Detection of Fraud Transactions Using Recurrent Neural Network during COVID-19

[1]Shawni Dutta and [2]Prof. Samir Kumar Bandyopadhyay

[1]Department of Computer Science, The Bhawanipur Education Society College, Kolkata, India.

[2] Academic Advisor, The Bhawanipur Education Society College, Kolkata, India

Abstract-

Online transactions are becoming more popular in present situation where the globe is facing an unknown disease COVID-19. Now authorities of Countries requested peoples to use cashless transaction as far as possible. Practically it is not always possible to use it in all transactions. Since number of such cashless transactions have been increasing during lockdown period due to COVID-19, fraudulent transactions are also increasing in a rapid way. Fraud can be analysed by viewing a series of customer transactions data that was done in his/her previous transactions. Normally banks or other transaction authorities warned their customers about the transaction If any deviation is noticed by them from available patterns. These authorities think that it is possibly of fraudulent transaction. For detection of fraud during COVID-19, banks and credit card companies are applying various methods such as data mining , decision tree, rule based mining, neural network, fuzzy clustering approach and machine learning methods. These approaches is try to find out normal usage pattern of customers based on their past activities. The objective of this paper is to find out such fraud transactions during such unmanageable situation.

Digital payment schemes are often threatened by fraudulent activities. Detecting fraud transaction in during money transfer may save customers from financial loss. Mobile based money transactions are focused in this paper for fraud detection. A Deep Learning (DL) framework is suggested in this paper that monitors and detects fraudulent activities. Implementing and applying recurrent neural network on PaySim generated synthetic financial dataset, deceptive transactions are identified. The proposed method is capable to detect deceptive transactions with an accuracy of 99.87%, F1-Score of 0.99 and MSE of 0.01.

Keywords: Fraud Detection, Recurrent Neural Network, PaySim, Financial Transactions, Deep Learning.

Introduction-

Fraud detection is an emerging problem during the present situation when coronavirus has been spreading throughout the world. The extensive availability of uncontrolled consumer communication channels (e.g., internet, mobile banking, telephone banking etc.), the challenge of controlling fraud has been increased substantially. In online purchases, the customer frequently used online transactions very often. A significant increase in the volume of electronic transactions mainly due to the popularization of World Wide Web as well as for COVID-19. The reason is lockdown due to high mortality of humans for the disease. The latest technological inventions are also facing problems of hacking user accounts easily. Therefore it is needed urgently to develop techniques that can assist in fraud detection. It is the main motivation of the paper.

The preference for E-commerce websites for purchasing various products at a more economic or reasonable price have a positive impact on growth of the target market. Mobile payment system facilitate nearly any type of payments. Most merchants prefer online system of operations for online shopping during COVID-19. Any payment can be made if a person has online transaction facility and has mobile. Mobile is required for receiving One Time Password (OTP). Mobile wallets helps to increase the overall use of mobile payment. It is found that mobile payments have reached $194.1 billion in 2017 and $30.2 billion in 2017 as compared to $18.7 billion in 2016 [1]. The market using global mobile wallet is expected to value at more than $0.5 billion in 2019 [2]. During COVID-19, it is definitely increased more due to lockdown faced by most of the peoples in the globe.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2020 doi:10.20944/preprints202006.0368.v1

The objective of this paper is to establish an effective and accurate fraudulent financial mobile money transaction detection model with high efficiency and low error rate. It utilises Deep Learning (DL) [3] techniques for implementing this model. These techniques are beneficial since it automatically captures hierarchical features present in the financial dataset. Recurrent Neural Network (RNN) [4] follows DL architecture which is utilised in this paper. A stacked RNN model is proposed as a recommender system for detection of fraud transaction. Automatic recognising of suspicious activities that trigger illegal attempts will alarm the customers so that economic loss can be prevented. Analysis of the proposed algorithms includes determination of quantitative, qualitative, comparative and complexity measures. The proposed methods have been rigorously tested using dataset.

Related Works-

Numerous studies have been carried out for fraud detection. A rule based fraud detection scheme [5] has been proposed for recognising scams in telecommunication industry. The proposed model performs well with low rate of false triggering rates [5]. For explaining the overall process of detecting fraud payment by mobile. Supervised and unsupervised methods are proposed in [1] to detect fraud and process large amounts of financial data. Unsupervised ML includes EM, K-Means, Farthest First, XMeans, Density-based clustering those are applied on financial data. Naïve Bayes, SVM, Logistic regression, OneR, Decision tree, C4.5, Random Forests, Random Tree are implemented by [1] for financial fraud detection.

Using machine learning techniques such as Logistic regression and Support Vector Machine have been applied effectively to the problem of payments related fraud detection [6]. Another study [7] revealed financial statement fraud from a selection of Greek manufacturing firms using Decision Tree, Neural networks, Bayesian belief networks with an efficiency of 72.5%, 77.5% and 88.9% respectively. Financial statement fraud with managerial statements was detected by implementing text mining and singular validation decomposition vector with specificity of 95.65% [8]. An investigation in [9] has introduced Classification and Regression Tree (CART) for identifying false financial statements. Johan Perols [10] investigated and compared six machine learning algorithms such as logistic regression, support vector machines, artificial neural network, bagging, C4.5, and stacking. Experimental study concluded that logistic regression, support vector machines provide relatively better results over other specified classifier models.

Proposed Methodology-

Deep learning (DL) [3] belongs to broader family of Machine Learning. These techniques are consisting of algorithms those are inspired by operations of human brains. The popularity of DL techniques relies on its self-learning structure with minimal amount of processing. Deep neural networks (DNN) are often considered as an improvement over traditional artificial neural network (ANN) [11] in the sense that it incorporates multiple layers into its architecture. DNN can learn hierarchical feature representation from the data itself by discovering higher level feature extraction from lower level features [3]. Any deep models are thought of as multi-layer architecture that accepts input vector and maps them into corresponding output labels. Recurrent Neural Network (RNN) is a kind of deep models that allows feedback loop structure in its architecture. The word 'recurrent' is used since for every input of data same function is performed and the output of current input depends on the previous computation. RNN is dominant because it can model sequences by considering inter-depending relationships in the samples of the sequences [4]. While designing deep model, it is necessary to consider activation function, which is a step that maps input signal into output signal [12]. Sigmoid and tanh are two popular activation functions those are employed in this framework. Sigmoid activation function [12] transforms input data in the range of 0 to 1 and it is shown in equation(1). The hyperbolic tangent (tanh) [12] is a smoother and zero-centred function. The range of this function range lies between -1 to 1, thus the output of the tanh function is given as equation (2).

$$f(x) = 1/(1 + exp^{-x}) \quad (1)$$

$$f(x) = (e^{x} - e^{-x})/(e^{x} + e^{-x}) \quad (3)$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2020 doi:10.20944/preprints202006.0368.v1

Initially neural network models are configured and training process is started. The training process goes through one cycle and it is known as an epoch. During this period the dataset is partitioned into smaller sections. Finally, iterative process is executed over a couple of batch size as a subsections of training dataset for completing epoch execution [13]. This entire process is inclined towards solving binary classification problem so binary cross entropy function is used as training criterion. Binary cross entropy measures the distance from the true value (which is either 0 or 1) to the prediction for each of the classes and then averages these class-wise errors to obtain the final loss [14].

The aim of the paper is to detect suspicious activities of money transaction during COVID-19. A classifier model associates input data into output classes after learning from training data. A stacked RNN based model is proposed as classifier model that identifies transactions that may have deceptive issues. Multiple RNN layers are stacked into a single platform for obtaining the proposed model. Four simple RNN layers along with four dropout layers are incorporated into a sequential model. Incorporating Dropout layers randomly deactivate a fraction of the units or connections in a network during each of the training iterations, thus reducing the problem of over-fitting [15]. The model is again followed by four dense layers. Table 1 provides detailed description of the implemented model in terms of type of layers, number of nodes or dropout rate, shape of output produced by each layer, number of parameters accepted by each layer, activation function used. These layers are compiled using 'adam' [16] optimizer and binary cross entropy loss function. Adam is computationally efficient optimizes with less memory requirement. It is easy to implement and is applicable for first-order gradient-based optimization of stochastic objective functions. It is based on adaptive estimates of lower-order moments. It is e well accepted due to its applicability on non-stationary objectives and problems with very noisy and/or sparse gradients [16].

While fitting the training set into the classifier model, 2 epochs and 64 batch sizes is used. During training the model accepts a total of 33,065 trainable parameters and uses those parameters for obtaining prediction results.

Layers	Type of Layer	Number of Nodes/Rate	Number of Parameters Received	Activation Function Used
Layer 1	Simple RNN	128	16640	Sigmoid
Layer 2	Dropout	0.2	0	None
Layer 3	Simple RNN	64	12352	Sigmoid
Layer 4	Dropout	0.2	0	None
Layer 5	Simple RNN	32	3104	Sigmoid
Layer 6	Dropout	0.2	0	None
Layer 7	Simple RNN	16	784	Tanh
Layer 8	Dropout	0.2	0	None
Layer 9	Dense	8	136	None
Layer 10	Dense	4	36	None
Layer 11	Dense	2	10	None
Layer 12	Dense	1	3	Sigmoid

Table 1: Architecture of Proposed Stacked-RNN model

Dataset Used-

Financial dataset simulated by PaySim [17] that identifies mobile money transactions based on a sample of real transactions. These transactions are collected from one month financial logs of a mobile money service implemented in an African country. The original dataset is scaled down to ¼ th of the original dataset and the resultant one is available at Kaggle. The dataset consists of 6362620 online transaction records during COVID-

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2020 doi:10.20944/preprints202006.0368.v1

19 and each record is formulated as a collection of several attributes. The attributes along with their description is provided in table2. The transaction type in the dataset along with the number of occurrences is shown in figure 1. The non-numeric data present in the dataset is transformed into numeric data. Next, all the numeric data are scaled down into a specific range from 0 to 1. This will help in pre-processing dataset on which proposed classifier is applied. Cash-out and transfer type transactions are having suspicious transaction set. The exact scattering of these two types of transaction is depicted in Figure 2. The dataset is divided into training and testing dataset with a ratio of 8:2. The training dataset is fitted into stacked-RNN classifier model and later predictions are made for testing dataset. The attribute 'isFraud' is kept as target variable of classification procedure. The distribution of fraud and non-fraud transactions in the dataset is shown in Figure 3.

Attribute Name	Description
step	Maps a unit of time in the real world.
type	Transaction Type: CASH-IN, CASH-OUT, DEBIT, PAYMENT and TRANSFER.
amount	Transaction amount
nameOrig	Customer name who initiated the transaction
oldbalanceOrg	Sender's balance before transaction
newbalanceOrig	Sender's balance after transaction
nameDest	Recipient customer name
oldbalanceDest	Recipient's balance before transaction
newbalanceDest	Recipient's balance after transaction
isFraud	Transactions made by the fraudulent agents inside the simulation.
isFlaggedFraud	Flags illegal attempts.

Table 2: Summary of Collected dataset

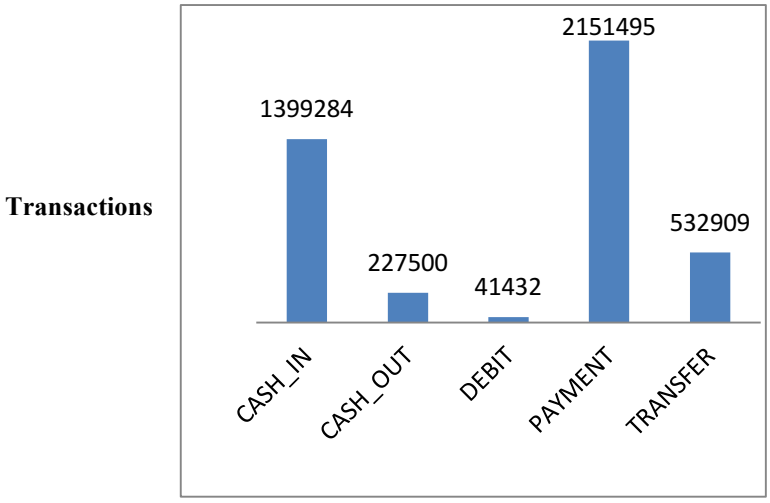

Figure1: Statistics of type of transactions.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2020 doi:10.20944/preprints202006.0368.v1

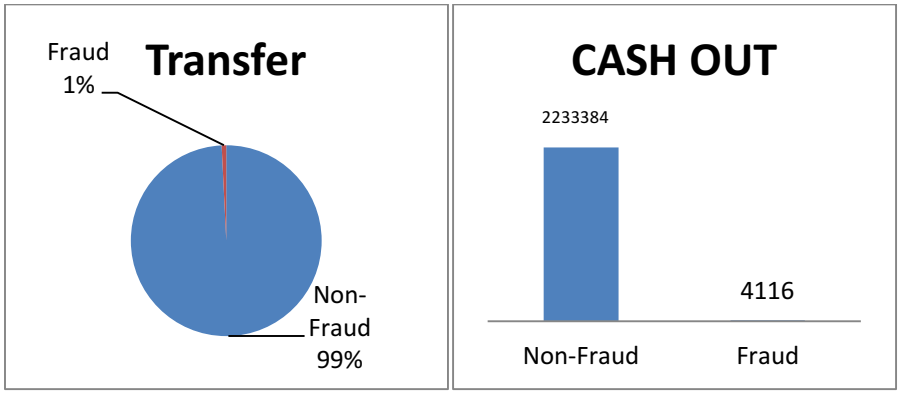

Figure2: Distribution of fraud and non-fraud transactions for transfer and cash-out type transaction

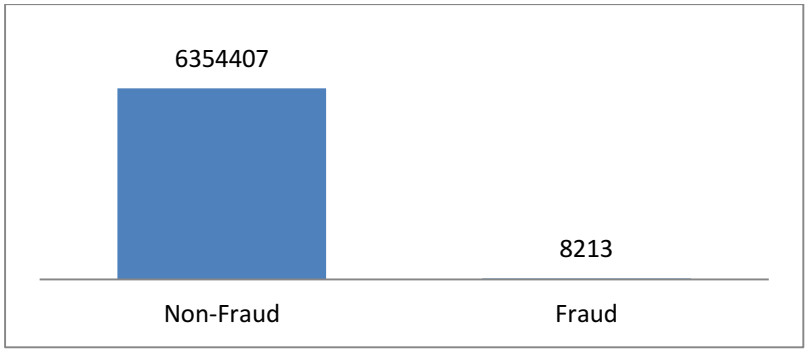

Figure3: Distribution of fraud transactions over the dataset.

Experimental Results-

The performance of any predictive model needs to be evaluated which instantiates the importance of evaluation metrics. This section discusses the metrics those are employed to measure the performance of the classifier models. In this research, following metrics are considered as performance evaluating metrics in order to justify the prediction results.

1. Accuracy [18] is a metric that detects the ratio of true predictions over the total number of instances considered. However, the accuracy may not be enough metric for evaluating model's performance since it does not consider wrong predicted cases. Hence, for addressing the above specified problem, precision and recall is necessary to calculate.

2. Precision [19] identifies the ratio of correct positive results over the number of positive results predicted by the classifier. Recall [18] denotes the number of correct positive results divided by the number of all relevant samples. F1-Score or F-measure [18] is a parameter that is concerned for both recall and precision and it is calculated as the harmonic mean of precision and recall. The best value of F1-score, precision, and recall is known to be 1.

3. Mean Squared Error (MSE) [19] is another evaluating metric that measures absolute differences between the prediction and actual observation of the test samples. MSE produces non-negative floating point value and a value close to 0.0 turns out to be the best one.

Precisely, the above mentioned metrics can be defined as follows with given True Positive, True Negative, False Positive, False Negative as TP,TN,FP,FN respectively-

$$\text{Accuracy} = TP+TN/(TP+FP+TN+TP)$$

$$\text{Recall} = TP/(TP+FN) \qquad \text{Precision} = TP/(TP+FP)$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 June 2020 doi:10.20944/preprints202006.0368.v1

F1- Measure or F1-Score= 2* Recall * Precision / (Recall + Precision)

MSE= $(\sum_{i=1}^{N}(Xi - Xi')^2$ / N) where Xi is the actual value and Xi' is the predicted value.

The Stacked-RNN model is evaluated in terms of aforementioned evaluating metrics and the result is shown in table 2. This analysis shows that the proposed model performs significantly well in terms of fraud transaction detection. During training of this model, some loss is acquired for each epoch which is depicted in Figure 4. As the numbers of epochs are increasing, the loss is decreased and attains minimised loss. The minimised loss will indicate better performing model.

Stacked-RNN Model	Accuracy	F1-Score	MSE
	99.87%	0.99	0.01

Table2: Performance of Stacked-RNN

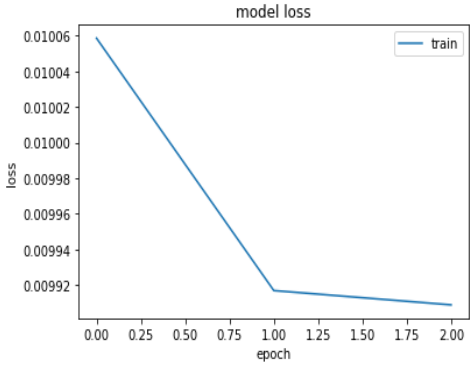

Figure4. Loss acquired for each epoch during training.

Conclusions-

Due to increasing demand of mobile money transfer, it is necessary to discover fraud activities during transactions. This is now inevitable during COVID-19. Discovering illegal attempts will prevent the customers to be harassed from financial dispute. The study has been made from the announcement of Covid-19 to first unlock period announced by the Government. The main aim of the to minimize fraud as far as possible. The predicted results by the proposed model proved mathematically that fraud transactions are less than non-fraud transactions. It shows that the method is practical and is highly suitable for implementation at the present scenario. It detects the feasibility of using deep learning techniques for identifying fraudulent financial transactions during lockdown period. For this purpose, a stacked-RNN model is proposed and implemented with necessary fine-tuning of hyper-parameters. Adjusting of hyper-parameters will assist in obtaining more fine-grained model with maximised performance. From experimental results, it is quite clear that the proposed model is capable of recognizing suspicious transactions with promising efficiency. This proposed method is favourable because of its applicability on large financial dataset. An efficient and low error system is required in the field of mobile transaction since it will notify the customers by triggering deceptive transactions.

References-

[1] D. Choi and K. Lee, "Machine Learning based Approach to Financial Fraud Detection Process in Mobile Payment System," *IT Converg. Pract.*, vol. 5, no. 4, pp. 12–24, 2017.

[2] S. Tathe, "Mobile Wallet Market By Mode Of Payment (Remote Payment , And Request Sample," no. September, 2019.

[3] J. Liu, J. Liu, W. Du, and D. Li, "Performance analysis and characterization of training deep learning models on mobile device," *Proc. Int. Conf. Parallel Distrib. Syst. - ICPADS*, vol. 2019-Decem, pp. 506–515, 2019, doi: 10.1109/ICPADS47876.2019.00077.

[4] A. Sherstinsky, “Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) network,” *Phys. D Nonlinear Phenom.*, vol. 404, no. March, pp. 1–43, 2020, doi: 10.1016/j.physd.2019.132306.

[5] S. S. Rajani, S. Vuniversity, and P. M. Padmavathamma, “A Model for Rule Based Fraud Detection in Telecommunications Abstract : Telecommunications fraud is a worldwide problem that deprives operators of enormous sums of money every year .. Fraud detection is an increasingly important and data applications are ,” vol. 1, no. 5, pp. 1–7, 2012.

[6] J. Besenbruch, “Fraud Detection Using Machine Learning,” 2018.

[7] S. Chen, “Detection of fraudulent financial statements using the hybrid data mining approach,” *Springerplus*, vol. 5, no. 1, pp. 1–16, 2016, doi: 10.1186/s40064-016-1707-6.

[8] F. H. Glancy and S. B. Yadav, “A computational model for financial reporting fraud detection,” *Decis. Support Syst.*, vol. 50, no. 3, pp. 595–601, 2011, doi: 10.1016/j.dss.2010.08.010.

[9] X. Y. Belinda Bai., Jerome Yen., “False Financial Statements : Characteristics,” *Int. J. Inf. Technol. Decis. Mak.*, vol. 7, no. 2, pp. 339–359, 2008.

[10] J. Perols, “Financial statement fraud detection: An analysis of statistical and machine learning algorithms,” *Auditing*, vol. 30, no. 2, pp. 19–50, 2011, doi: 10.2308/ajpt-50009.

[11] S. Harvey and R. Harvey, “An introduction to artificial intelligence,” *Appita J.*, vol. 51, no. 1, 1998.

[12] C. Nwankpa, W. Ijomah, A. Gachagan, and S. Marshall, “Activation Functions: Comparison of trends in Practice and Research for Deep Learning,” pp. 1–20, 2018.

[13] Y. You, J. Hseu, C. Ying, J. Demmel, K. Keutzer, and C. J. Hsieh, “Large-batch training for LSTM and beyond,” *Int. Conf. High Perform. Comput. Networking, Storage Anal. SC*, pp. 1–15, 2019, doi: 10.1145/3295500.3356137.

[14] K. Janocha and W. M. Czarnecki, “On loss functions for deep neural networks in classification,” *Schedae Informaticae*, vol. 25, pp. 49–59, 2016, doi: 10.4467/20838476SI.16.004.6185.

[15] S. H.-I. Shen Dinggang, Wu Gurrong, “Deep Learning in Medical Image Analysis,” *Annu. Rev. Biomed. Eng*, vol. 19, no. March, pp. 221–248, 2017, doi: 10.1146/annurev-bioeng-071516.

[16] D. P. Kingma and J. L. Ba, “Adam: A method for stochastic optimization,” *3rd Int. Conf. Learn. Represent. ICLR 2015 - Conf. Track Proc.*, pp. 1–15, 2015.

[17] E. A. Lopez-Rojas , A. Elmir, and S. Axelsson. "PaySim: A financial mobile money simulator for fraud detection". In: The 28th European Modeling and Simulation Symposium-EMSS, Larnaca, Cyprus. 2016

[18] P. Baldi, S. Brunak, Y. Chauvin, C. A. F. Andersen, and H. Nielsen, “Assessing the accuracy of prediction algorithms for classification: An overview,” *Bioinformatics*, vol. 16, no. 5, pp. 412–424, 2000, doi: 10.1093/bioinformatics/16.5.412.

[19] H. M and S. M.N, “A Review on Evaluation Metrics for Data Classification Evaluations,” *Int. J. Data Min. Knowl. Manag. Process*, vol. 5, no. 2, pp. 01–11, 2015, doi: 10.5121/ijdkp.2015.5201.

 doi:10.20944/preprints202006.0368.v1