SMOTEDeep: A Novel Link based Classifier for Fraud Detection

Dr. Ashoka.S.B.[1], Manjunath S. R.[2]
[1] *Department of Computer Science [PG]*
Maharani's Science College for Women, Bangalore-01

Abstract - Increasing incidences of fraud in credit card transactions are observed these days, owing to the popularity of electronic fund transfer. Such frauds cause a threat to privacy of mankind, resulting in financial losses. There is a need for designing advanced fraud detection solutions to minimize the hazards of these frauds. In this context, this work focuses on link-based classification of fraud instances. Initially, credit card fraud dataset is downloaded from Kaggle and feature selection techniques are employed to select relevant variables from data. Eight features are considered to be significant. Link based classification is performed primarily using SMOTE algorithm to balance the classes of fraud and non-fraud instances. The sampled class occurrences are further subjected to deep learning architecture for predicting the occurrence of fraud instances to form SMOTEDeep learner for predicting credit card fraud. The performance of this classifier is adjudicated using statistical metrics and cross validation technique. Results revealed that SMOTEDeep algorithm achieved enhanced performance in fraud detection with an accuracy of 96.4 percent. Based on these observations, it is revealed that link analysis is significant in exploring the dynamics of fraud network.

Keywords - credit card, fraud, SMOTEDeep

I. INTRODUCTION

Advent of internet has provided access to enormous content on worldwide platform. As an outcome, banking sector has digitalized its transactions for facilitating electronic modes of authorization. Newfangled technologies like credit and debit cards have replaced the age old paper accounts [1]. These machineries have enforced built in encryption protocols for ensuring secure transactions. However, these protocols are often spoofed by criminals resulting in fraudulent activities [2]. Such theft is time and again observed in electronic transactions over the years. Credit card fraud is one of the commonly observed crime activity which aims to access sequestered badges from an authentic user to perform illegal transactions. According to the 2018 Global Fraud and Identity Report, about 63 percent of businesses have experienced losses due to fraud activities in recent years [3]. Even though banks are coming up with advanced algorithms for tackling fraud, there are several instances of fraud alerts happening across the globe.

In this context, it is important to mitigate such illicit undertakings to minimize personal damage. Detection of fraud is thus an essential step which is to be acknowledged for dwindling off suspicious accomplishments. There are numerous contrivances designed for detecting fraud with an intention of curtailing instances of fraud. Network analysis is a popular approach which models the fraud instances as a graph [4]. This graph-based approach recognizes illegal protuberances to further destabilize them by analyzing the link structure across the network. Fraud detection is considered as a typical imbalance classification problem in network approach. The reason being fraud data usually comprises of larger instances of legitimate cases when compared with criminal ones. Such data is highly imbalanced and skewed. Most of the conventional classifiers fail to detect the classes due to ignorance of minimal cases of fraud instances [5]. Oversampling and undersampling of the class instances are feasible options for balancing the attribute. However, these sampling techniques are susceptible to overfitting and data loss [6]. Hence, there is a need to devise better algorithms for detecting imbalanced fraud instances to apprehend the vibrant conduct of an impostor.

Based on these observations, this study aims to identify fraud instances from credit card transactions. Initially, credit card fraud dataset is downloaded from Kaggle data repository. This dataset is further subjected to feature reduction techniques to identify relevant attributes. These attributes are further subjected for balancing the skewed fraud instances using SMOTE algorithm. To further determine the predictive performance of the balanced data, deep learning algorithm is employed. This classifier considers the output from SMOTE algorithm as input to deep network, to generate an enhanced classifier, SMOTEDeep. The predictive performance of SMOTEDeep is improved as it learns effectively from previous classifiers (i.e. SMOTE and deep learning) resulting in Area Under the Curve (AUC) threshold of 0.964.

II. METHODOLOGY

A. Identifying the credit card fraud dataset -

The credit card fraud dataset is collected and analyzed from Kaggle data repository. The dataset comprises of 2, 84,807 instances of credit card transactions from European customers [7]. The dataset includes 28 financial attributes along with the class attribute. The class variable includes 492 instances of fraud out of 2, 84, 807 transactions, which accounts to 0.172% of the class variable. These fraud instances clearly highlight the imbalanced nature of this dataset.

B. Feature reduction -

It is difficult to build a predictive model for a dataset having large number of instances (i.e. 28 in this data). Hence, feature reduction techniques are employed on the credit card dataset for selecting relevant attributes using a two-fold approach. The correlated features are initially removed from the dataset based on the pre-defined threshold value of 0.75. After removing the correlated features, the credit dataset is once again subjected for feature reduction by employing

wrapper-based method, Boruta [8]. The reduced features at the end of this process are used for classifying the fraud instances.

C. Balancing the imbalanced instances using SMOTE

The imbalanced fraud data instances are balanced using oversampling technique, SMOTE [9]. The minority based oversampling classifier balances the fraud and non-fraud instances in the dataset resulting in a balanced distribution of the class attribute.

D. SMOTEDeep Implementation -

Outcome from SMOTE algorithm is fed to a deep network to develop an enhanced classifier. Based on the characteristics of the link in SMOTE evaluation, this algorithm classifies data instances as fraudulent or legitimate. Predictive ability of the ensemble learner is estimated and evaluated.

II. RESULTS AND DISCUSSION

The methodology adopted for detection of credit card fraud detection is shown in Fig. 1.

A. Feature selection and data spliting -

The credit card fraud data collected from Kaggle data repository is initially subjected to two way feature reduction process. Correlation based filter is applied on the dataset to eliminate correlated attributes above the pre-defined threshold of 0.75. Eight features are removed from the dataset resulting in 20 features. These 20 features are once again subjected to wrapper based feature reduction via Boruta algorithm available in R programming language. The algorithm identifies eight features after 166 iterations as significant ones. These eight features are enlisted in Table 1 along with their importance scores. Their distributions are depicted in Fig. 2. The reduced dataset with eight features is further subdivided into training (75%) and test (25%) datasets.

B. Oversampling the imbalanced data using SMOTE -

Fraud data instances are to be balanced with the legitimate instances in the credit card dataset prior to classification. Hence, oversampling is performed on the fraud instances using SMOTE algorithm. The algorithm analyzes the link information from the dataset to balance the class attribute. After oversampling, positive and negative fraud instances are matched. This balanced credit card fraud dataset is employed for classification. The credit data at different stages is depicted pictorially in Fig. 3.

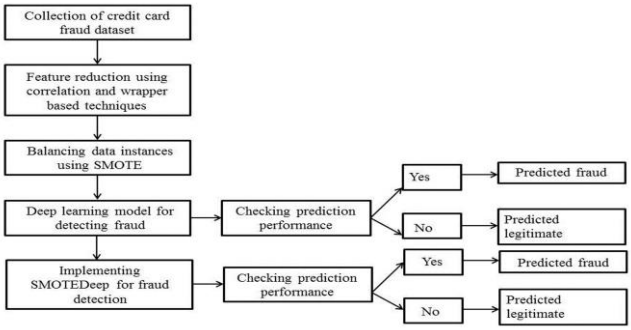

Fig. 1. The pipeline of credit card fraud detection

TABLE I. Features selected by Boruta algorithm after two-fold approach

Sl. No	Data attributes	Importance score
1.	V3	60.89
2.	Amount	58.98
3.	V6	49.99
4.	V4	45.61
5.	V12	42.29
6.	V10	40.09
7.	V14	39.92
8.	V17	38.85

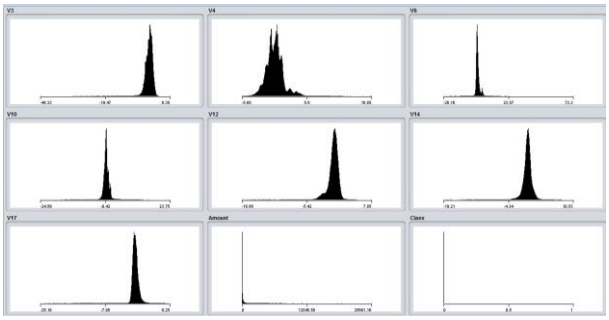

Fig.2. Distribution of various data parameters

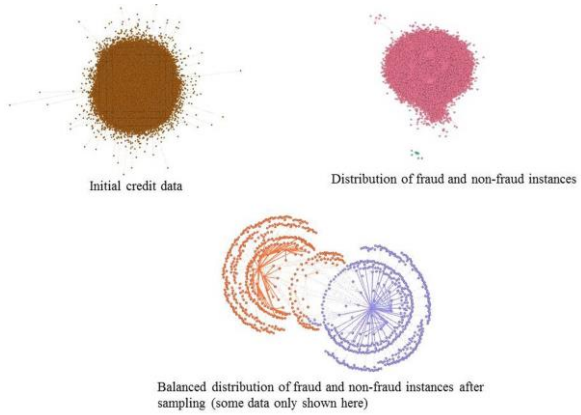

Fig. 3. Representation of fraud data instances at different stages, showing instances of fraud and non-fraud instances

C. Classification using SMOTEDeep -

The balanced credit card fraud training data is subjected to classification using deep networks. The output from SMOTE is fed as input to the deep learner, hence the name SMOTEDeep. This algorithm is considered suitable for this study based on the capability of the model to learn from already balanced instances [10]. The algorithm is evaluated using 10-fold cross validation on test data to determine its predictive ability. It is found that this classifier achieves enhanced performance with 2 input layers, 68 hidden layers with a minimal sum of error (MSE) of 0.035. The performance of this algorithm is determined using the statistical metrics defined below:

True positive = the occurrences where SMOTEDeep classifier classifies fraud instances as fraud

False positive = the occurrences where SMOTEDeep classifier classifies the legitimate instances as fraud

True negative = the occurrences where SMOTEDeep classifier classifies legitimate instances as legitimate

False negative =the occurrences where SMOTEDeep classifier classifies legitimate instances as fraud

Based on these values, the confusion matrix and Receiver Operating Curve (ROC) curve are obtained. They are shown in Table 2 and Fig.4 respectively. The ROC curve is plotted as a function of true positive rate (TPR) and false positive rate (FPR).

TABLE II: The confusion matrix

	True positive	False negative
False positive	1, 99, 076	4999
True negative	5001	75,731

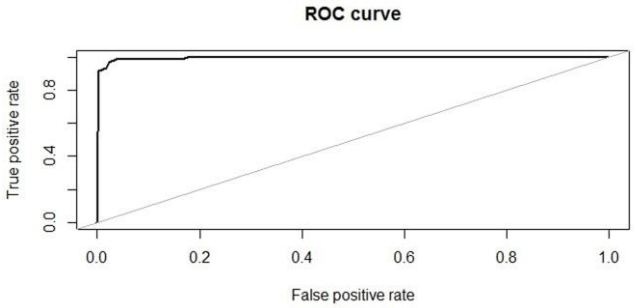

Fig. 4. The performance of SMOTEDeep shown in ROC curve indicating its predictive performance

As seen from the figure, the algorithm achieves increased area under the curve (AUC) metric of 0.964. These results indicate that SMOTEDeep performs superior classification of fraudulent and non-fraudulent instances.

III. CONCLUSION

This study focuses on developing link based classifier for identifying fraud instances form the credit card dataset. Initially the dataset is separated based on its link information into two distinct classes: fraud and legitimate. Based on the occurrences of these instances, SMOTE based oversampling is performed on the fraud attributes as they are minimal compared to the legitimate ones. The balanced dataset is then subjected to deep neural network for classifying the fraudulent cases. After cross validation, the algorithm classified 96.4% of the fraudulent cases effectively. Thereby, this study reflects the light on exploring link dynamics to identify interesting patterns of fraud in credit card transactions.

IV. REFERENCES

[1] M. A. Sirbu, "Credits and debits on the Internet," *IEEE Spectrum*, vol. 34, no. 2, pp. 23–29, 1997.

[2] L. Vasiu, M. Warren, and D. Mackay, "Defining Fraud: Issues for Organizations from an Information Systems Perspective," in *7th Pacific Asia Conference on Information Systems*, 2003, pp. 971–979.

[3] Experian, "The 2018 Global Fraud and Identity Report," 2018, Accessed at: https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf.

[4] J. J. Xu and H. Chen, "The topology of dark networks," *Communications of the ACM*, vol. 51, no. 10, pp. 58–65, 2008.

[5] P. Juszczak, N. M. Adams, D. J. Hand, C. Whitrow, and D. J. Weston, "Off-the-peg and bespoke classifiers for fraud detection," *Computational Statistics & Data Analysis*, vol. 52, no. 9, pp. 4521–4532, 2008.

[6] B. S. Alexander Yun-chung Liu, "The Effect of Oversampling and Undersampling on Classifying Imbalanced Text Datasets," 2004.

[7] A. D. Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating Probability with Undersampling for Unbalanced Classification," in *Symposium on Computational Intelligence and Data Mining*, 2015, pp. 159–166.

[8] M. B. Kursa, "Wrapper Algorithm for All Relevant Feature Selection," 2018, Retrieved from: https://cran.r-project.org/web/packages/Boruta/Boruta.pdf

[9] 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, pp. 321–357, 2002.

[10] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature Review*, vol. 521, pp. 436–444, 2015.