Intelligent Transaction System for Fraud Detection using Deep Learning Networks

Intelligent Transaction System for Fraud Detection using Deep Learning Networks

J Fenila Naomi[1], Roshan Jeniel R[1], Sakthi Eswaran K[1], Sanjeev Kumaar N M[1]

[1]Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India
naomijoseph26@gmail.com

Abstract. Detecting online transaction fraud is a basic study of the new era of electronic transactions. Because the payment patterns of customers and the fraud behaviour of offenders are continually changing, improving the consistency of the fraud detection model and ensuring its stability is exceedingly challenging. In this report, we will look at We concentrate on acquiring deep feature representations of legal and fraud transactions from the perspective of a deep neural network's loss function in this report. Our aim is to increase the separability and discrimination of features in order to boost the efficiency and stability of our fraud detection platform, with the rapid evolution of the technology, the world is turning to use online transaction instead of cash in their daily life, which opens the door to many new ways for fraudsters to use these cards in a nefarious manner. Global losses are projected to reach $35 billion by 2020, according to the Nilson report. To guarantee that users of these credit cards are secure, the credit card issuer should provide a program that protects them from any threats they can experience. As a result, we illustrate our framework for predicting whether transactions are genuine or illegitimate using Kaggel's IEEE-CIS Fraud Detection dataset. BiLSTM-MaxPooling-BiGRUM is the name of our model. Long bi-directional gated repeated unit and long bi-directional memory term (BiLSTM) are used in axPooling (BiGRU).

Keywords: Online transaction, fraud detection, credit cards, Long bi-directional gated repeated unit and long bi-directional memory (BiLSTM)

1. Introduction

For a long time, online transaction fraudsters and detectors play a complex role. Transaction fraud happens more often than ever before, particularly in today's Internet era, and it causes major financial losses [1]. The Nilson study included an in-depth examination of the global situation around online transaction fraud. Online transaction fraud cost the economy around $21 billion in 2015, around $24 billion in 2016, and more than $27 billion in the year 2017. The rate of global online transaction fraud is expected to rise year after year, reaching $31.67 billion in 2020. As a result, banks and financial service providers may require an automatic online fraud detection mechanism to identify and monitor online transactions. Fraud identification systems are designed to distinguish unusual activity patterns from a vast number of transactional records and then use those patterns to identify or track incoming transactions [2]. Machine learning has shown to be very fruitful at extracting these patterns. To put it another way, a large number of transaction reports may be used to train a high-performing fraud classifier. Despite the fact that supervised learning has been extremely successful in detecting fraudulent transactions, the advancement of transactional fraud analysis technologies will never stop. Small enhancements too will save business a significant amount of money.

There are some problems with the new approach to unsupervised and controlled online fraud identification. Machine learning (ML) methods, to the contrary, were used to forecast automatically distinguishes between suspicious and non-suspicious transactions. using classifiers [3]. As a result, a combination of machine learning and data mining strategies was able to differentiate genuine and non-genuine transactions by learning the patterns of data in a correctly categorized dataset. The most commonly used fraud detection techniques are KNN, NB and SVM. To construct classifiers these techniques may can be used on its own or in combination with techniques for group or meta learning.

To enhance the distinguishability of the functions that are trained ,a new functionality for loss called ACL is proposed. Since it resolves the issue of maximal angle separation, ACL is an optimised SL feature. By combining ACL and DCL, we create a new FCL.By taking into account the distance and angle of transaction features, FCL guarantees a greater potential to map initial transaction attributes into even more discrete deep representations [4]. Using two huge data sets, we describe the state-of-the-art loss functionality used for deep representation learning approaches and compare them to ours. We also prove that our model is more accurate in terms of performance [5].

2. Literature Survey

[6-8] in the suggested Markov process structures are unfit for representing the habits. We are proposing BP's abstract Graph (LGBP) as a full command-based paradigm for representing the reasoning relationship between transaction record attributes in this paper. Using transaction of LGBP and user's info, we are able to measure a route dependent conversion Probability from one attribute to the next. Simultaneously, we define a diversity coefficient dependent on knowledge entropy to measure a user's transaction behaviour diversity. We also describe transition probability matrix to capture the time attributes of a user's transactions. As the result, we will build a BP for each user to use it decide whether or not an incoming transaction is valid. Our analyses show that our process outscoring three other oneness models on real data set.

[9] There are three significant contributions in their work. First, with the assistance of a business associate, we propose formalisation of the issue of fraud detection specifically describes the working FDSs' conditions that analyse vast streams of online transactions on a regular basis. We'll show you how to use the most successful performance criteria for detecting fraud. Secondly, we develop and we test a novel education approach to address issues. Thirdly, We show how class has an influence. imbalance and concept swing in our studies using a about 75 million purchases in real-world results accepted over a three-year span.

[10] The latest developments in probabilistic simulations, auto encoders, deep learning, and auto encoders are discussed in this summary of recent research in the field of deep learning and unsupervised learning. This raise concerns over the best targets for researching computing representations, such as inference and geometrical representations, as well as the long-term relationships among representation learning, density estimation, and manifold learning.

[11] Without any modifications, the suggested method can be used to solve both binary and multi-class problems. We also do not change the original data distribution, unlike data-level approaches, resulting in a lower computing cost during planning. Our findings indicates that the proposed strategy outperforms reference algorithms by a significant margin on six massive image classification datasets. Comparing with traditional methods and the cost sensitive classifiers displays the superior efficiency of our the alternative suggested.

3. Proposed Methodology

Furthermore, owing to the accelerated spread of emerging technology in all sectors, most enterprises and organisations are moving their activities to online platforms [12]. Thus, internet transactions necessitate the use of online transaction in order to access facilities and complete transactions in such a timely and effective fashion that using cash payment will be complicated and time-consuming [13]. Online payments excluding, on the other hand, vulnerable cyber criminals who engage in online transaction theft. Fraudsters commit fraud by obtaining unauthorized entry to online transaction records, resulting in financial damages for the business and customer as well [14]. As a function of the threats posed by illegal operations, the demand for online transaction fraud detection systems has increased. The researchers are attempting to develop fraud detection technologies that uses deep learning, data mining and machine learning techniques to determine whether the online transactions are real or fake based on the transaction databases. However, the detection of online transaction fraud is getting more and more difficult as illegal payments becomes closer to legitimate ones [15].

Using Kaggle's IEEE-CIS dataset for online transaction fraud detection, we show deep learning and deep machine models to give solution to the problem of online frauds in transaction. This implementation of a online-fraud detection model is based on a DLMNN classifier is the research's main contribution. Finally, we're contrasting the results of the new model to existing models. Model efficiency is measured using product performance metrics such as accuracy, recall, and F1-Score.

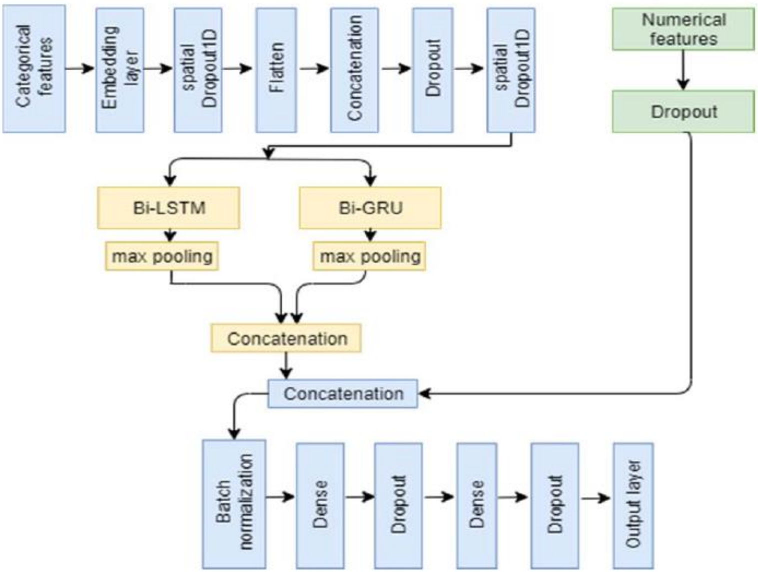

Figure 1. Fraud transaction detection model

Figure.1 shows two facets of the fraudulent transaction perception model described in our model: For achieving distinct and discriminative interpretations, DNN model layers like CNN for example are used, and for the purpose of supervising training of the model, a fully central loss layer. By improving loss function, the aim of this article is to improve the efficiency of those studied deep features as well as the efficiency of fraudulent transactional perception. The learning of deep convolutional neural neural network that maps the actual feature vectors of transactions into a deep feature vector is supervised by the loss functionality. The objective is to keep the transactions with the same class as close together as possible while keeping the transactions of various different classes as far as possible. To do the same, we devised an FCL that incorporates the two kinds of loss: ACL is used to deal with transaction interpretability through classes, while DCL is used to cope with transaction symmetry inside the same class. The method of developing an online transaction fraud identification model is depicted in Figure 2.

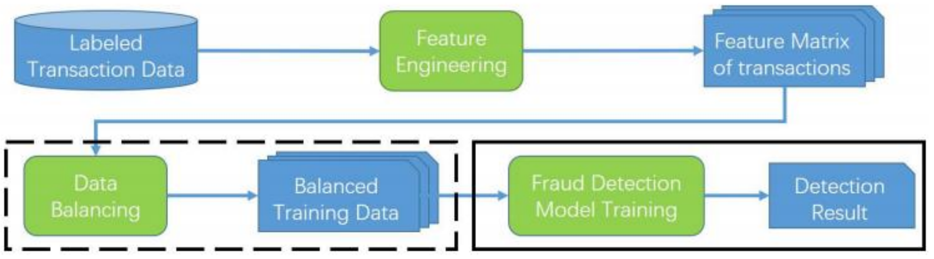

Figure 2. Online transaction fraud detection model

4. Model Evaluation Metrics

We used a number of metrics to determine how well the proposed model worked. Since the dataset used in this analysis was heavily distorted, depending exclusively on the accuracy parameter to determine the model's output would be inadequate. Our work was evaluated using a number of measurement criteria.

The AUC score is a binary classification or multi-label classification implementation in which calculation scores are used to quantify the area under the receiver's working characteristic curve, and then the average curve. is resulted using many methods, including macro, micro, samples and weighted macro default. This can also measured using scikit-learn metrics as in (1 and 2):

$$False\ Positive\ Rate = \frac{FP}{(FP+TN)} \tag{1}$$

$$False\ Positive\ Rate = \frac{TP}{(TP+FN)} \tag{2}$$

Precision is measured by dividing the total amount of true positive by the total amount of true positive and false positive. The total No. of positive class value forecasts divided by the total No. of approving forecasts is how we can define it. The recall is calculated by the division of total No. of true positives as dividend to the total number of true positive and false negative as divisors, for the number of positive predictions divided by the number of positive class values in the test data, the recall value is processed. It's also known as the True Positive Rate or Sensitivity. The F1 score seeks the right mix of accuracy and recall. You will use the following equations (3) to calculate:

$$False\ Positive\ Rate = 2 * \frac{(Precision*Recall)}{(Precision+Recall)} \tag{3}$$

5. Conclusion

In this report, for online transaction fraud detection, deep Representation of Learning Model is proposed, which has the benefit of achieving strong and stable results. On the IEEE-CIS Fraudulent Detection datasets, we used a computer machine and deep learning function to determine if an online digital transaction is genuine or fraudulent, and we created our online transaction fraud detection model. Undersampling, oversampling, and SMOTE were among the approaches studied to work with strongly imbalanced datasets. Model efficiency is evaluated using a series of measurement criteria. Higher the area under the curve was achieved it is by strong polling upsampling and downsampling techniques, according to the results of machine learning classifiers, which were 80 percent and 81 percent respectively. Machine learning classification algorithms, on the other hand, did not do well relative to our model with an auc of 91.37 per cent.

References

[1] L. Zheng, G. Liu, C. Yan, and C. Jiang, Transaction fraud detection based on total order relation and behavior diversity, IEEE Trans. Comput. Soc. Syst., vol. 5, no. 3, pp. 796–806, Sep. 2018.

[2] A. D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, Online transaction fraud detection: A realistic modeling and a novel learning strategy, IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 8, pp. 3784–3797, Sep. 2018.

[3] S. H. Khan, M. Hayat, M. Bennamoun, F. A. Sohel, and R. Togneri, Cost-sensitive learning of deep feature representations from imbalanced data, IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 8, pp. 3573–3587, Aug. 2018.

[4] Y. Bengio, A. Courville, and P. Vincent, Representation learning: A review and new perspectives, IEEE Trans. Pattern Anal. Mach. Intell., vol. 35, no. 8, pp. 1798–1828, Aug. 2013.

[5] H. Yao, S. Zhang, R. Hong, Y. Zhang, C. Xu, and Q. Tian, Deep representation learning with part loss for person re-identification, IEEE Trans. Image Process., vol. 28, no. 6, pp. 2860–2871, Jun. 2019.

[6] X. Wu, R. He, Z. Sun, and T. Tan, A light CNN for deep face representation with noisy labels, IEEE Trans. Inf. Forensics Security, vol. 13, no. 11, pp. 2884–2896, Nov. 2018.

[7] Y. Wen, K. Zhang, Z. Li, and Y. Qiao, A discriminative feature learning approach for deep face recognition, in Proc. Eur. Conf. Comput. Vis. (ECCV). Cham, Switzerland: Springer, 2016, pp. 499–515.

[8] J. Dorronsoro, F. Ginel, C. Sgnchez, and C. Cruz, Neural fraud detection in credit card operations, IEEE Trans. Neural Netw., vol. 8, no. 4, pp. 827–834, Jul. 1997.

[9] D. Dighe, S. Patil, and S. Kokate, Detection of credit card fraud transactions using machine learning algorithms and neural networks: A comparative study, in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). IEEE, 2018, pp. 1–6.

[10] M. Puh and L. Brkic´, Detecting credit card fraud using selected machine learning algorithms, in 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2019, pp. 1250–1255.

[11] M. Suganya and H. Anandakumar, Handover based spectrum allocation in cognitive radio networks, 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), Dec. 2013.doi:10.1109/icgce.2013.6823431. doi:10.4018/978-1-5225-5246-8.ch012

[12] Haldorai and A. Ramu, An Intelligent-Based Wavelet Classifier for Accurate Prediction of Breast Cancer, Intelligent Multidimensional Data and Image Processing, pp. 306–319.

[13] D. Malekian and M. R. Hashemi, An adaptive profile based fraud detection framework for handling concept drift, in Proc. 10th Int. ISC Conf. Inf. Secur. Cryptol. (ISCISC), Aug. 2013, pp. 1–6.

[14] A. Krizhevsky, I. Sutskever, and G. E. Hinton, ImageNet classification with deep convolutional neural networks, in Proc. Adv. Neural Inf. Process. Syst., 2012, pp. 1097–1105.

[15] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, ImageNet: A large-scale hierarchical image database, in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2009, pp. 248–255.