Identification and Mitigation of Fraudulent Transaction using Deep Autoencoder

Vipin Khattri[1], Sandeep Kumar Nayak[2 *]

[1]*Research Scholar, Department of Computer Application, Integral University, Lucknow, India*

[2]*Associate Professor, Department of Computer Application, Integral University, Lucknow, India*

vipinkhattri@gmail.com[1], nayak.kr.sandeep@gmail.com[2]

Abstract: *In an ancient era, physical resources used to apply for transacting messages, treaty content, monarchy schemes, and policies and associated national or territorial currency which consumes time duration in the heavy count with negligible security. But as time passes, technological advancement has tendered its valuable and qualitative inputs to make the conventional transaction more better at its highest level of the extent, and as a qualitative and progressive resultant, the world is breathing in the current era of the digital environment with high-security priority. The responsibility of researchers and concerned authorities is to protect the online digital transaction under the safe digital environment. Therefore continuous enhancement is required in the upgrade of the security of the transaction system to handle digital transaction fraud. This research study suggests an approach of deep autoencoder for identifying fraudulent payment card transactions. To assess the outcome and validity of the projected approach of deep autoencoder for identifying fraudulent payment card transactions, testing was executed with the help of two datasets. The first dataset is a real credit card fraud dataset that is public available in world and the second dataset are generated by collecting the data using payment card transaction including genuine transaction and fraudulent transactions. A comparative analysis performed which is based on a comparison with different method and used first dataset. The proposed integration approach performed exceptionally with the different method and accomplished the maximum performance with respect to area under receiver operating characteristic curve (AUC) (95.37%).*

Keywords: **Deep Autoencoder, Deep Learning, Online Transaction fraud, Payment Card Transaction, Oversampling.**

1. INTRODUCTION

The shifting of commercial purchasing to the online and the e-payment transactions that take place in the constantly increasing non-cash wealth have prepared the precise identification of fraud an important feature in protecting such transactions. Payment card transaction fraud happens when a fraudster make use of payment card details to accomplish buy procedures without authorization from the payment card user. The extensive utilization of payment cards and a short of efficient defense systems consequence in losses of money (billion-dollar) to payment card fraud [1]. Since payment card industries are typically reluctant to declare such information, it is not easy to find a accurate estimation of the fall. But, assured data related to the money loss originated by fraudulent payment transaction are openly available. The use of payment card in absence of robust safety measures performs million dollar losses [2]. Worldwide losses caused by payment card fraud approximate to $28.65 billion in 2018 and are projected to constantly rise [3]. By 2025, the figure of fraud is estimated to attain $35.31 billion [3].

This research study proposes a method for identifying payment card fraud transaction that utilizes algorithm of deep autoencoder. The proposed method is principally related with differentiating between fraudulent and genuine payment card transactions. The major involvement of this research study is an approach for identifying the fraud in payment card transactions with the help of oversampling technique i.e. SMOTE and machine

learning algorithm of deep autoencoder learning. The working of the proposed approach is identified with the help of first public dataset and evaluated with other machine learning technique using performance measures. It is also evaluated using second dataset that are generated by collecting the data using payment card transaction including genuine transaction and deceitful transactions.

The all part of this research study is sectioned as follows. Review of literature related to the research is carried out in the second segment of the paper. Third section of the paper elaborates proposed an approach for identification of payment card fraud. The fourth section describes the experimental outcome. At last, the outcome of the research study is concluded in the fifth section.

2. Review of Literature

There are two ways for identifying payment card fraud transaction with the algorithm of machine learning i.e. unsupervised and supervised algorithm of learning. The algorithm of unsupervised learning is related to the straight classification of transactions of payment card using data pattern that are regard as genuine transaction. After that, the algorithm differentiates transactions which are not match to that data patterns as a payment card fraud transactions. In the algorithm of supervised learning, past payment card transactions is tagged as genuine or fraudulent. Then, it begins learning with the past labeled transaction data to develop a model and used to classify new instances. Both the learning algorithms such as unsupervised [4] and supervised [5], have been employed for payment card transaction fraud identification.

Kirkos et al. [6] implemented two different approaches i.e. decision support system and bayesian belief networks for identifying fraudulent transactions. For evaluating the performance of implemented approaches, a dataset of 76 Greek companies related to financial transaction were collected. Comparisons made between implemented approaches and observed that bayesian belief networks performed with much better accuracy (90.3%) as compared with the accuracy of decision tree (73.6%).

Olszewski [7] used a self-organizing map to build an unsupervised learning model for identification of fraudulent transaction. The benefits of this approach are that it does not need predefined label information and the model is revised regularly by appending new payment card transactions. The drawback of this approach is that identification of fraudulent transaction may be hard with accuracy.

Recently, deep learning has turned out to be a dominant element of machine learning and accomplished encouraging results in different domains, such as fraud detection [8]. The research study implemented a deep learning approach that is long short-term memory for identification of payment card transaction under the supervised learning approach.

3. Proposed Methodology and Materials

The framework of the projected technique for payment card fraud identification is shown in the figure 1. This proposed framework has four steps to carry out an identification of payment card transaction fraud and these steps are elaborated in the following paragraphs.

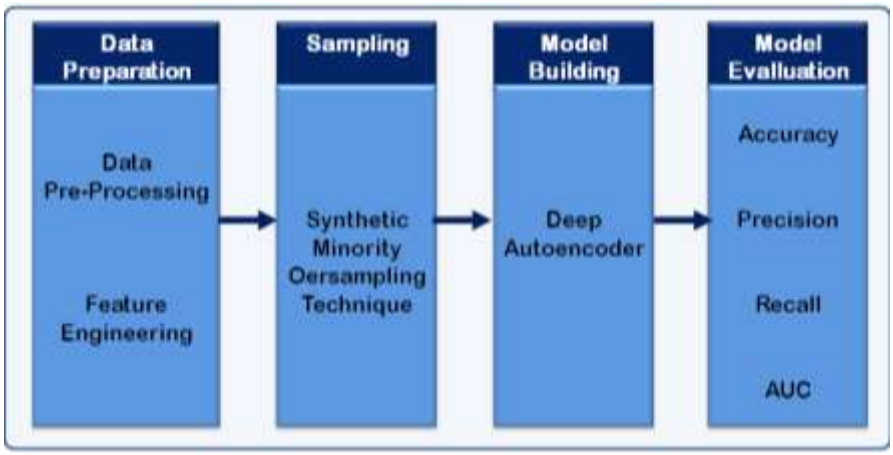

Figure 1. Framework of Deep Autoencoder for Identification of Payment Card Fraud Transaction

3.1. Data Preparation

3.1.1. Data Preprocessing: Data preprocessing [9] is a method of converting unprocessed data into a processed data format. Data processing is a very important step in building machine learning model because data processing ensures the accuracy, completeness, consistency and interpretability of the dataset. If the value of the data in dataset is inaccurate, results of the machine learning algorithm will be unreliable.

3.1.2. Feature Engineering: Features of dataset participate a very essential function in getting the high performance of machine learning algorithm [10]. Therefore, dataset is to be made compatible with algorithm of machine learning.

3.2. Sampling

Algorithms of Machine learning frequently not succeed or show evasively confident result on the dataset based on classification including an unbalanced class division. The problem occurs because algorithms of numerous machine learning are developed to execute for data using balanced samples of each class. Since, the algorithms of machine learning train the samples of both the class and if the samples of any class are less then, the training of algorithm can be done with few samples. The consequence of this situation can result in poor performance. In this research paper, unbalanced datasets are handled by using the SMOTE and it is explained the following paragraph.

3.2.3. SMOTE: An issue with unbalanced dataset shows that samples of fraudulent transactions are very less as compared with samples of genuine transactions and it is used for learning the decision boundary for a model. This issue can be solved by implementing the SMOTE (SMOTE). Although various techniques are available but in this research, the performance of SMOTE with unbalanced dataset is very efficient with small dataset and large dataset.

An enhancement on reproduction samples of the fraud class is to produce new samples from the fraud class. The working behind the SMOTE [11] is that it first selects those samples which are very near to the feature space and it creates a link between samples and creates a new example on the joining line at any point. A random selection of samples is used to join the line between them. After that randomly 5 nearest neighbor samples are selected to join among them and create new samples on that line. This technique is very efficient and successful because the newly created samples are close to the feature space.

3.3. Model Building

3.4.1 Deep Autoencoder: A deep autoencoder works on the basis of unsupervised learning with the help of artificial neural network architecture [12]. This paper implemented anomaly detection technique using deep autoencoder by analyzing the difference between input and output with respect to genuine and fraudulent transactions. During the development of deep autoencoder model, 4 layers that are fully connected are used. Layer one and two represents encoder and later third and fourth represent decoder. In addition to the layer, two activation functions such as rectified linear unit and hyperbolic tangent function are used for encoder and decoder.

3.4 Model Evaluation

The most important part of the study is the model evaluation because based on the evaluation of the model, proposed model can be judged as good or bad. Therefore, the outcome of the projected model is assessed using metrics of performance which are based on confusion matrix. The following confusion matrix [13] (see table 1) and performance metrics [14] (figure 2) are used to examine the outcome of the projected model.

Table 1. Confusion Matrix [13]

	Actual Genuine Transaction	Actual Fraudulent Transaction
Predicted Genuine Transaction	True Negative (TN)	False Negative (FN)
Predicted Fraudulent Transaction	False Positive (FP)	True Positive (TP)

S.No.	Performance Evaluation Metrics	Formula
1	Accuracy	$\frac{(TP+TN)}{(TP+TN+FP+FN)}$
2	Recall	$\frac{TP}{TP+FN}$
3	True Negative Rate	$\frac{TN}{TN+FP}$
4	Precision	$\frac{TP}{TP+FP}$
5	F1-score	$2*\frac{(Precision*Recall)}{(Precision+Recall)}$
6	G-mean	$\sqrt{(Precision*Recall)}$

Figure 2. Performance Metrics [14]

3.5. Dataset

The following table (see table 2) shows the characteristics of dataset that are used in the

experiment of the project model.

Table 2. Dataset Summary

Dataset	Dataset_I	Dataset_II
Total Transactions	2,84,807	880
Genuine Transactions	2,84,315	800
Fraudulent Transactions	492	80
Number of Features	31	17
Type of Features	Numeric	Numeric
Reference	[15]	Primary Data Collection by the author

4. Results with Discussion

The key objective behind the proposed study is to identify the fraudulent transaction of payment card. To accomplish the objective, an approach using deep autoencoder is developed and executed on two different dataset (real world dataset and primary data collected dataset). The outcome of the projected model is measured based on the metrics of performance such as true positive rate, true negative rate, false positive rate, precision, recall, G-mean, F1-Score and AUUC graph.

The outcome of the projected model based on dataset 1is generated and shown in the following figure (figure 3) and it is also compared with the other research [16] study on same dataset_I.

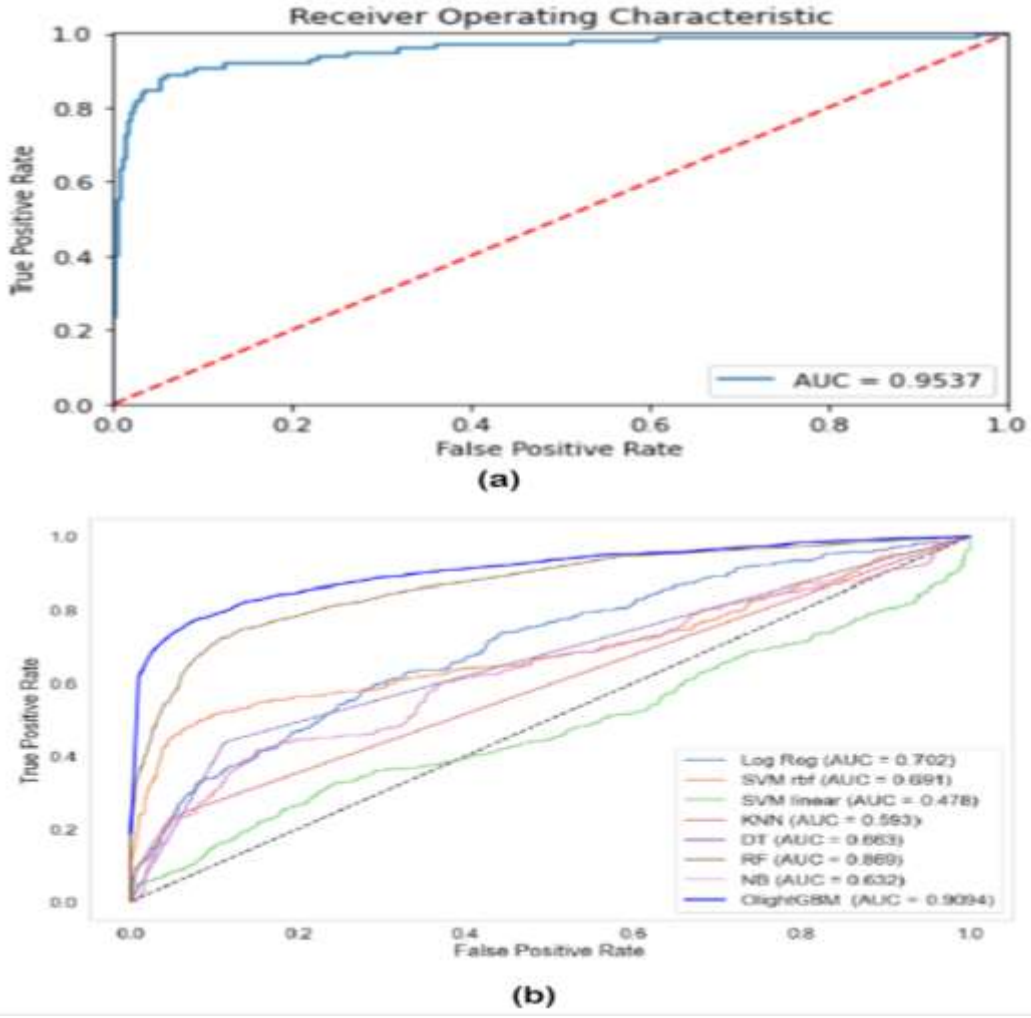

Figure 3. (a) AUC Score of the proposed model on dataset 1 (b) AUC Score [16] of the other models on dataset_I

The result of the projected model related to the AUC score is 95.37% which is higher than the

other proposed models such as Optimized Light Gradient Machine (90.94%), that shows the capability of the proposed model in differentiating the fraudulent and genuine payment card transactions.

The outcome of the proposed model based on dataset_II is also generated and shown in the following table (table 3).

Table 3. Performance of Deep Autoencoder Fraud Detection Model for Dataset_II

S.No.	Performance Metrics	Performance Result
1.	True Positive Rate	0.932
2.	True Negative Rate	0.997
3.	G-Mean	0.964
4.	Precision	0.976
5.	F1-Score	0.953
6.	Accuracy	0.990

Although total number of instances of dataset_II is small and this dataset is utilized for accessing the capability of the proposed model. The proposed model achieves good results with respect to the accuracy (99%) and the precision (97.6%).The performance result of the proposed model gives good perception for identifying the fraudulent transaction of payment card.

5. Conclusion

The identification of payment card transaction fraud is an important task to the enhanced consumption of payment card. With huge and continuous money losses being faced by economic organization and provided the rise in complexity issue of identifying payment card transaction fraud, it is essential to implement more precise methods for identifying payment card transaction fraud.

This study proposed an approach for identifying fraud in payment card transaction using deep autoencoder. This paper is experimented the model using two dataset (real world and primary dataset collection). The ability of the integrated approach was considered by judging against the other research outcomes. The results of the proposed model showed the excellent outcome related to various performance metrics. The outcomes exposed that the proposed model is better than the other classifiers.

Acknowledgment

We would like to say great thanks and show our gratefulness towards the Integral University for supporting research work and providing Manuscript Communication Number- IU/R&D/2021-MCN0001190.

References

[1] X. Zhang, Y. Han, W. Xu and Q. Wang, “HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture”, *Information Sciences*, (2019).

[2] N. Carneiro, G. Figueira and M. Costa, “A data mining based system for credit-card fraud detection in e-tail”, *Decision Support Systems*, vol. 95, (2017), pp.91-101.

[3] Nilson Report. (2021, June). Card Fraud Losses Reach $28.65 Billion. Available: https://nilsonreport.com/mention/1313/1link/.

[4] M. Carminati, R. Caron, F. Maggi, I. Epifani and S. Zanero, “BankSealer: A decision support system for online banking fraud analysis and investigation”, *computers & security*, vol. 53, (2015), pp.175-186.

[5] S. Bhattacharyya, S. Jha, K. Tharakunnel and J. C. Westland, “Data mining for credit card fraud: A comparative study”, *Decision support systems*, vol . 50, no. 3, (2011), pp.602-613.

[6] E. Kirkos, C. Spathis and Y. Manolopoulos, “Data mining techniques for the detection of fraudulent financial statements”, *Expert systems with applications*, vol. 32, no. 4, (2007), pp.995-1003.

[7] D. Olszewski, “Fraud detection using self-organizing map visualizing the user profiles”, *Knowledge-Based Systems*, vol. 70, (2014), pp.324-334.

[8] J. Jurgovsky, M. Granitzer, K. Ziegler, S. Calabretto, P. E. Portier, L. He-Guelton and O. Caelen, "Sequence classification for credit-card fraud detection", *Expert Systems with Applications*, vol. 100, (2018), pp.234-245.
[9] S. García, J. Luengo and F. Herrera, *Data preprocessing in data mining*. Cham, Switzerland: Springer International Publishing, (2015).
[10] C. R. Turner, A. Fuggetta, L. Lavazza and A. L. Wolf, "A conceptual basis for feature engineering," *Journal of Systems and Software*, vol. 49, no. 1, (1999), pp.3-15.
[11] N. V. Chawla, K. W. Bowyer, L. O. Hall and W. P. Kegelmeyer, "SMOTE: synthetic minority over-sampling technique", Journal of artificial intelligence research, vol. 16, (2002), pp.321-357.
[12] S. Misra, S. Thakur, M. Ghosh and S. K. Saha, "An autoencoder based model for detecting fraudulent credit card transaction", *Procedia Computer Science*, vol. 167, (2020), pp.254-262.
[13] I. Mekterović, L. Brkić and M. I. R. T. A. Baranović, "A systematic review of data mining approaches to credit card fraud detection", *WSEAS Transactions on Business and Economics*, vol. 15, (2018), p.437.
[14] M. A. Al-Shabi, "Credit card fraud detection using autoencoder model in unbalanced datasets", *Journal of Advances in Mathematics and Computer Science*, (2019), pp.1-16.
[15] *Credit Card Fraud Dataset*, (June 2021), Available: https://www.kaggle.com/mlg-ulb/creditcardfraud/data
[16] A. A. Taha and S. J. Malebary, "An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine", *IEEE Access*, vol. 8, (2020), pp.25579-25587.