Credit Card Fraud Detection Using LSTM

D.N.Bindu
Department of E.C.E
R.V.R and J.C College of Engineering
dnbindu2002@gmail.com

A.Bhanu Srikar Reddy
Department of E.C.E
R.V.R and J.C College of Engineering
abhanuabhanu9@gmail.com

B.Divya Datta
Department of E.C.E
R.V.R and J.C College of Engineering
bonthudivyadatta194@gmail.com

1 Abstract

As credit card becomes the most popular payment mode particularly in the online sector, the fraudulent activities using credit card payment technologies are rapidly increasing as a result. The purpose of this work is to develop a novel system for credit card fraud detection based on sequential modeling of data, using attention mechanism Long Short Term Memory(LSTM) deep Recurrent Neural Networks(RNN) and Synthetic Minority Oversampling Technique Edited Nearest Neighbour(SMOTE-ENN). The proposed approach aims to capture the historic purchase behavior of credit card holders with the goal of improving fraud detection accuracy on new incoming transactions. Experiments show that our proposed model gives strong results and its accuracy is quite high.

keywords: Credit Card, SMOTE-ENN, FraudDetection, Machine learning,LSTM.

2 Introduction

In recent years, credit card transactions have been set as the most popular payment mode thanks to the improvement of technology and the emergence of new e-service payment solutions, such as e-commerce and mobile payments. However, credit card fraud has also increased with the advent of these new technologies. Growing credit card fraud is nothing but an unauthorized transaction carried out by an unauthorized person without the knowledge of card owner[1,2]. Fraud detection methods are constantly being developed to prevent criminals from adapting to their fraudulent tactics[2]. These crimes are classified as:

* Credit Card Fraud: Online and Offline

* Card theft

* Device Login

* Application Fraud

* Fake Card

* Communication Fraud

The security of card payments and the trust of consumers in making card payments is a matter of concern for any bank in the world. According to the statistics published by the Nilson Report site in 2017, the financial losses caused by credit card fraud were amounted to 24.71 billion dollar in 2016 and 27.69 billion dollar in 2017[3]. Despite developing advanced technologies to prevent fraud, such as the use of chip and pin verification, 3-D Secure for on- line transactions and security questions for internet banking, traditional machine learning models used to automate detection of fraud are inadequate, as they fail to predict whether a transaction is fraudulent or not[4].The decesion is extremely challenging because of the following reasons:

1. Enormous Data is processed every day and the model build must be fast enough to respond to the scam in time.

2. Imbalanced Data i.e most of the transac-tions (99.8 percentage) are not fraudulent which makes it really hard for detecting the fraudulent ones.

3. Data availability is not much more as the data is mostly private.

4. Misclassified Data can be another major issue, as not every fraudulent transaction is caught and reported.

5. Adaptive techniques used against the model by the scammers.

DOI: 10.55041/IJSREM18428

In these situations, the implementation of an accurate fraud detection system that adapts to new fraud behaviors and evolves continuously is of crucial importance for financial institutions in order to pre- vent fraud before it occurs, protect consumers' inter- ests and reduce the damages caused by fraud.In this project, we propose a new credit card fraud detection system based on Long Short-Term Memory (LSTM) networks to predict the fraudulent behavior of credit card transactions and deliver good fraud detection performance. In the process, we implement an effective feature engineering method via resampling of the imbalanced data using the SMOTE-ENN technique. We provide the experimental results to validate the effectiveness of our approach.
The rest of this work is structured as follows: Section 3 discusses the credit card fraud detection dataset, together with the conventional LSTM techniques and SMOTE-ENN. Section 4 presents the results and discussions while Section 5 concludes the paper and provides future research direction.

3 Background

3.1 Dataset

This research utilizes the well-known credit card fraud detection dataset[5]. The dataset was prepared by the University Libre de Bruxelles (ULB) Machine Learning Group on big data mining and fraud detection. The dataset contains credit card transactions performed within two days in September 2013 by European credit card clients. The dataset is imbalanced, with only 492 fraudulent transactions out of 284807. Meanwhile, all the attributes except "Time" and "Amount" are numerical due to the transformation carried out on the dataset, and they are coded as V1, V2, . . . , V28 for confidentiality reasons. The "Amount" attribute is the cost of the transac- tion and the "Time" attribute is the seconds that elapsed between a transaction and the first transac- tion in the dataset. Lastly, the attribute "Class" is the dependent variable, and it has a value of 1 for fraudulent transactions and 0 for legitimate transactions.

3.2 LONG SHORT TERM MEMORY NEURAL NETWORK

Long Short-Term Memory(LSTM) neural network is a special type of artificial Recurrent Neural Network (RNN) architecture used to model time series infor- mation in the field of deep learning that has achieved excellent performance in learning long-term depen- dencies and avoids the gradient disappearance prob- lem[2]. LSTM consists of a memory cell c_t to remem- ber the previous information and three types of gates that controls how the historical information is used and processed. The three gates are forget gate f_t, input gate X_t and output gate h_t. Gates are introduced in order to limit the information. ouput will be in the range of 0-1. The second sigmoid layer is the input gate that decides what new information is to be added to the cell.It takes two inputs h_{t-1} and x_t .The tanh layer creates a vector c_t of the new candidate values. Their point-wise multiplication (i_t , c_t) tells us the amount of information to be added to the cell state. The result is then added with the result for the forget gate multiplied with previous cell state(f_t * c_{t-1}) to produce current cell state c_t. The sigmoid layer decides which part of the cell will present in the output whereas tanh layer shifts the output in the range of [-1,1].Figure 1 depicts the LSTM unit structure.

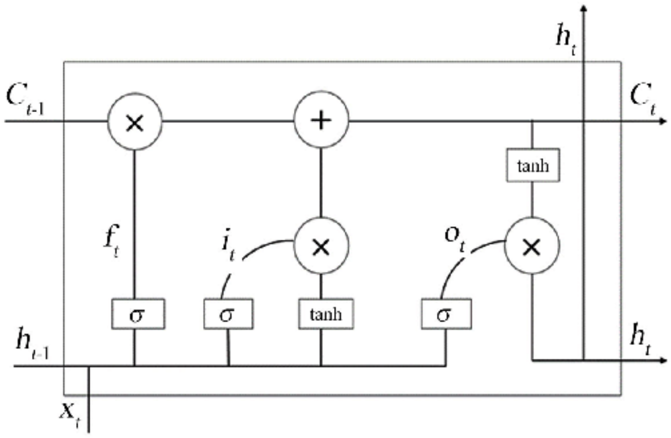

Figure 1: LSTM PROCESS

The LSTM layers are updated using the following equations:

$$\boldsymbol{i}_t = \sigma(\mathrm{w}_{\boldsymbol{i}}[h_{t-1}, x_t] + bi) \cdots$$
$$(1)\ \boldsymbol{f}_t = \sigma(\mathrm{w}_{\boldsymbol{i}}[h_{t-1}, x_t] + b_{\boldsymbol{f}}) \cdots$$
$$(2)\ o_t = \sigma(\mathrm{W}_o[h_{t-1}, x_t] + b_o) \cdot\cdot$$
$$\cdot\ (3)$$

where
i_t- > represents input gate
f_t- > represents forget gate
o_t- > represents output gate
w_x -> represents weight for the respective gate(x) neurons
h_{t-1} -> represents output of the previous LSTM block
x_t- > input at current timestamp
b_x-> biases for the respective gates (x)
An LSTM cell serves as a memory to write, read, and delete information depending on the decisions given by the input, output, and forget gates, respectively[4].

3.3 SYNTHETIC MINORITY OVERSAMPLING TECHNIQUE AND EDITED NEAREST NEIGHBOUR (SMOTE- ENN)

The credit card dataset used in the study is highly imbalanced, leading to poor performance when used to build ML models. The synthetic minority oversampling technique (SMOTE) is widely used in solving the imbalanced class problem. Figure-2 represents the flow chart of how SMOTE-ENN works. SMOTE (synthetic minority oversampling technique) is one of the most commonly used oversampling methods to solve the imbalance problem. It aims to balance class distribution by randomly increasing minority class examples by replicating them.

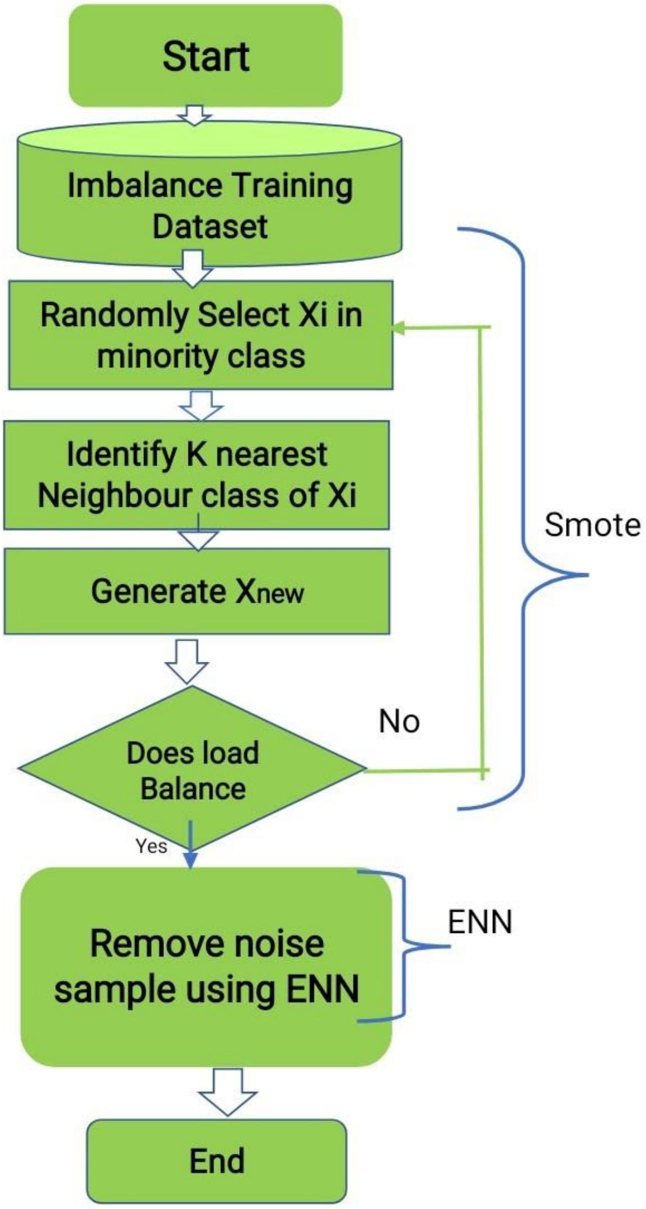
Start
Imbalance Training Dataset
Randomly Select Xi in minority class
Identify K nearest Neighbour class of Xi
Generate Xnew
Does load Balance
No
Yes
Smote
Remove noise sample using ENN
ENN
End

Figure 2: SMOTE-ENN flowchart

SMOTE synthesises new minority instances between existing minority instances. It generates the virtual training records by linear interpolation for the minority class[6,7]. After the oversampling process, the data is reconstructed and several classification models can be applied for the processed data. ENN is an under-sampling technique. It aims to balance class distribution by randomly eliminating majority class examples. When instances of two different classes are very close to each other, we remove the instances of the majority class to increase the spaces between the two classes. This helps in the classification process. To prevent problem of information loss in most undersampling techniques, near-neighbor methods are widely used[6].

Therefore, the proposed credit card fraud detection model employs the synthetic minority oversampling technique and edited nearest neighbor (SMOTE-ENN) method to obtain a balanced dataset. The SMOTE-ENN is a hybrid resampling technique that performs both oversampling and undersampling of the data. It uses SMOTE to oversample the minority class samples and ENN to remove overlapping instances. This algorithm employs the neighborhood cleaning rule from the ENN to remove examples that differ from two in the three nearest neighbors[7].

4 RESULTS AND DISCUSSION

The proposed LSTM ensemble is benchmarked against some classifiers, including the SVM, MLP, decision tree, LSTM, and the traditional AdaBoost[8]. We performed experiments using the original and resampled datasets to demonstrate the impact of the SMOTE-ENN resampling technique on the performance of the various classifiers. Meanwhile, we used the Python programming language and its associated machine learning libraries for all the experiments.

The performance of the models is evaluated using the following performance evaluation metrics: sensitivity, specificity and accuracy. Sensitivity, also called recall, indicates the proportion of fraud samples correctly predicted by the classifier. In contrast, specificity (true negative rate) is the proportion of legitimate transactions predicted correctly by the classifier[9]. From the experimental results, the proposed method obtained a sensitivity of 0.9885,specificity of 0.8891, and accuracy of 0.9368. The sensitivity, specificity and accuracy can be represented mathematically as:

$$Sensitivity = \frac{TP}{TP + FN}$$

$$Specificity = \frac{TN}{TP + FP}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

where

· True positive (TP) represents an instance where a trans- action is fraudulent, and the classifiers correctly classify it as fraudulent.

- True negative (TN) denotes an instance where a transaction is legitimate, and the classifiers cor-rectly predict it as legitimate.

- False-positive (FP) represents a case where a transaction is legitimate, and the classifier classifies it as fraudulent.

- False-negative (FN) is an instance where a fraudulent transaction is wrongly classified as legitimate.

5 conclusion

Recently, machine learning has been crucial in detecting credit card fraud, though the class imbalance has been a significant challenge. This paper proposed an efficient approach for credit card fraud detection. Firstly, the SMOTE- ENN technique was employed to create a balanced dataset. Secondly, a robust deep learning ensemble was developed using the LSTM neural network. From the experimental results, using the well-known credit card fraud detection dataset, the proposed LSTM ensemble with SMOTE-ENN data resampling achieved a sensitivity of 98.85%, a specificity of 88.91%, and an acuracy of 93.68%, which is superior to the other benchmark algorithms and state-of-the-art methods. Therefore, combining the SMOTE-ENN data resampling tech- nique and the boosted LSTM classifier is an efficient method in detecting fraud in credit card transac- tions. Future research would consider more resam- pling techniques and improved feature selection tech- niques for enhanced classification performance.

References

1. EBENEZER ESENOGHO, IBOMOIYE DO- MOR MIENYE, THEO G. SWART AND GEORGE OBAIDO,”Neural Network ensem- ble with featured Engineering for Improved Credit Card” VOLUME 10, 2022, IEEE Ac- cess.

2. Sharayu Pradeep Gulhane, Nitin N.Mandaogade, ”Credit Card Fraud Detection using Hidden Markov Model”, International Journal for Modern Trends in Science and Technology,8(04):106-109,2022.

3. H. Tingfei, C. Guangquan, and H. Kuihua, ”Using variational auto encoding in credit card fraud detection,” IEEE Access, vol. 8, pp. 149841–149853, 2020.

4. Ibtissam Benchaji,Samira Douzi,Bouabid El Ouahidi and Jaafar Jaafari,”Enhanced credit card fraud detection based on attention mechanism and LSTM deep model”, Journal Of BigData 8,Article number:151(2021).

5. Credit Card Fraud Detection. Accessed: Oct. 2021, 26. [Online]. Available: https://kaggle.com/mlg-ulb/creditcardfraud.

6. A. Ishaq, S.Sadiq, M.Umer, S.Ullah, S.Mirjalili, V.Rupapara, and M.Nappi, ”Improving the prediction of heart failure Patients’ survival using SMOTE and effective data mining techniques,” IEEE Access, vol.9,pp. 39707–39716, 2021.

7. Asniar, N.U.Maulidevi, and K.Surendro, ”SMOTE-LOF for noise identification in imbalanced data classification,” J.King Saud Univ. Comput.Inf. Sci., Feb. 2021.

8. S.Subudhi and S.Panigrahi, ”Use of optimized fuzzy C-Means clustering and supervised classifiers for automobile insurance fraud detection,” J.King Saud Univ. Comput. Inf. Sci., vol.32, no.5, pp. 568–575, Jun. 2020

9. S.A.Ebiaredoh-Mienye, E.Esenogho, and T.G.Swart, ”Integrating enhanced sparse autoencoder-based artificial neural network technique and softmax regression for medical diagnosis,” Electronics, vol.9, no.11,pp.1963, Nov. 2020.

10. A. Mishra, C. Ghorpade, “Credit Card Fraud Detection on the Skewed Data Using Various Classification and Ensemble Techniques” 2018 IEEE International Students’ Conference on Electronics ,Electrical and Computer Science (SCEECS) pp. 1-5. IEEE.