Generative Adversarial Neural Networks based Oversampling Technique for Imbalanced Credit Card Dataset

Said El Kafhali
Hassan First University of Settat
Faculty of Sciences and Techniques, IR2M Laboratory,
Settat, Morocco
said.elkafhali@uhp.ac.ma

Mohammed Tayebi
Hassan First University of Settat
Faculty of Sciences and Techniques, IR2M Laboratory,
Settat, Morocco
m.tayebi@uhp.ac.ma

2022 6th SLAAI International Conference on Artificial Intelligence (SLAAI-ICAI) | 978-1-6654-7607-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/SLAAI-ICAI56923.2022.10002630

***Abstract*—The imbalanced dataset is a challenging issue in many classification tasks. Because it leads a machine learning algorithm to poor generalization and performance. The imbalanced dataset is characterized as having a huge difference between the number of samples that contain each class. Unfortunately, various resampling methods are proposed to solve this problem. In our work, we target enhancing the handling of the imbalanced dataset using a new oversampling technique based on generative adversarial neural networks. Our method is benchmarked against the widely used oversampling technique including the synthetic minority oversampling technique (SMOTE), random oversampling technique (ROS), and the adaptive synthetic sampling approach(ADSYN). Additionally, three machine learning algorithms are used for evaluation. The outcome of our experiments on a real-world credit card dataset shows the strong ability of the proposed solution against the competitive oversampling techniques to overcome the imbalanced problem in the European credit card dataset.**

Keywords— Imbalanced classification, oversampling techniques, generative adversarial neural networks

I. Introduction

The detection of abnormal transactions is a classification problem aimed at distinguishing between normal and abnormal transactions [1]. In literature, a lot of work proposed different approaches to solve this problem using the power of machine learning algorithms [2]. Recently, the crime associated to credit card transactions is growing due to the new methods used by fraudsters to steal credit card information [3]. So, it is not unexpected that a large amount of research has been done over many years on the subject of fraud detection, a subdomain of anomaly detection, where the use of machine learning can have a substantial financial impact on businesses suffering from large frauds [4].

Mining extremely uneven data sets are one of the biggest obstacles in knowledge discovery and data mining, especially in the financial context [5]. When a class is more uncommon than other classes, there is a problem with class imbalance. We shall assume that the positive class is the minority class and the negative class is the dominant class without losing generality. Several approaches have been utilized to handle the imbalanced datasets issue [6]. Those methods are divided into two categories: oversampling technique [7]. The mechanism of this method is to reduce the number of the majority classes to have the same number between the two classes [8]. In contrast, the under-sampling technique aims at generating new samples of the minority classes to have the same number of samples between the two classes [9]. In our work, we are targeting enhancing the problem of the imbalanced dataset using generative adversarial neural networks to generate new fraud transaction samples. Those new samples are added to the training dataset [10].

Deep learning is a sub-field of machine learning technique based on artificial neural networks, which is used in supervised learning, semi-supervised learning and unsupervised learning tasks [11]. There are a lot of deep learning architectures such as generative adversarial neural networks [12], deep neural networks [13], convolutional neural networks [14], deep belief networks [15], recurrent neural networks [16], deep reinforcement learning [17], differential evolution [18] and Transformers [19]. These architectures have been applied to solve many complex problems in different domains including computer vision, natural language processing [20], speech recognition [21], bio-informatics [22], drug design [23], medical image analysis [24], machine translation [13], climate science and so on [25]. Generative adversarial neural network (GANs) is a deep learning architecture used in unsupervised tasks [26]. which aims at discovering hidden patterns in a dataset to divide the dataset into clusters. Recently, GANs are utilized to generate new fake samples based on the real dataset. This technique is composed of two components which are the generator which aims at generating a new representation of the dataset [27]. The output of the generator is evaluated using the discriminator.

The main contribution of this work can be demonstrated as follows; the imbalanced dataset is an issue in fraud transaction detection to reach higher performance and efficiency using machine learning algorithms. Many works were conducted to solve this problem using the classical resampling methods and they show different results which

need enhancement. In this paper, we introduce an intelligence approach for handling the imbalanced problem. To achieve this goal we are exploiting the power of one of the strong deep learning architectures in mimicking a representation of a dataset. The utilized model is the generative adversarial neural networks model. For evaluation, a real-world dataset is used and various evaluation metrics are proposed for measurements.

This paper is structured as follows: in section I, an introduction to the credit card transaction problem is presented. In section II, we review important paper published in the field of using generative adversarial networks for fraud transaction detection. Beside, in section III, the implementation of the proposed solution is described. In section IV, the outcome of our experiments is presented. Finally, we conclude with the conclusion and future work.

II. Related work

This section review some important works in detecting fraud transactions using generative adversarial neural network architectures. In [28], the authors presented a novel technique to deal with the imbalanced credit card transactions dataset for detecting fraud transactions. The proposed solution aims at applying a new generative adversarial fusion network architecture to cope with the class imbalance in the used dataset. They compared its performance against a lot of convolutional algorithms and deep learning algorithms. To conclude their solution shows better performance, thus emphasizing the efficiency of their purpose. Likewise, the work proposed in paper [29], implemented an intelligent generative adversarial neural network to enhance the performance of the chosen machine learning classifiers. As a result, based on many experiments conducted, the proposed solution showed promising results and highlighted its strength potential in enhancing the classification of unauthorized transactions.

Another work presented in paper [30], exploits the power of generative adversarial networks for mimicking the data structure. The suggested solution aims at using a new generative adversarial network architecture to solve the imbalanced issue in the credit card dataset. The experimental results demonstrate that the recommended architecture is stable in training and produces more realistic normal transactions in comparison with other GANs. Moreover, the conditional version of GANs in which labels are set by k-means clustering does not necessarily improve the non-conditional versions of GANs. Furthermore, In paper [31], they applied deep learning architecture to solve the issue of imbalanced datasets. Its proposed solution is described as follows; firstly they used a sparse autoencoder (SAE) for obtaining representations of legal transactions and then train a generative adversarial network (GAN) with the obtained representations. Finally, they combined the SAE and the discriminator of GAN and applied them to distinguish between fraud transactions and no fraud samples. The experimental results highlighted the outperforms of their purpose against the other state-of-the-art methods. In work [32], the authors suggested a new oversampling technique by exploiting the generative adversarial network's ability for generating a new representation of a dataset based on historical samples. Its solution was evaluated through comparison with traditional oversampling techniques including,Adaptive Synthetic Sampling, the Synthetic Minority Oversampling Technique, and random oversampling. Moreover, the obtained results prove the superiority of generative adversarial networks for achieving higher performance in detecting fraud transactions.

III. Research methodology

A. Dataset

To evaluate our proposed technique the famous European credit card dataset are proposed [33], this dataset was used for evaluation in many papers, and it is characterized as having 284315 samples. 492 are fraud transactions, which demonstrate the imbalance class in this dataset. Moreover, it contains 31 numerical features named $\left\{V_{i=1}^{21}\right\}$, Time, Amount. and Class which denote the type of the transaction, 0 if it is legitimate otherwise, 1 if it is fraudulent. All features are scaled except Time, and Amount we are using MinMaxscaler to scale them.

B. The proposed oversampling technique

Generative adversarial neural networks (GANs) are a popular research topic recently. That is due to various applications and a lot of research papers that proposed GANs as a solution for many problems. For example in finance, they used GANs to solve the issue of imbalanced credit card transactions. The target of this paper is to propose a GANs architecture for solving the imbalanced issue in our European credit card dataset.

Mathematically, our purpose is formulated as follows, first, we denote the Generator by G , and the Discriminator by D. The goal of GANs is to learn the representation of fraud transactions to generate new fake fraud transactions $G(\sigma) \sim p_{data}$. based on a random distribution $\sigma \sim p_{noise}$, by optimizing the following min-max optimization problem

$$\begin{aligned} &\min_{\omega_G} \max_{\omega_D} E_{\chi \sim p_{data}} \left[\log D(\chi, \omega_g)\right] \\ &+E_{\sigma \sim p_{noise}} \left[\log(1 - D(G(\sigma, \omega_g), \omega_d))\right] \end{aligned} \tag{1}$$

Where, ω_d, ω_g are the parameters of D and G respectively. On the other hand $\log D(\sigma, \omega_g)$ and $\log(1 - D(G(\sigma, \omega_g), \omega_d))$ are two cross-entropy between $[1, 0]^T$. In our model, D aims to predict $D(\chi) = 1$ for real fraud transactions and $D(G(\sigma)) = 0$ for fake fraud transactions generated. the GAN learns how to fool D by finding G which is optimized on hampering the second term in equation 1.

On the first iteration, a minibatch of m noize samples $\left\{\sigma^1, \cdots \sigma^m\right\} \sim p_{noise}$ and a minibatch of m real fraud transactions samples $\left\{\chi^1, \cdots \chi^m\right\} \sim p_{data}$ are sampled. then the discriminator D is updated by ascending its stochastic gradient.

$$\nabla_{\omega_d} \frac{1}{m} \sum_{i=1}^{m} \left[\log D(\chi^i, \omega_d) + \log(1 - D(G(\sigma^i, \omega_g), \omega_d))\right] \tag{2}$$

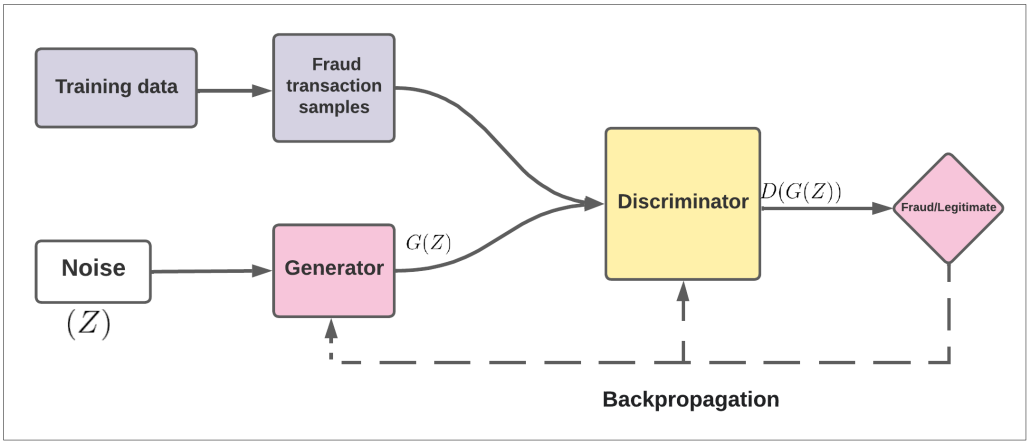

Fig. 1. Architecture of the proposed oversampling methods

In the second iteration a minibatch of noise samples $\{\sigma^1, \cdots \sigma^m\} \sim p_{noise}$ are sampled, then G is updated by descending its stochastic gradient.

$$\nabla_{\omega_g} \frac{1}{m} \sum_{i=1}^{m} \log(1 - D(G(\sigma^i, \omega_g), \omega_d)) \tag{3}$$

this process keeps going until 100 iterations, after that, we generate a random noise and we passed throw G to generate fraud transaction samples then the training dataset is updated by adding these new fraud samples.

C. Metrics

This section introduces the selected measurement for evaluating our proposed solution, those metrics are presented as follows:

- Accuracy: This metric gives an idea about the percentage of transactions correctly classified.

$$Accuracy = \frac{T^{(p)} + T^{(n)}}{T^{(p)} + T^{(n)} + F^{(p)} + F^{(n)}} \tag{4}$$

- Precision: this metric is important in every classification problem. It denotes the percentage of fraud transactions correctly identified.

$$Precision = \frac{T^{(p)}}{T^{(p)} + F^{(p)}} \tag{5}$$

- Sensitivity: is a metric utilized to show how the proposed technique is efficient in classifying normal transactions correctly.

$$Sensitivity = \frac{T^{(p)}}{T^{(p)} + F^{(n)}} \tag{6}$$

- Specificity: is a measure utilized to show the number of legitimate transactions correctly classified as legitimate.

$$Specificity = \frac{T^{(n)}}{T^{(n)} + F^{(p)}} \tag{7}$$

Where
$T^{(n)}$: refers to the number of legal transactions correctly identified,
$F^{(p)}$:is the number of normal transactions that are classified as abnormal transactions
$F^{(n)}$: is the number of fraud transactions classified as normal transactions
$T^{(p)}$ denotes the number of normal transactions correctly classified.

IV. Results and Analysis

The experiments were done for evaluating our oversampling technique and show more important results against the traditional oversampling methods including SMOTE, ROS, and ADSYN. The machine learning utilized for computing are: LightGBM (LBM), XGBoost (XGB), CatBoost (CB). Table I shows the outcome of the conducted experiments, overall we notice that the proposed technique is more beneficial than other techniques. To be more clear, our methods achieved the best Precision score for the machine learning algorithms used. For the XGB classifier, we achieved a percentage of 97.37 percent of fraud transactions correctly classified. Moreover, CB reached the highest Precision score which is 95.57 percent of illegal transactions correctly identified using the proposed technique. Likewise, LBM can classify more than 94.16 percent of fraudulent transactions correctly. To conclude, the discussed results highlighted the utility of our proposed oversampling technique to handle the issue of the imbalanced class in the European credit card dataset.

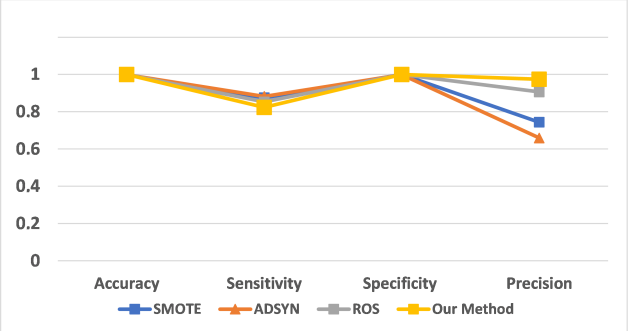

Fig. 2. Performance of XGB using varoius oversampling technique

Figures 2 to 4 show a comparative study using the proposed oversampling technique against traditional methods. From these figures, we reveal that the purpose can enhance the handling of the imbalanced credit card dataset.

TABLE I
PERFORMANCE EVALUATION OF THE PROPOSED SOLUTION USING VARIOUS RESAMPLING METHODS

Classifier	Method	Accuracy	Sensitivity	Specificity	Precision
XGB	SMOTE	0.9993	0.875	0.9995	0.74375
	ADSYN	0.9990	0.8823	0.9992	0.6593
	ROS	0.9996	0.8529	0.9998	0.9062
	Our Method	**0.9996**	**0.8235**	**0.9999**	**0.9739**
CB	SMOTE	0.9988	0.8823	0.9990	0.6
	ADSYN	0.9986	0.9988	0.9992	0.5384
	ROS	0.9994	0.875	0.9996	0.7777
	Our Method	**0.9996**	**0.7941**	**0.9999**	**0.9557**
LBM	SMOTE	0.9985	0.8897	0.9986	0.5193
	ADSYN	0.9977	0.8897	0.9979	0.4074
	ROS	0.9995	0.8676	0.9997	0.8613
	Our Method	**0.9996**	**0.8308**	**0.9999**	**0.9416**

Fig. 3. Performance of CB using varoius oversampling technique

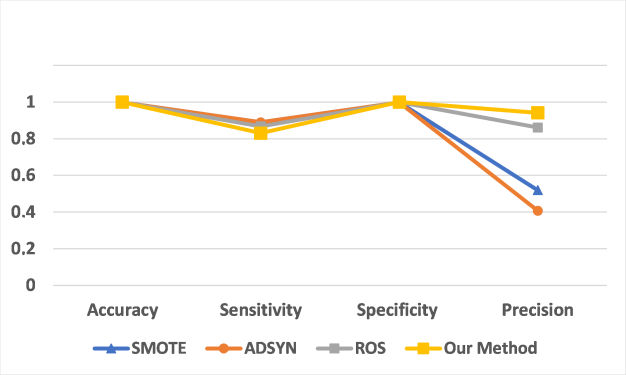

Fig. 4. Performance of LBM using varoius oversampling technique

Additionally, Figure 5, the performance of our oversampling technique on the three machine learning algorithms for detecting fraud transactions. Overall, it is clear that XGB got the highest Precision score which proves the superiority of this model to classify fraud transactions correctly.

V. CONCLUSION AND FUTURE WORKS

Fraud transaction detection became a more important field, due to the largest number of fraud transactions committed every year. As a consequence, a lot of papers are

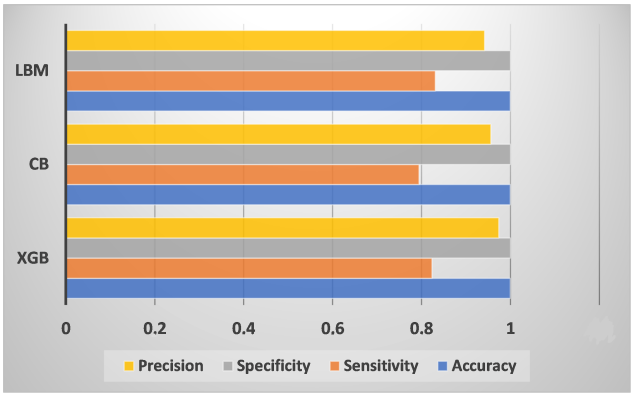

Fig. 5. Performance of our method using various algorithms

published handling this problem based on deep learning and machine learning. Imbalanced class in credit card transactions is another issue that caused the overfitting and led to poor classification and poor performance. In literature, many resampling techniques are presented as a solution. Those techniques are categorized into two categories: oversampling and undersampling techniques. In this paper, a new oversampling technique is implemented based on a generative model. This new oversampling technique exploits the power of generative models to generate a new representation of fraud transactions; those new samples generated are added to the training dataset. Based on the experiments conducted comparing the new technique with three famous oversampling techniques we notice promising results obtained for the three machine learning classifiers used. To conclude, our purpose resampling methods are beneficial and superior to the other oversampling methods in terms of the Precision score. In future work, a modified particle swarm optimization method is proposed for hyperparameters optimization for detecting fraud transactions using recurrent neural networks.

REFERENCES

[1] Bin Sulaiman, R., Schetinin, V., & Sant, P. (2022). Review of Machine Learning Approach on Credit Card Fraud Detection. Human-Centric Intelligent Systems, 1-14.

[2] Roseline, J. F., Naidu, G. B. S. R., Pandi, V. S., alias Rajasree, S. A., & Mageswari, N. (2022). Autonomous credit card fraud detection using machine learning approach. Computers and Electrical Engineering, 102, 108132.

[3] Tayebi, M., & El Kafhali, S. (2022). Deep Neural Networks Hyperparameter Optimization Using Particle Swarm Optimization for Detecting Frauds Transactions. In Advances on Smart and Soft Computing (pp. 507-516). Springer, Singapore.

[4] Lim, K. S., Lee, L. H., & Sim, Y. W. (2021). A review of machine learning algorithms for fraud detection in credit card transaction. International Journal of Computer Science Network Security, 21(9), 31-40.

[5] Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402.

[6] Hemdan, Ezz El-Din, and D. H. Manjaiah. "Anomaly Credit Card Fraud Detection Using Deep Learning." Deep Learning in Data Analytics. Springer, Cham, 2022. 207-217.

[7] Tayebi, M., & El Kafhali, S. (2021, June). Hyperparameter optimization using genetic algorithms to detect frauds transactions. In The International Conference on Artificial Intelligence and Computer Vision (pp. 288-297). Springer, Cham.

[8] Itoo, F., & Singh, S. (2021). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. International Journal of Information Technology, 13(4), 1503-1511.

[9] Tayebi, M., & El Kafhali, S. (2023). Performance analysis of metaheuristics based hyperparameters optimization for fraud transactions detection. Evolutionary Intelligence, 1-19.

[10] Prasetiyo, B., Muslim, M. A., & Baroroh, N. (2021, June). Evaluation performance recall and F2 score of credit card fraud detection unbalanced dataset using SMOTE oversampling technique. In Journal of Physics: Conference Series (Vol. 1918, No. 4, p. 042002). IOP Publishing.

[11] Mehbodniya, A., Alam, I., Pande, S., Neware, R., Rane, K. P., Shabaz, M., & Madhavan, M. V. (2021). Financial fraud detection in healthcare using machine learning and deep learning techniques. Security and Communication Networks, 2021.

[12] Aggarwal, A., Mittal, M., & Battineni, G. (2021). Generative adversarial network: An overview of theory and applications. International Journal of Information Management Data Insights, 1(1), 100004.

[13] Carrasco, R. S. M., & Sicilia-Urbán, M. Á. (2020). Evaluation of deep neural networks for reduction of credit card fraud alerts. IEEE Access, 8, 186421-186432.

[14] Chen, J. I. Z., & Lai, K. L. (2021). Deep convolution neural network model for credit-card fraud detection and alert. Journal of Artificial Intelligence, 3(02), 101-112.

[15] Voican, O. (2021). Credit Card Fraud Detection using Deep Learning Techniques. Informatica Economica, 25(1), 70-85.

[16] Lin, W., Sun, L., Zhong, Q., Liu, C., Feng, J., Ao, X., & Yang, H. (2021). Online Credit Payment Fraud Detection via Structure-Aware Hierarchical Recurrent Neural Network. In IJCAI (pp. 3670-3676).

[17] Dang, T. K., Tran, T. C., Tuan, L. M., & Tiep, M. V. (2021). Machine Learning Based on Resampling Approaches and Deep Reinforcement Learning for Credit Card Fraud Detection Systems. Applied Sciences, 11(21), 10004.

[18] Tayebi, M., & El Kafhali, S. (2022). Credit card fraud detection based on hyperparameters optimization using the differential evolution. International Journal of Information Security and Privacy (IJISP), 16(1), 1-19.

[19] Singh, V., Chen, S. S., Singhania, M., Nanavati, B., & Gupta, A. (2022). How are reinforcement learning and deep learning algorithms used for big data based decision making in financial industries–A review and research agenda. International Journal of Information Management Data Insights, 2(2), 100094.

[20] Maulud, D. H., Zeebaree, S. R., Jacksi, K., Sadeeq, M. A. M., & Sharif, K. H. (2021). State of art for semantic analysis of natural language processing. Qubahan Academic Journal, 1(2), 21-28.

[21] Li, J. (2022). Recent advances in end-to-end automatic speech recognition. APSIPA Transactions on Signal and Information Processing, 11(1).

[22] Gurung, A. B., Ali, M. A., Lee, J., Farah, M. A., & Al-Anazi, K. M. (2021). An updated review of computer-aided drug design and its application to COVID-19. BioMed research international, 2021.

[23] Wang, J., Zhu, H., Wang, S. H., & Zhang, Y. D. (2021). A review of deep learning on medical image analysis. Mobile Networks and Applications, 26(1), 351-380.

[24] Montenegro, H., Silva, W., & Cardoso, J. S. (2021). Privacy-preserving generative adversarial network for case-based explainability in medical image analysis. IEEE Access, 9, 148037-148047.

[25] Boulaguiem, Y., Zscheischler, J., Vignotto, E., van der Wiel, K., & Engelke, S. (2022). Modeling and simulating spatial extremes by combining extreme value theory with generative adversarial networks. Environmental Data Science, E5, 1-18.

[26] Herr, D., Obert, B., & Rosenkranz, M. (2021). Anomaly detection with variational quantum generative adversarial networks. Quantum Science and Technology, 6(4), 045004.

[27] Fajardo, V. A., Findlay, D., Jaiswal, C., Yin, X., Houmanfar, R., Xie, H., ... & Emerson, D. B. (2021). On oversampling imbalanced data with deep conditional generative models. Expert Systems with Applications, 169, 114463.

[28] Lei, K., Xie, Y., Zhong, S., Dai, J., Yang, M., & Shen, Y. (2020). Generative adversarial fusion network for class imbalance credit scoring. Neural Computing and Applications, 32(12), 8451-8462.

[29] Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences, 479, 448-455.

[30] Ba, H. (2019). Improving detection of credit card fraudulent transactions using generative adversarial networks. arXiv preprint arXiv:1907.03355.

[31] Chen, J., Shen, Y., & Ali, R. (2018, November). Credit card fraud detection using sparse autoencoder and generative adversarial network. In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 1054-1059). IEEE.

[32] Gangwar, A. K., & Ravi, V. (2019, December). Wip: Generative adversarial network for oversampling data in credit card fraud detection. In International Conference on Information Systems Security (pp. 123-134). Springer, Cham.

[33] Credit Card Fraud Dataset. [Online]. Available at: https://www.kaggle.com/mlg-ulb/creditcardfraud/data