2024 Second International Conference on Data Science and Information System (ICDSIS)

An Improved Variational Autoencoder Generative Adversarial Network with Convolutional Neural Network for Fraud Financial Transaction Detection

1st Basava Ramanjaneyulu Gudivaka
Raas Infotek
Delaware, USA
basavagudivaka@ieee.org

2nd Muntather Almusawi
Department of Computers Techniques Engineering
College of Technical Engineering
The Islamic University
Najaf, Iraq
muntatheralmusawi@gmail.com

3rd Priyanka M S
Department of AI-ML
Nitte Meenakshi Institute of Technology
Bengaluru, India
priyanka.ms@nmit.ac.in

4th Madhava Rao Dhanda
Department of CSE(AI&ML)
Vignana Bharathi Institute of Technology
Ghatkesar, India
danda.madhav@gmail.com

5th Thanjaivadivel M
Department of Computing & Information Technology
REVA University
Bengaluru, India
thanjaivadivel@gmail.com

***Abstract*—In recent years, the rapid development of e-commerce technologies has made it possible for people to conveniently shop from stores worldwide without leaving their homes. Unfortunately, credit card fraud has become common due to online payments. This fraudulent activity causes significant financial losses, and financial institutions need to install automatic deterrent mechanisms to check these actions. Fraudulent transactions do not follow a specific pattern and continuously change their shape and behavior, making it difficult to detect them. To overcome these problems this paper proposed an improved generator part of the Variational Autoencoder Generative Adversarial Network (VAEGAN) along and introduces a new oversampling method that generates convincing and diverse minority class data. Then in the classification process Convolutional Neural Network (CNN) uses the parameters for the classification process. This enhances fraud detection in the transaction and improves the detection accuracy. The performance of the proposed model is measured in terms of accuracy, precision, recall, and F1-score. This shows that the proposed method outperforms existing methods such as CNN, LightGBM, and Long Short-Term Memory (LSTM) ensemble in terms of accuracy of 99.78%, precision of 88.97%, recall of 95.24, and f1-score of 95.00%.**

Keywords*—Classification, Convolutional Neural Network, Detection, Fraud transaction, Variational Autoencoder Generative Adversarial Network.

I. Introduction

In average schedules use credit cards to purchase products in which includes online payment or actual cards for transactions that are disconnected [1]. This makes the fraudsters to be more active in their attacks on credit card transactions now than before [2]. Due to shortcomings and defensive insecurities in the digital environment, the attack on transactions occur in terms of fraud related issues, anomalous and privacy violation also, the size of the transaction increases the chance of fraud in financial transactions [3] [4]. Most of the researchers used ML algorithms, Neural Networking models, and clustering techniques for the early detection of credit card fraud [5] [6]. These methods not only reduce financial losses but also enhance the customer's faith and assurance [7][8]. In order to minimize fraud in the financial industry there exist many approaches to detecting fraud in transactional processing some of these are; predictive analytics as well as data mining particularly modeling algorithm for instance clustering techniques and anomaly detection [9]. The VAEGAN proposed a novel oversampling technique that produced definite and diverse minority class data and for the classification process CNN uses the parameters. This enhances fraud detection in the transaction and improves the detection accuracy. The main contributions of the research are mentioned as follows;

- Dimensionality reduction in a pre-processing step excludes irrelevant features and noise in an effort to enhance the accuracy the learning features and also reduce the amount of time needed for training.
- As for oversampling techniques, a new technique called the VAEGAN provides enhanced rates of credit card fraud detection for the minority class data, by creating realistic data.
- The credit card fraud detection model using CNN is capable of learning client's spending behavior and transaction sequences.

The remaining portion is organized as: Section 2 indicates the literature survey. Section 3explains about proposed methodology. Section 4 discusses the results. Section 5 contains the overall conclusion of the paper.

II. Literature Review

Fawaz Khaled Alarfaj *et al.* [10] presented Machine Learning (ML) and Deep Learning (DL) algorithms for credit card detection problems. ML algorithms are applied for the dataset which improved accuracy in fraud detection and DL methods like Convolutional Neural Networks (CNN) with its layer to improve performance in fraud detection. This showed better performance than traditional algorithms in fraud detection. However, the class imbalance problem has not been solved which affects the detection in classification process.

Seyedeh Khadijeh Hashemi *et al.* [11] implemented an ML approach for fraud detection in terms of improving performance. LightGBM method improved the performance by accounting for the voting mechanism. Also, performance improved using DL to fine-tune the hyperparameters, particularly for weight-tuning. For unbalanced datasets, the

979-8-3503-8166-5/24/$31.00 ©2024 IEEE

use of recall-precision metrics in addition to the standard ROC-AUC.

Ebenezer Esenogho *et al.* [12] presented an approach to detect credit card fraud using a Neural Network (NN) ensemble classifier and a hybrid data resampling method. The initial model was an ensemble classifier attained that has Long Short-Term Memory (LSTM) in Adaboost, which from the base classifier. Next, hybrid resampling is performed by utilizing Synthetic Minority Oversampling Technique and Edited Nearest Neighbor (SMOTE-ENN) method. Though the SMOTE method has some benefits such as additional information and dimensionality reduction, there are some issues which is not acceptable in banking for customer orientation such as an increase in false positive rate.

Mohammed Rashad Baker *et al.* [13] addressed fraud transactions in credit card using ensemble learning along with supervised ML models. Application of SMOTE approach has been made in dealing with imbalanced dataset with regard to the classes. Different majority voting combination of ML classifiers such as Naïve Bayes (NB), Bagging, Random forest (RF), AdaBoost, Logistic regression (LR), Decision tree (DT), and Support vector machine (SVM) are used. MV ensemble learning method combines the forecasts produced by multiple underlying models into a single prediction output. This approach was found to be superior to any original model used in the approach in terms of total accuracy.

Ibomoiye Domor Mienye *et al.* [14] presented robust DL approach that consists LSTM and Gated Recurrent Unit (GRU). In this work, NN were employed as the base classifiers to build a stacking ensemble model, in which MLP was used as the meta-classifier. The proposed method to balance the class distribution in the dataset was SMOTE-over-sampling combined with ENN technique. This approach was able to yield sensitivity, specificity, and AUC and was better than the sample benchmark classifiers, such as AdaBoost, random forest, MLP, LSTM, and GRU. But the FPR of SMOTE is higher than other measures this leads to a reduction in the detection rates as noted in the classification step.

III. Proposed Methodology

In Fraud transaction detection, the proposed method includes three major stages. The framework includes a dataset description, pre-processing which includes Dimensionality reduction, then VAEGAN oversampling method, and a classification process by CNN. The framework of this paper is shown in Figure 1.

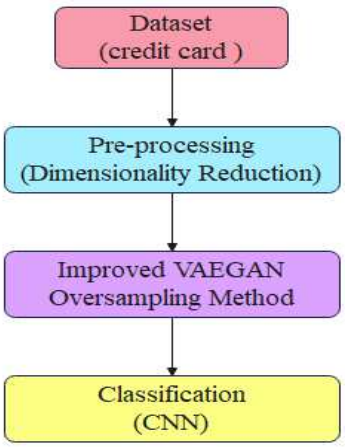

Fig. 1. The framework of the proposed method

A. Dataset description

A developed method is assessed by using the credit card dataset comprising of the transaction of a cardholder over a two-day period, that is, from September 2018 [15]. Overall, there were 284,807 transactions, and 492 of those were fraud transactions, which is 0. 172 percent, were fraudulent. The positive class (frauds) is made up of 0. and revealed that 172% of all transactions; therefore, the current dataset is highly imbalanced. This has only numeric predictor variables derived by applying the Principal Component Analysis (PCA) to original dataset. Alas, the origin of the features and some additional information on the data are missing here because of the principles of confidentiality and privacy.

B. Pre-processing

Dimensionality Reduction is a crucial step in ML that helps to eliminate redundant features, noisy data, and irrelevant data, which leads to better accuracy and shorter training time. Linear Discriminant Analysis (LDA), PCA, and Autoencoder are commonly used techniques for DR. For the autoencoder branch, the features of the dataset were normalized using Min-Max normalization.

C. VAEGAN Oversampling Method

VAEGAN is a category of productive model that integrates abilities of VAE and GAN to learn representation and distribution of samples in latent space using two-step training. The advantage of the VAEGAN has several of them, namely, the trained latent space description is more selective, which allows it to distinguish one data from the other better. Second, generator learns from the strengths of both VAE and GAN in every iteration, thus generating considerably more realistic and different data sets. Finally, representation of the resulting latent vectors in accessible feature spaces enables analysis and interpretation. This was done to determine whether adding extra encoders would help to enhance the accuracy of the oversampling results or whether it was simply the increasing of the number of layers that was the primary beneficial factor. However, the encoder can result in overfitting into a certain extent and affects the effectiveness of the samplings.

Remarkably, fraud credit card data with only 30 dimensions and basic features can be greatly assisted by using two encoders. The initial VAEGAN model incorporates solely one encoder, thus restricting the exposure to the intricate structure of the data as well as having multiple levels of features. This leads to a lack of model and generalization capabilities. At the same time, the representation ability of the latent space is insufficient, meaning there is a low level of sample diversity in the generated region and low realism, which can negatively influence the generalization of the model. To build a better VAEGAN model, one needs to incorporate more encoders, the latent space needs to be enhanced, and the model also has to be made scalable more.

The present method enhances VAEGAN model by incorporating the encoder to VAE segment of original VAEGAN. The data is fed in separately and through encoder E1 and encoder E2. E1 and E2 receive input real data as input and convert them into mean and variance codes separately. This means that the second set of codes known as the mean and variance codes of the second encoder are used to obtain the latent code. Furthermore, decoder develops false

information by decoding latent code. A first phase to be realized is the integration of the second mean and variance by two encoders. VAEGAN are fused by obtaining the product of two normal distribution probability density functions in Eqs (1-6)

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma_1} e^{-\frac{(x-\mu_1)^2}{2\sigma_1^2}} \quad (1)$$

$$g(x) = \frac{1}{\sqrt{2\pi}\sigma_2} e^{-\frac{(x-\mu_2)^2}{2\sigma_2^2}} \quad (2)$$

Multiply (1) & (2)

$$h(x) = A. \frac{1}{\sqrt{2\pi}\sigma_0} e^{-\frac{(x-\mu_0)^2}{2\sigma_0^2}} \quad (3)$$

Value of A is:

$$A = \frac{e^{-\frac{(\mu_1-\mu_2)^2}{2(\sigma_1^2+\sigma_2^2)}}}{\sqrt{2\pi(\sigma_1^2+\sigma_2^2)}} \quad (4)$$

Value of μ_0 is:

$$\mu_0 = \frac{\mu_1\sigma_2^2+\mu_2\sigma_1^2}{\sigma_1^2+\sigma_2^2} \quad (5)$$

Value of σ_0^2:

$$\sigma_0^2 = \frac{\sigma_1^2\sigma_2^2}{\sigma_1^2+\sigma_2^2} \quad (6)$$

Equation (3) defines $h(x)$ as product of a normal distribution $N(\mu_0, \sigma_0^2)$ by a scaling factor A where μ_0 and σ_0^2 are the mean and variance of a normal distribution, achieving that the product of the probability density functions can be represented by another normal distribution $N(\mu_1, \sigma_1^2)$ and $N(\mu_2, \sigma_2^2)$ is also equivalent to $N(\mu_0, \sigma_0^2)$ multiplied by A. When two Gaussian distributions are multiplied, the result is a Gaussian distribution that is scaled. Note that the value of the density function changes based on the chosen random variable for A, but the expected sum of the product variance remains unchanged— implying that post-product distribution relationship is unaffected by A. To merge information on mean and variance encoded by two different encoders such that resulting distribution is still normal, eliminate scale factor A from $h(x)$ to get $h'(x)$ is represented in Eq. (7).

$$h'(x) = \frac{1}{\sqrt{2\pi}\sigma_0} e^{-\frac{(x-\mu_0)^2}{2\sigma_0^2}} \quad (7)$$

D. Convolutional Neural Network (CNN) for Classification

CNN is a DL model that has been designed to solve imaging challenges and its architecture can as well serve the purpose. Like all the neural networks, it is consisted of several layers such as input layer, convolutional layer, pooling layer and output layer. It is worth mentioning that visuals such as images can be effectively learnt since CNN model is accomplished the feature extraction. The input layer of CNN is dedicated linked to the output layer of the CNN through a convolution filter. This filter applies dot multiplication to generate multifractal feature extraction using sliding windows. The max-pooling layer is then employed to help reduce the level of complexity of the feature matrix and the resultant network. Last is convolutional layer which is designed for extracting feature from initial input.

IV. Experimental Results

The experimental analysis is simulated in Windows -10 with 64bit, Intel (R) Xeon (R) CPU processor and RAM – 8 GB. Anaconda Navigator 1.10.0, Python 3.8 and Jupyter Notebook 6.1.4 are the virtual machine are equipped in server. The server utilized the 4 CPU cores and virtual machine used 3 CPU cores with six threats. This paper employed a comprehensive evaluation strategy utilizing four key metrics: precision, accuracy, recall, and f1-score. These metrics provide a calculation of model's performance across various aspects. Equations (8), (9), (10), and (11) are used for performance metrics.

$$Accuracy = \frac{TruePositive+TrueNegative}{TruePositive+TrueNegative+FalsePositive+FalseNegative} \quad (8)$$

$$Precision = \frac{TruePositive}{TruePositive+FalsePositive} \quad (9)$$

$$Recall = \frac{TruePositive}{TruePositive+FalseNegative} \quad (10)$$

$$F1-score = \frac{2*Precision*Sensitivity}{Precision+Sensitivity} \quad (11)$$

A. Performance Analysis

This section shows the performance of fraud financial transaction detection using the credit card dataset. The performance is evaluated for VAEGAN-CNN with other oversampling methods. Table 1. Shows the performance evaluation of the different oversampling method with the proposed method for the fraud transaction in credit card.

TABLE I. Performance Evaluation of Oversampling Method

Oversampling method	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
GAN	80.00	81.62	81.66	79.76
VAE	82.22	83.42	78.09	85.66
SMOTE	87.42	84.86	84.23	87.86
VAEGAN - CNN	99.78	88.97	95.24	95.00

From Table 1, performance of the oversampling method is compared with other methods for performance measures. The present methods are used for classification mechanism are GAN, VAE and SMOTE. Significant accuracy of 99.78%, precision of 88.97%, recall of 95.24% and f1-estimate of 95.00% have been achieved by the mechanism using oversampling method.

B. Comparative analysis

A comparative analysis of with various existing research is shown in this section. Existing research such as CNN [8], LightGBM [9], and LSTM ensemble [10] are used to evaluate an efficacy of proposed approach. Table 2 Shows the comparison of with other models and it is shown that performance of this proposed technique is enhanced than the other models.

TABLE II. PERFORMANCE EVALUATION OF VAEGAN- CNN WITH DIFFERENT METHODS

Method	Precision (%)	F1-score (%)	Recall (%)	Accuracy (%)
CNN [10]	NA	NA	NA	93.00
LightGBM [11]	79.00	76.90	NA	99.00
LSTM ensemble [12]	NA	93.30	90.00	NA
VAEGAN - CNN	88.97	95.00	95.24	99.78

From Table 2. the proposed method VAEGAN-CNN showed improvements in the performance metrics. It achieved a notable accuracy of 99.78%, precision of 88.97%, recall of 95.24%, and f1-score of 95.00%. The performance improvement of the proposed method compared to CNN [8], LightGBM [9], and LSTM ensemble [10] is showed. Overall, the proposed method has achieved the highest results among previous models.

C. *Discussion*

The advantages of the proposed technique and disadvantages of present approaches are briefly discussed in this section. The present approach has some disadvantages in CNN [10] attained the class imbalance issues that had not been addressed which affected the detection in classification process. LightGBM [11] affected the reduction rate in detection that was observed in classification. LSTM ensemble [12] attained the limitations in banking for customer orientation such as an increase in false positive rate. VAEGAN is proposed to overcome the existing limitations and addressing the detection fraud financial transaction. VAEGAN was integrated with CNN attained the better performance and enhanced the detection rate.

V. CONCLUSION

In conclusion, the proposed method which is VAEGAN-CNN on credit card fraud detection using credit card dataset shows the efficiency in the detection. By using pre-processing method such as DR which helps to eliminate redundant features, noisy data, and irrelevant data, which leads to better accuracy in detection of fraud in the transaction. Then, VAEGAN over sampling method was used for classification problem of imbalanced data. At last, CNN is used in the classification process in which the parameters compare the obtained values with current fitness value to classify them into normal and fraud transaction. This method gives the potential of DL in tackling complex datasets, offering robust and accurate for fraudulent transaction detection. The conducted experiment showed that proposed approach accomplished a higher classification accuracy of 99.78%, precision of 88.97%, recall of 95.24%, and f1-score of 95.00% which is compared to other methods such as CNN, LightGBM, and LSTM ensemble. In the future, to extend the application of the prediction model to assess additional datasets and explore different timeframes for the selected data.

REFERENCES

[1] Vuppula, K., 2021. An advanced machine learning algorithm for fraud financial transaction detection. Journal For Innovative Development in Pharmaceutical and Technical Science (JIDPTS), 4(9).

[2] Senthilkumar, A. and Gaddam Paneesh, R., 2024. An X-band conformal FSS with enhanced shielding effectiveness. International Journal of Electronics, pp.1-13.

[3] Ashfaq, T., Khalid, R., Yahaya, A.S., Aslam, S., Azar, A.T., Alsafari, S. and Hameed, I.A., 2022. A machine learning and blockchain based efficient fraud detection mechanism. Sensors, 22(19), p.7162.

[4] Madhurya, M.J., Gururaj, H.L., Soundarya, B.C., Vidyashree, K.P. and Rajendra, A.B., 2022. Exploratory analysis of credit card fraud detection using machine learning techniques. Global Transitions Proceedings, 3(1), pp.31-37.

[5] Almazroi, A.A. and Ayub, N., 2023. Online Payment Fraud Detection Model Using Machine Learning Techniques. IEEE Access, 11, pp.137188-137203.

[6] Nguyen, N., Duong, T., Chau, T., Nguyen, V.H., Trinh, T., Tran, D. and Ho, T., 2022. A proposed model for card fraud detection based on Catboost and deep neural network. IEEE Access, 10, pp.96852-96861.

[7] Alfaiz, N.S. and Fati, S.M., 2022. Enhanced credit card fraud detection model using machine learning. Electronics, 11(4), p.662.

[8] Seera, M., Lim, C.P., Kumar, A., Dhamotharan, L. and Tan, K.H., 2024. An intelligent payment card fraud detection system. Annals of operations research, 334(1), pp.445-467.

[9] Vishnu, C., Abhinav, G.V., Roy, D., Mohan, C.K. and Babu, C.S., 2023. Correction to "Improving Multi-Agent Trajectory Prediction Using Traffic States on Interactive Driving Scenarios". IEEE Robotics and Automation Letters, 8(11), pp.7519-7519.

[10] Alarfaj, F.K., Malik, I., Khan, H.U., Almusallam, N., Ramzan, M. and Ahmed, M. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access, 10, 2022, pp.39700-39715.

[11] Hashemi, S.K., Mirtaheri, S.L. and Greco, S., 2022. Fraud detection in banking data by machine learning techniques. IEEE Access, 11, pp.3034-3043.

[12] Esenogho, E., Mienye, I.D., Swart, T.G., Aruleba, K. and Obaido, G., A neural network ensemble with feature engineering for improved credit card fraud detection. IEEE Access, 10, 2022, pp.16400-16407.

[13] Baker, M.R., Mahmood, Z.N. and Shaker, E.H., 2022. Ensemble Learning with Supervised Machine Learning Models to Predict Credit Card Fraud Transactions. Revue d'Intelligence Artificielle, 36(4).

[14] Mienye, I.D. and Sun, Y., 2023. A deep learning ensemble with data resampling for credit card fraud detection. IEEE Access, 11, pp.30628-30638.

[15] Credit Card Fraud detection dataset- https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud (accessed on May 03 2024).