NVEO
Natural Volatiles & Essential Oils

Hybrid CNN- BILSTM-Attention Based Identification and Prevention System for Banking Transactions

Aayushi Agarwal[1], Md Iqbal[2], Baldivya Mitra[3], Vimal Kumar[4], Niranjan Lal[5]

[1,2,3,4]Department of Computer Science & Engineering, Meerut Institute of Engineering and Technology, Meerut, UP, India

[5]CSE, School of Engineering and Technology, Mody University of Science and Technology, Lakshmangarh, Sikar, Rajasthan, India

[1]aashi04agarwal@gmail.com, [2]md.iqbal@miet.ac.in , [3]baldivya.mitra@miet.ac.in, [4]vimal.kumar@miet.ac.in, [,5]niranjan_verma51@yahoo.com*

Abstract:

With the increase in digitalization and more pressure on cashless transactions being put forth by our government there is a major risk of the credit card fraud in budgetary exchanges. Hence, the credit card fraud detection is the utmost responsibility and a crucial challenge up here for researchers to lessen the incurring losses by the banks and customers. The Customary detection method by organizations would mainly rely on rules. But there are some limitations to such rule-based methods as each rule has a corresponding threshold and being absolute in nature, they are inefficient when used alone. Moreover, they cannot treat a large amount of data at the same time. Nowadays, researchers are laboring hard into techniques such as Artificial Intelligence, Machine Learning, Data Mining, etc. In this paper, I have used Deep Learning techniques like CNN, BILSTM with ATTENTION layer. Using these techniques, the maximum efficiency which could be attained is 95%. Analytical outcomes applied to the real-world transaction information given by a business bank shows that our proposed strategy achieve desirable accuracy than any other techniques.

Keywords: Credit card Fraud Detection, Deep learning, CNN, BILSTM.

1. INTRODUCTION:

The world is enhancing its steps forward day by day to newer technologies and making our lives more comfortable than before. Online transactions, in just a click are the boon for all of us. But convenience comes with a cost and so are frauds. With the emergence of digital transactions, the fraudsters are doing illegitimate deeds leading to a massive number of fraudulent activities every day. The credit card fraud report shows $24.26 billion losses in the year 2018. RTI claims since Jan 2015 to Dec 2018 there is total of Rs 14,165 lakhs loss and estimated that in 2020 there would be an increment in the frauds costing $32 billion. It is very easy to conduct fraud by using very little amount of information about the card only. The fraudsters are using different and new mechanisms to perform such fraud actions so that it can be difficult to track them. For reducing the fraud success it is necessary to introduce a fraud detection technique. Credit card fraud detection is one of the applications of prediction analysis as fraudulent transactions are predicted based on the historical information of credit card transactions. Historical information of of card transactions will be the training data for the fraud transaction prediction. The next actions of the customer can be predicted using this information. This kind of fraud is identified when the actual owner of the card has no knowledge about the transactions being made from his card. Of course there will be no contact with the card owner and the actual user will not receive any loss repayment from the fraudulent person.

Predictive analytics is for identifying the patterns and predicting the future possibilities. A mathematical model is developed using the information related to previously occurred event such that the events that could possibly occur in future could be predicted. The scores are assigned to the data based on certain predictive analytical models. The model which focuses on the behavior of an individual customer is the most commonly used predictive model in today's applications. The sample data in which the known attributes are involved helps in training the model. This model can further be helpful in analyzing the new data as well as its behavior.

Types of Fraud:

a. Application Fraud: Applying for a credit card with false identity, where a person uses someone else's information to issue the credit card.

b. Lost/Stolen cards: When a person loses his card and if somebody found it then he can use it for his own personal use without informing the cardholders or the authorized authority. It is best way for the fraudsters to get information about someone else's account. It is the difficult form of fraud to tackle.

c. Account Takeover: This type of fraud takes place when the fraudsters attain information illegally. The fraudsters have the power to control complete account unless someone recognizes the fraud.

d. Fake and Counterfeit cards: In this type of fraud, the fraudsters can make fake card with the help of all the stolen/lost cards. The fraudsters always come up with new and advanced techniques to create illegal cards.

In this paper, the problems are investigated and solutions are presented to identify credit card fraud by applying deep learning techniques on the IEEE-CIS Fraud Detection dataset by Kaggle [10]. The paper is prearranged as follows: Section 2 encloses the related work. Section 3 exhibit details on proposed methodology. In Section 4 the results are discussed. Conclusions and references are discussed in sections 5 and 6 respectively.

2. RELATED WORK:

Hassan Najadat et al. presented a way to deal with real or counterfeit payments on the dataset taken from Kaggle [1]. The models applied here are Bi-LSTM and Bi-GRU both with max pooling layer which yields better results than machine learning techniques. In addition various classifiers are applied are Naive Bayes, Voting, Adaboosting, Random Forest, Decision Tree, and Logistic Regression. Contrasting the outcomes of classifiers and the model proposed shows that model accomplished good accuracy of 91.37%.

John O. Awoyemi et al. [2] presented a study through which the different fraudulent detection techniques designed to prevent credit card based frauds were investigated. A dataset that was used in this investigation was collected from the transactions done by the European cardholders. In order to perform oversampling as well as under-sampling, the hybrid approach was proposed that includes Naive bayes, KNN and Logistic Regression for the imprecise data. Python was used here for applying three various techniques on both raw as well as pre-processing data. The evaluation of performances was done by calculating the performance parameters. The result outcomes showed that the proposed technique outperformed previous techniques since it provided higher accurate results.

Pranali Shenvi et al. [3] in this paper, a technique for Fraud Detection based on Deep Learning is used. Contrasting all the famous techniques, for example, Random Forest, Support Vector Machines, and so on are done. At last, a conclusion is made that Neural Networks, despite the fact that are difficult to prepare, will be an ideal technique. The two techniques are used: under sampling and over sampling, by diminishing the number of false transactions or by replicating deceitful class transactions. The outcomes convey these techniques increment the efficacy of the model.

Abhimanyu Roy et al.[4] introduced four discrete methods of Deep Learning : Artificial Neural Networks, RNN, LSTM, and GRU. The dataset used in the paper consists of 80 million transactions which are labeled as fraudulent and genuine. The fraudulent classes are less as compared to the genuine class. So, the feature engineering and under sampling techniques are also applied. The GRU model performed the accuracy of 0.916 and LSTM model had an accuracy of 0.912.

M.Puh et al.[5] presented Supervised ML techniques such as Random Forest, Support Vector Machine and Logistic Regression. The dataset used here consists the exchanges done by European credit cardholders in September 2013, results in 284,807 total transactions containing 492 illegitimate transactions, 31 features and 28 numerical input variables transformed using Principal Component Analysis. To balance the dataset this paper used SMOTE technique. The result of this paper shows that by using SVM it has achieved the performance which was not good while Logistic Regression achieved better performance.

Sharmistha Dutta et al. [6] proposed a research that was based on identifying the crimes related to credit cards. For avoiding any identity theft few issues are faced when dealing with the non-data mining techniques. If, to prevent frauds, the non-data mining techniques are applied, few problems can be faced. To prevent such common issues, a new data mining layer was designed in this research [11,12]. For generating this new layer, two algorithms known as Communal Detection and Spike Detection were applied. Large amount of time is needed to generate the results. Even with the continuous updates on algorithms, no actual evaluation is performed since the behaviors do not change depending upon the algorithms used. Thus, the adaptability concept cannot be visualized clearly here. The future work of this research can be to extend the proposed method for resolving such issues.

Krishna Modi et al. [7]enclosed numerous methods to present an analysis to detect the fraud and draw comparison among the models presented in this paper used to detect fraudulent transactions. The techniques used or their combination can be utilized to identify deceitful transactions. More features can be included and different examining strategies can be utilized to prepare the model for training to get better results.

Kang Fu et al. [8] put forward a CNN based architecture to identify the inherent patterns in transactions of credit card. Moreover, the trading entropy is used to demonstrate progressively complex expending practices. Also, they recombine the trading output to matrix and use in CNN. Test results from the genuine dataset of a bank show that the proposed strategy performed here has given better results compared to other strategies.

3. PROPOSED METHODOLOGY:

The strategy used to implement the proposed objective can be understood by following steps:

1. Importing and collecting the dataset.

2. Extracting important features for training the model.

3. Using SMOTE technique to balance the dataset.

4. Performing Feature Scaling.

5. Splitting the dataset into training and testing.

5. Creating a model.

3.1. DATASET DESCRIPTION:

For the creation of a model we use the dataset from Kaggle namely IEEE-CIS Fraud Detection [10]. The data consists of csv files, test transaction and test identity, train transaction and train identity. As we are working on the credit card detection, so we have taken out the transactions containing only of credit card. The transaction and identity files were combined on the basis of Transaction ID column, eventuating in 436 features in the dataset and 148986 total cases. Although, the features are ignored on the basis of null and repeated values. Then, the XGB classifier is applied to filter the important features to train the model and thus deleted the remaining features. The remaining columns that comprises of null values were replaced with 0 and categorical columns are converted into numerical using Label encoding technique. Since the dataset given is imbalanced, which results in 93.32% transactions classified as real transactions, while there are 6.68% classified as counterfeit transactions and this leads the model to get biased towards the legitimate class which will not result in good prediction. To overcome this problem we use SMOTE technique which leads to increase in the percentage of that class which has less number of cases.

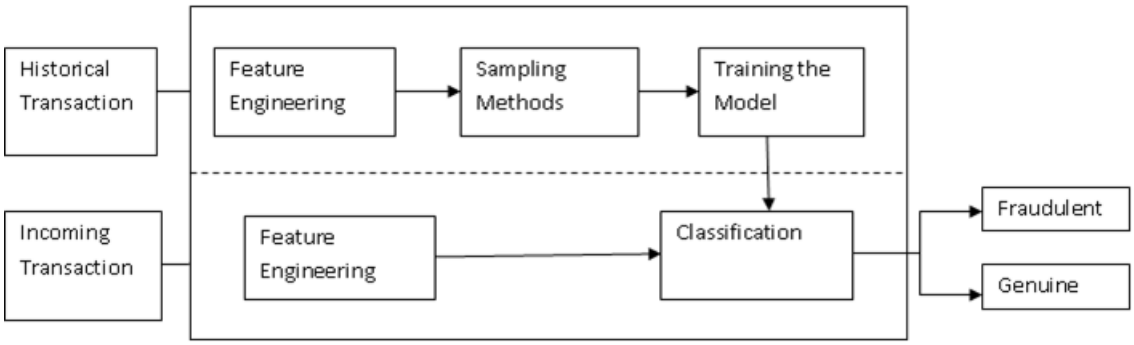

Fig.1: Implementation process

3.2 IMPLEMENTATION:

In this paper, the model is constructed by using Deep Learning Techniques, namely convolutional layer, Bi-LSTM layer and followed by attention layer. First , the neural network is train by passing the input data in the form of matrix into the convolutional layer and apply 'relu' as an activation function which allow model to learn at a faster rate and perform better than others and introduces non-

linearity in the network.. Then the output of the convolutional layer which is reduced matrix is passed into the Bi-LSTM layer to learn long term dependencies where 'tanh' is used as an activation function to do classification between two classes. After that dropout layer of 0.5 is used to prevent a model from over fitting, further an attention layer is used to assign the weights to the important features and neglecting the irrelevant features. At last, dense layer is applied with a sigmoid activation function. Next, Adam is used as an optimizer to reduce the loss function with 0.001 as a learning rate and binary cross-entropy as a loss function is taken. The combination of all these layers results in the enhancement of classification process.

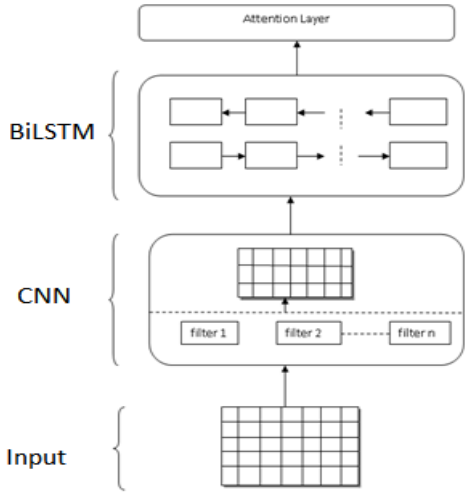

Fig.2: Architecture of the model

CNN: Convolution Neural Network is a form of Artificial Neural Network used effectively in certain fields, for example, image classification, computer vision etc. A Convolutional neural network is a multilayer network, this means the output of one layer will be the input to the next layer and comprises of an input layer, hidden layers and an output layer. The function of the ConvNet is to decrease the input into a structure which is simpler to process, without losing important information for getting a good prediction.

In our approach, we are using first layer as convolution for processing the data with 128 filters and a kernel size as 3. We pass the input matrix of m by n where m is no of rows and n is the no of variables which results an output matrix of dim x and y.

$G[x , y] = (m*n)[x , y] = \sum\sum h[j , k]f[m-j , n-k]$.

BILSTM: Bidirectional Long Short-Term Memory is a kind of Recurrent Neural network [13]. It consists of two hidden layers and processes the data in forward and backward direction so that the structure should have the backward direction so that the structure should have the knowledge of previous data also. It is the second layer in our proposed architecture and is used to memorise the previous transactions which are useful to predict the output y , which can be formulated as follows-

$y^t = g(w_y [h^t,c^t]+ b_y)$

where t = transaction , w is the weight value assigned to the concatenation of the hidden and current state generated by the Bi-LSTM , h and c are the hidden and current state.

Attention layer: We need a mechanism to find the multicolinearity in a given transaction, so we attempt to use a attention layer which functions in the same manner as our brain, focusing on relevant things while ignoring others, resulting into easier learning and good results. Combining attention layer to Bi-LSTM yields a good output. Then output of Bi-LSTM layer, the features are passed into the attention layer and the weights are assigned to each feature for better approximation of the result. Each transaction is represented by a weighted average of the features in this layer:

$z = \sum_{i=1}^{k} ai * wi$

Where z is the weighted average of a transaction, k is the total number of variables in a transaction , w_i is the feature and a_i is the weight of each feature .

4. RESULTS :

For the model, dataset is splitted in the ratio of 70:30 for the training and testing. Then, data was balanced by using SMOTE technique and finally applied to the model. The summary of the deep learning models applied is shown in fig 3, and the Learning curves to diagnose the deep learning models are shown in fig 4 and 5 respectively.

Table 1: Explanation of the model

Layer (type)	Output Shape	Param #
input_1 (InputLayer)	(None, 146, 1)	0
conv1d_1 (Conv1D)	(None, 144, 128)	512
bidirectional_1 (Bidirection	(None, 144, 512)	788480
batch_normalization_1 (Batch	(None, 144, 512)	2048
attention_1 (attention)	(None, 512)	656
dropout_1 (Dropout)	(None, 512)	0
dense_1 (Dense)	(None, 1)	513

Total params: 792,209
Trainable params: 791,185
Non-trainable params: 1,024

During the process of training in a deep learning model, the model is evaluated at each step to give a notion of how well the model is 'learning' from the training dataset. It can likewise be assessed on a validation or test dataset to give a notion of how well the model is 'generalizing'[9].

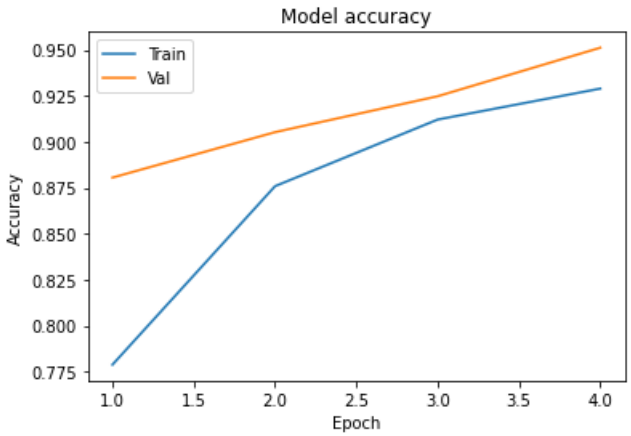

Fig.3: Accuracy Learning Curve

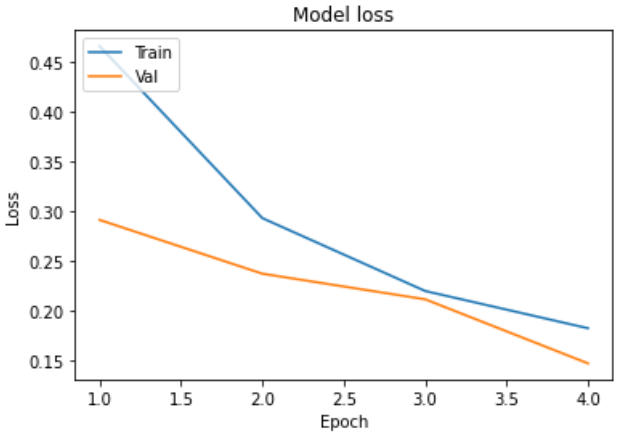

Fig.4: Loss Learning Curve

And in our case, where we are dealing with the classification predictive problem, the model is optimized according to cross-entropy loss and performance is estimated using classification accuracy, two learning curves are constructed, one gives the accuracy of the model and other gives the loss of the model, on the train and validation set in terms of number of epochs.

CRITERIA FOR EVALUATION:

To evaluate the model's performance, various metrics are calculated.

1. Accuracy: Accuracy can be defined as number of correct predictions estimated by the model to the total number of samples.

Accuracy = TP + TN/ Total

2. Precision: Precision is calculated as number of samples which are positive divided by the number of samples the model classifies as correct.

Precision = TP/TP+FP

3. Recall: Recall is defined as the number of positive samples identified by the model to the number of actual positives in the dataset.

Recall = TP/TP+FN

Table 2 : Confusion matrix

		Actual	
		0	1
Predicted	0	TP = 40822	FP=899
	1	FN =1284	TN=1691

The classification outcomes of proposed technique is shown by the confusion matrix in Table 2. The parameters defined in the table are as follows: 0 indicates the non-fraud transactions and 1 indicates the fraud transactions. Therefore, by looking at the matrix we can conclude that our model correctly identifies 40822 and 1691 transactions marked as TP (True Positive), and TN(True Negative), 899 and 1284 transactions are predicted wrong labeled as FN(False Negative) and FP(False Positive) out of 44696 training samples.

5. CONCLUSION

In this paper, the issue of fraudulent cases of credit card transaction are considered and thus proposed a constructive CNN-Bi-LSTM-ATTENTION model which combined attention mechanism and deep neural networks to detect and classify the illegitimate transactions. Compared with the most extensively used LSTM model, the CNN-Bi-LSTM-ATTENTION model achieve a good accuracy in detecting the fraudulent class. Analysis results show the adequacy of the model, and results into 95% accuracy. And the outcomes prove that addition of attention layer improves in the performance of model, hence correctly distinguishing between the fraudulent or genuine transactions.

REFERENCES

[1] Hassan Najadat, Ola Altiti, Ayah Abu Aqouleh and Mufaz Younes, "Credit Card Fraud Detection Based on Machine and Deep Learning," 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2020, pp. 204-208.

[2] J. O. Awoyemi, A. O. Adetunmbi and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," 2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos, 2017, pp. 1-9.

[3] Pranali Shenvi, Neel Samant, Shubham Kumar and Vaishali Kulkarni, "Credit Card Fraud Detection using Deep Learning," 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, 2019, pp. 1-5.

[4] Abhimanyu Roy, Jingyi Sun, Robert Mahoney, Loreto Alonzi, Stephen Adams and Peter Beling, "Deep learning detecting fraud in credit card transactions," 2018 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, 2018, pp. 129-134.

[5] M.Puh and Ljiljana Brkić, "Detecting Credit Card Fraud Using Selected Machine Learning Algorithms," *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, 2019, pp. 1250-1255.

[6] S. Dutta, A. K. Gupta and N. Narayan, "Identity Crime Detection Using Data Mining," 2017 3rd International Conference on Computational Intelligence and Networks (CINE), Odisha, 2017, pp. 1-5.

[7] K. Modi and R. Dayma, "Review on fraud detection methods in credit card transactions," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, 2017, pp. 1-5.

[8] Fu K., Cheng D., Tu Y., Zhang L. (2016) Credit Card Fraud Detection Using Convolutional Neural Networks. In: Hirose A., Ozawa S., Doya K., Ikeda K., Lee M., Liu D. (eds) Neural Information Processing. ICONIP 2016.

[9] https://machinelearningmastery.com/learning-curves-for-diagnosing-machine-learning-model-performance/ [Accesses on: 22 Dec 2020].

[10] https://www.kaggle.com/c/ieee-fraud-detection [Accesses on: 22 Dec 2020].

[11] N. Lal, S. Qamar, M. Kalra, “K- Mean Clustering Algorithm Approach for Data Mining of Heterogeneous Data” , ICT4SD, LNNS, Springer Proceeding, Vol. 10, pp.61-70, 2017.

[12] N. Lal, M. Singh, S. Pandey and A. Solanki, "A Proposed Ranked Clustering Approach for Unstructured Data from Dataspace using VSM," 2020 20th International Conference on Computational Science and Its Applications (ICCSA), Cagliari, Italy, 2020, pp. 80-86, doi: 10.1109/ICCSA50381.2020.00024.

[13] Hidayatullah, A., Cahyaningtyas, S., & Pamungkas, R. (2020). Attention-based CNN-BiLSTM for dialect identification on Javanese text. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 5(4).

[14] doi:https://doi.org/10.22219/kinetik.v5i4.1121