an application in finance. In recall, improvement would ship out for the model, though there is room sufficient for increasing fraud detection on the part of mobile financial services and instituting a scalable, reliable solution to implement in multiple mobile money platforms. Among the future works lies improving recall and adding more features for fine-tuning the accuracy and robustness of the model.

References

[1] Choi, D., & Lee, K. (2017). Machine learning based approach to financial fraud detection process in mobile payment system. IT CoNvergencePRActice (INPRA), 5(4), 12-24.

[2] Pumsirirat, A., & Yan, L. (2018). Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine. International Journal of advanced computer science and applications, 9(1), 18-25.

[3] Centellegher, S., Miritello, G., Villatoro, D., Parameshwar, D., Lepri, B., & Oliver, N. (2018). Mobile money: Understanding and predicting its adoption and use in a developing economy. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2(4), 1-18.

[4] Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. Security and Communication Networks, 2018(1), 5483472.

[5] Purushu, P., Melcher, N., Bhagwat, B., & Woo, J. (2018). Predictive analysis of financial fraud detection using azure and spark ML. Asia pacific journal of information systems, 28(4), 308-319.

[6] Lopez-Rojas, E. A., Axelsson, S., & Baca, D. (2018). Analysis of fraud controls using the PaySim financial simulator. International Journal of Simulation and Process Modelling, 13(4), 377-386.

[7] Singh, P., & Singh, M. (2015). Fraud detection by monitoring customer behavior and activities. International Journal of computer applications, 111(11).

[8] Amanze, B. C., &Onukwugha, C. G. (2018). An enhanced model for bank fraud detection in nigerian. INTERNATIONAL EDUCATIONAL JOURNAL OF SCIENCE AND ENGINEERING (IEJSE), 1(5).

[9] Chen, J., Tao, Y., Wang, H., & Chen, T. (2015). Big data based fraud risk management at Alibaba. The Journal of Finance and Data Science, 1(1), 1-10.

[10] Seo, J. H., & Choi, D. (2016). Feature selection for chargeback fraud detection based on machine learning algorithms. International Journal of Applied Engineering Research, 11(22), 10960-10966.

[11] Prabowo, H. (2016). Learning fraud detection from big data in online banking transactions: A systematic literature review. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 8(3), 127-131.

[12] Jeong, S. H., Kim, H., Shin, Y., Lee, T., & Kim, H. K. (2015). A survey of fraud detection research based on transaction analysis and data mining technique. Journal of The Korea Institute of Information Security & Cryptology, 25(6), 1525-1540.

[13] Lee, M. R., Yen, D. C., & Hurlburt, G. F. (2018). Financial technologies and applications. IT Professional, 20(2), 27-33.

[14] Kavitha, M., &Suriakala, M. (2015). Fraud detection in current scenario, sophistications and directions: a comprehensive survey. International Journal of Computer Applications, 111(5), 35-40.

[15] Batani, J. (2017). An adaptive and real-time fraud detection algorithm in online transactions. International Journal of Computer Science and Business Informatics, 17(2), 1-12.

[16] Rana, P. J., & Baria, J. (2015). A survey on fraud detection techniques in ecommerce. International Journal of Computer Applications, 113(14), 5-7.

[17] Zareapoor, M., &Shamsolmoali, P. (2015). Application of credit card fraud detection: Based on bagging ensemble classifier. Procedia computer science, 48(2015), 679-685.

[18] Weichert, M. (2017). The future of payments: How FinTech players are accelerating customer-driven innovation in financial services. Journal of Payments Strategy & Systems, 11(1), 23-33.

[19] Oghenekaro, L. U., & Ugwu, C. (2016). A novel machine learning approach to credit card fraud detection. International Journal of Computer Applications, 140(5), 45-50.

[20] Sadgali, I., Sael, N., &Benabbou, F. (2018). Detection of credit card fraud: State of art. Int. J. Comput. Sci. Netw. Secur, 18(11), 76-83.

[21] Alhaddad, M. M. (2018). Artificial intelligence in banking industry: a review on fraud detection, credit management, and document processing. ResearchBerg Review of Science and Technology, 2(3), 25-46.

[22] Qi, Y., & Xiao, J. (2018). Fintech: AI powers financial services to improve people's lives. Communications of the ACM, 61(11), 65-69.

[23] La, H. J., & Kim, S. D. (2018). A machine learning framework for adaptive Fintech security provisioning. Journal of Internet Technology, 19(5), 1545-1553.

[24] Leite, R. A., Gschwandtner, T., Miksch, S., Gstrein, E., & Kuntner, J. (2018). Visual analytics for event detection: Focusing on fraud. Visual Informatics, 2(4), 198-212.

[25] Barman, S., Pal, U., Sarfaraj, M. A., Biswas, B., Mahata, A., & Mandal, P. (2016). A complete literature review on financial fraud detection applying data mining techniques. International Journal of Trust Management in Computing and Communications, 3(4), 336-359.

[26] Dong, W., Liao, S., & Zhang, Z. (2018). Leveraging financial social media data for corporate fraud detection. Journal of Management Information Systems, 35(2), 461-487.

[27] Liu, C., Chan, Y., Kazmi, S. H. A., & Fu, H. (2015). Financial fraud detection model: Based on random forest. International journal of economics and finance, 7(7), 178.

[28] Hasheminejad, S. M., & Salimi, Z. (2018). FDiBC: a novel fraud detection method in bank club based on sliding time and scores window. Journal of AI and Data Mining, 6(1), 219-231.

[29] Omolara, A. E., Jantan, A., Abiodun, O. I., Singh, M. M., Anbar, M., & Kemi, D. V. (2018). State-of-the-art in big data application techniques to financial crime: a survey. International Journal of Computer Science and Network Security, 18(7), 6-16.

[30] Zoldi, S. (2015). Using anti-fraud technology to improve the customer experience. Computer Fraud & Security, 2015(7), 18-20.

[31] Rohit, K. D., & Patel, D. B. (2015). Review on detection of suspicious transaction in anti-money laundering using data mining framework. International Journal for Innovative Research in Science & Technology, 1(8), 129-133.

[32] Talekar, D. L., &Adhiya, K. P. (2015). Credit card fraud detection using hmm and image click point authentication. International Journal of Advanced Studies in Computers, Science and Engineering, 4(3), 1.

[33] Tade, O., & Adeniyi, O. (2017). Automated teller machine fraud in south-west Nigeria: Victim typologies, victimisation strategies and fraud prevention. Journal of Payments Strategy & Systems, 11(1), 86-92.