IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

Anomaly Detection using Generative Adversarial Network VAE

Jaiprakash Prajapati[1] and Prof. Nilesh Choudhary[2]
Student, Department of Computer Engineering [1]
Professor, Department of Computer Engineering[2]
Godavari College of Engineering, Jalgaon, Maharashtra, India

Abstract: *Fraudulent credit card transactions continue to be one of the problems facing businesses and banks. It causes us to lose billions of dollars each year. Designing efficient algorithms is one of the most important challenges in this field. This paper aims to propose an efficient approach that automatically detects fraud in credit card transactions using Generative Adversarial Network Variational Auto encoders. The effectiveness of the proposed method (Generative Adversarial Network VAE) has been proved in identifying fraud in actual data from transactions made by credit cards. However, the typical credit card data set presents an imbalanced classification landscape due to highly skewed class distributions. Researchers have proposed several strategies to address these imbalances, but draw backs still remain. The proposed method is tested on an open credit card fraud dataset, which contains 20 million transactions generated from a multi-agent virtual world simulation performed by IBM. Experimental results show that the VAE method performs better than traditional deep neural network methods. Through experiments, compared with the VAE and traditional fully connected neural networks, the results showed the proposed algorithm improves the classification accuracy of a minority class of imbalanced datasets.*

Keywords: Anomaly Detection, Generative Adversarial Network, Variational Autoencoder, Fraudulent credit card, Deep learning

I. INTRODUCTION

Credit card fraud is a growing threat with far-reaching consequences in the finance industry, corporations, and government. Fraud can be defined as criminal deception with the intent of acquiring financial gain. As credit cards became the most popular method of payment for both online and offline transactions, the fraud rate also accelerates. The main reason for fraud is due to the lack of security, which involves the use of stolen credit cards to get cash from the bank through legitimate access. This makes it very difficult to prevent credit card fraud.

The Association for Payment Clearing Services (APACS) estimates that total credit card fraud losses in the UK have surged from £122 million in 1997 to £440.3 million in 2010[1]. According to the Nelson Report [2], global credit and prepaid card losses were $24.71 billion in 2016, an increase of 11.2% from 2015. The total fraud loss is borne by the card issuer and merchant, and the acquirer of the ATM and merchant transaction. A key feature of the report, the LexisNexis Fraud Multiplier [3], estimates the total loss incurred by merchants based on the actual dollar value of fraudulent transactions. It has increased from $2.23 a year ago to $2.40 in 2016, according to the Fraud Multiplier tool. The report also found that the volume of fraudulent activity increased sharply from last year, with average monthly successful fraudulent transactions increasing from 156 to 206 and prevented fraudulent transactions from 177 to 236, while revenue Fraud levels as a percentage also increased slightly from 1.32 percent to 1.47 percent.

Financial and bank fraud cases in the Kingdom of Saudi Arabia halved to 2,046 in 2017, compared with 4,275 the previous year. In 2016 the fraudulent activities worth 520 million SAR, and last year the financial fraud amounted to 214 million SAR[4].Financial institutions face many risks in the current situation. Foremost among these is the issue of fraud, especially with the advancement of modern technologies such as the Internet and computers [5], scammers are developing ways to obtain illicit financial gains that can be remedied as soon as possible which requires fraud detection technology.

Financial fraud is a problem that has far-reaching implications for both the financial industry and everyday life. Fraud can reduce confidence in the industry, destabilize the economy, and affect people's cost of living. Jarrod West et al.[6]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

defined financial fraud as the deliberate use of unlawful methods or practices for the purpose of obtaining financial gain. Financial losses incurred as a result of fraud at merchants or financial institutions. Unpaid amounts or non-monetary losses may affect the institution's losses to its customers.

Hard to discern in the short term, but obvious in the long term. Electronic financial fraud disclosure can be described as using a computer system to determine whether a newly licensed transaction falls into a fraudulent or legitimate transaction category. A fraud detection system (FDS) should not only be effective, but it should also be cheap.FDS receives the card details and purchase amount and verifies if the transaction is genuine.

Bhatla [7] argued that investigating his 2% of transactions could lead to a reduction in fraud losses of his 1% of the actual transaction value, but increased fraud detection costs. To minimize costs, machine learning-based experts use rules and models to perform an initial check between fraudulent and legitimate transactions, ensuring that only high-risk cases are reviewed requires investigators. ANOMALY detection has broad applications in various domains, such as the detection of insurance fraud and financial crime, surveillance of complex systems like datacenters and spacecraft, and identification of attacks and potential threats in cyberspace. Given these important applications, this task has been a popular research topic for decades, and numerous anomaly detection approaches have been introduced [8], [9].

II. OBJECTIVE

This paper aims to propose an efficient approach that automatically detects fraud in credit card transactions using a algorithm called Generative Adversarial Network Variational Autoencoder.

The main contributions of this work are as follows:

- Briefly understand previous algorithms, used to detect fraudulent credit card transactions depending on machine learning.
- Propose a new model for detecting Fraudulent credit card transactions using deep Learning Algorithm called Generative Adversarial Network Variational Autoencoders
- The proposed model can achieve higher performance than the other state-of-the-art one-class methods according to Recall.

III. LITERATURE SURVEY

The data mining technique is one notable method used in solving fraud detection problems. This is the process of identifying those transactions that belong to fraud or not, which is based on the behaviours and habits of cardholders, many techniques have been applied to this area, including artificial neural networks [11], genetic algorithms, support vector machine, frequent item set mining, decision tree, migrating bird's optimization algorithm, Naïve Bayes. In [12], a comparative analysis of logistic regression and Naive Bayes is performed. The performance of Bayesian and neural networks [13] is evaluated using credit card fraud data. Decision trees, neural networks, and logistic regression have been tested for applicability in fraud detection [14].

Several challenges are associated with credit card detection, namely fraudulent behaviour profile is dynamic, that is fraudulent transactions tend to look like legitimate ones; credit card transaction datasets are rarely available and highly imbalanced (or skewed); optimal feature (variables) selection for the models; suitable metric to evaluate the performance of techniques on skewed credit card fraud data. The performance of credit card fraud detection is highly influenced by the type of sampling approach used, the choice of variables, and the detection technique used.

Neural networks [16-18] and logistic regression [19, 20] are often chosen for their well-established popularity, giving them the ability to be used as a control method by which other techniques are tested. Comparatively, more advanced methods such as support vector machines and genetic programming have received substantially less attention [15]. Most research focuses on using machine learning methods for supervised and unsupervised learning. However, recent studies show a tendency to use the first two types of hybrid methods to combine their advantages.

O. S. Yee, S. Sagadevan, and N. H. A. H. Malim [10] used GAN to oversample credit card fraud and showed that, overall, it is better than the traditional SMOTE method. While acknowledging their success, we have chosen to focus on the GAN method for oversampling of the minority class data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

IV. VARIATIONAL AUTOENCODER

A variational autoencoder is a type of autoencoder with added constraints on the encoded representations being learned. It learns a latent variable model for its input data. So instead of letting your neural network learn an arbitrary function, it learns the parameters of a probability distribution modelingof a data. If you sample points from this distribution, you can generate new input data samples. This is the reason why variational autoencoders are generative models.

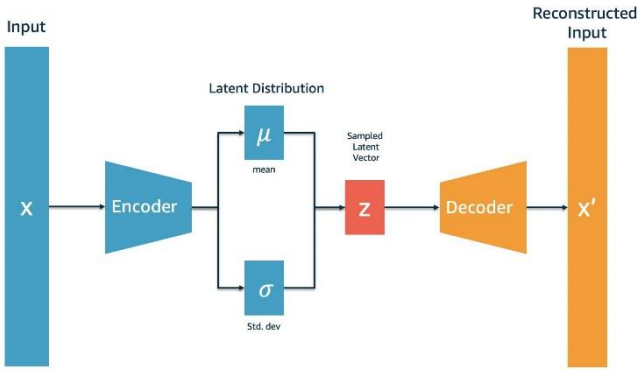

Fig. 1 The variational Autoencoder neural network

In the Fig. 1 First, the encoder network transforms the input samples x into two parameters of the latent space that can be represented by z_mean and z_log_sigma. Then take a random similar point z from a latent normal distribution that is supposed to generate data via z = z_mean + exp(z_log_sigma) * epsilon. wherein epsilon is a random regular tensor. Finally, the decoder network maps these potential spatial points to the original input data.

V. PROPOSED METHODOLOGY

Credit card fraud detection problems can be expressed as common binary classification problems. Different from the common classification problem, however, the distribution ofcases into the two categories (fraudulent, not fraudulent) isseriously imbalanced. Among them, fraudulent transactionsare only a small fraction of non-fraudulent, accounting for lessthan 0.122% of the total data.

To improve the effectiveness of classification results, a framework for detecting credit card fraud will usually try to eliminate the gap between the two categories of cases in the data set.

The framework adopted in this paper is the network architecture for VAE can vary between a simple Feedforward network, LSTM network, or Convolutional Neural Network depending on the use case. In this case, the Feedforward network will be used.VAE architecture consists of four main parts:

- Encoder: It is the part in which the model learns how to reduce the input dimensions and compress the input data into an encoded representation.
- Latent Vector (Bottleneck): This is a layer containing a compressed representation of the input data. This is the minimum possible dimensionality of the input data.
- Decoder: It is the model that learns how to reconstruct the data from the encoded representation to be as close to the original input as possible.
- Reconstruction Loss: It's a way to measure decoder performance and how close the output is to the original input.

The training then involves using back propagation to minimize the network's reconstruction loss. Four hyperparameters are required before setting out training an autoencoder:

- Code size: The number of nodes in the middle layer.
- Number of layers: flexible number of layers (depth of layers).
- Number of nodes per layer: The number of nodes in each layer decreases after the encoder and is increased again in the decoder, and the number of nodes can be selected in each layer according to need.
- Loss Function: The error resulting from the reconstruction of the input data in the output layer, and the Mean square error is used to calculate the error value, such as equation in the Fig. 2

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

$$l(x, \hat{x}) = \frac{1}{n} \sum_{i=1}^{n} (x_{i-\hat{x}_i})^2$$

Fig. 2 MSE Formula

VI. EXPERIMENTAL STAGES

6.1 Experiment Architecture

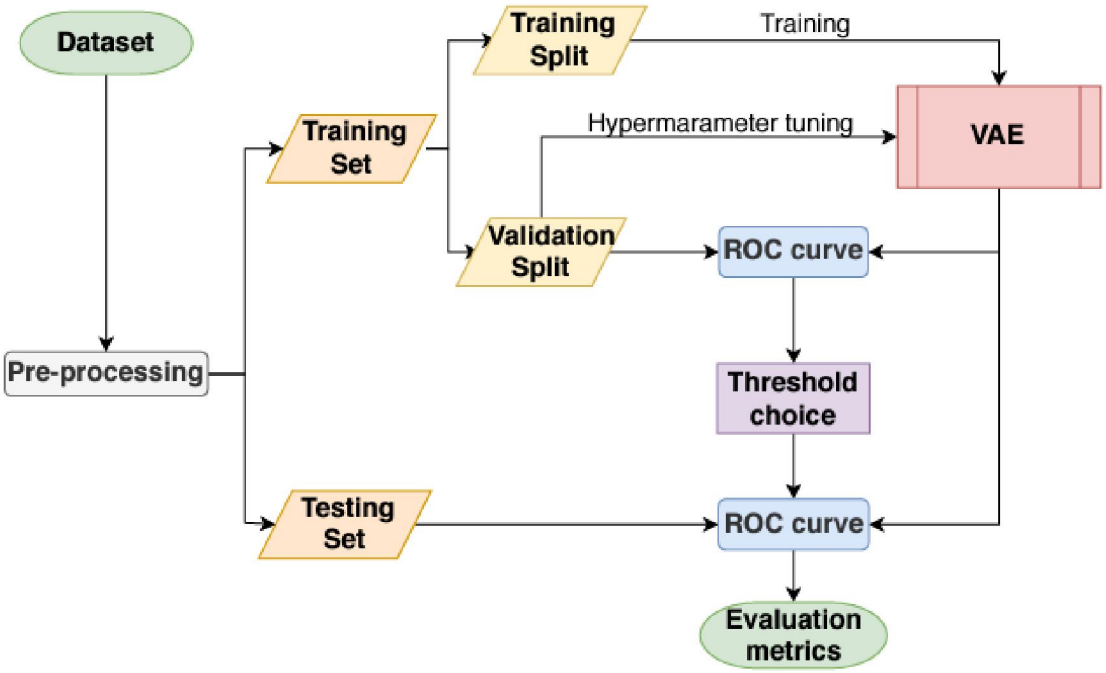

Fig. 3 Proposed Model Flow

6.2 Dataset

This dataset acquired from Kaggle has more than 24386900 transactions with 2000 unique consumers and a consumer owns at most 9 cards generated from a multi-agent virtual world simulation performed by IBM. The data covers 2000 consumers resident in the United States, but who travel around the world. The data also covers decades of purchases and includes multiple cards from many consumers. The most common type of transaction is swipe transactions

TABLE I: Summary of the Dataset

Data	Count	%
Total Transactions	24386900	100
Normal Transactions	24357143	99.878
Fraudulent Transactions	29757	0.122

6.3 Feature Importance

The feature importance plot shows the count by which a feature was used for a split in all weak learners. From the feature importance fig.4, we can see that model can probably identify users which are likely to cause fraudulent transactions along with numeric columns like Amount, Time of the day and so on.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

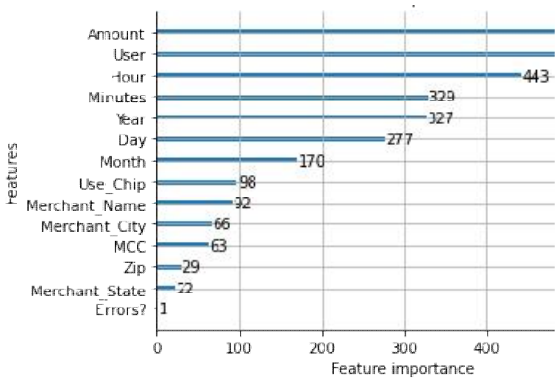

Fig. 4 Important features of dataset

6.5 Model Evaluation Methods

The proposed algorithm depends on neural network type VAEto evaluate its performance andensure its ability to detect fraud cases as appropriate. Several measures were used:

- Reconstruction error: The Mean squared error is used to calculate the value of the reconstruction error:

$$MSE = \frac{1}{n} \sum_{i=1}^{n} (x_{i-} \widehat{x_i})^2$$

Where, n: is the size of the input and output, **x**: is the input data $\bar{x}$: the output data of the reconstruction.
The high error value indicates the discovery of fraudulent transactions while the low value reveals legitimate transactions.

- Precision & Recall: Precision and Recall are one of the most widely used standards in unbalanced data, which reflect the precision of the suitability of the resulting scale and proximity to the expected solution, while recall measures the number of relevant results returned to the goal in each of them to approach the one. High score recall indicates a low False Negative (FN) rate, while high precision indicates a low False Positive (FP) rate. High Scores for both show that the classifier restores accurate results in addition to the recovery of the majority of the positive results.

TABLE II: Classification performance metrics

Measure	Definition
Accuracy	(TP+TN)/(TP+TN+FP+FN)
Precision	TP/(TP+FP)
Recall (Sensitivity)	TP/(TP+FN)
F1-Score	2 * Precision * Recall / (Precision + Recall)

Table II shows the performance measures for evaluating the performance of the model, three indicators are used (precision, recall, and f1 score). Precision (also called positive predictive value) is the fraction of true frauds among all samples which are classified as frauds, while recall (alsoknown as sensitivity) is the fraction of frauds that have been classified correctly over the total amount offrauds. TP (True Positive) refers to the amount of fraud properly classified. FP (False Positive) refers to the number of normal transactions classified as fraud. FN (False Negative) refers to the amount of fraud classified as normal. TN (True Negative) refers to the number of normal transactions correctly classified. However, these parameters may not be the most appropriate endpoints when evaluating fraud detection models because they implicitly assume that misclassified transactions have the same cost as correctly classified transactions.

VII. RESULTS

The proposed model's achieved accuracy is98.39% at an MSE threshold cut-off value of 2.63. The F1-Score for normal transactions is 0.99 and for fraudulent transactions is 0.87.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

TABLE III: Proposed Model Metrics

Class	Precision	Recall	F1-Score
Normal Transactions	0.99	0.99	0.99
Fraudulent Transactions	0.83	0.91	0.87

VIII. CONCLUSIONS

In this paper, advanced techniques have been introduced to detect the fraudulent transactions in credit card. This study reviewed how machine learning can be used to address some of the issues of financial fraud detection in credit cards. The focus, on the design model, can report the most fraudulent transactions for investigators using a generative adversarial variational autoencoder algorithm way that can deal with unbalanced datasets. The algorithm was able to detect 98.39% accurately at the MSE threshold cut-off value = 2.63.

The algorithm also provided a solution to avoid the problem of data balancing experienced by many of the algorithms currently used, which can be applied directly to data without the use of data balance methods such as the method of Under-Sampling.

The recommendation of the paper lies in the following suggestions for improvements to the currentalgorithm: Appling fraudulent work to different classification algorithms and comparing them withthis model; inserting a random value to confuse the fraudsters and disrupt theirpreviously acquired knowledge; and applying this algorithm to the data of BFSI companies.

REFERENCES

[1]. Delamaire L, Abdou HAH, Pointon J. Credit card fraud and detection techniques: A review. Banks and Bank systems. Banks and Bank Systems. 2009;4(2):57-68.

[2]. The Nilson report; 2016.Available:http://www.nilsonreport.com

[3]. LexisNexis. The true cost of fraud 2016 study.Available:https://risk.lexisnexis.com/insights-resources/research/lexisnexis-2016-true-cost-of-fraud

[4]. Argaam report; 2018.Available:https://www.argaam.com/en/article/articledetail/id/570536

[5]. [Yeh IC, Lien C. The comparisons of data mining techniques for the predictive accuracy of probabilityof default of credit card clients. Expert Systems with Applications. 2009;36(2):2473-2480.

[6]. West J, Bhattacharya M, Islam R. Intelligent financial fraud detection practices: An investigation. InInternational Conference on Security and Privacy in Communication Systems. Cham: Springer. 2014;186-203.

[7]. Bhatla PT, Vikram P, Amit D. Understanding credit card frauds. Cards Business Review. 2003;1:6.

[8]. C. C. Aggarwal, Outlier analysis. Springer, 2017.

[9]. G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, “Deep learning for anomaly detection: A review,” ACM Comput. Surv., vol. 54, no. 2,pp. 1–38, 2021.

[10]. O. S. Yee, S. Sagadevan, and N. H. A. H. Malim, ``Credit card fraud detection using machine learning as data mining technique," J. Telecommun., Electron. Comput. Eng., vol. 10, nos. 1-4, pp. 23-27, 2018.

[11]. Ogwueleka, F. N., (2011). Data Mining Application in Credit Card Fraud Detection System, Journal of Engineering Science and Technology, Vol. 6, No. 3, pp. 311 – 322

[12]. Ng, A. Y., and Jordan, M. I., (2002). On discriminative vs. generative classifiers: A comparison of logistic regression and naive bayes. Advances in neural information processing systems, 2, 841-848.

[13]. Maes, S., Tuyls, K., Vanschoenwinkel, B., &Manderick, B. (2002). Credit card fraud detection using Bayesian and neural networks. In Proceedings of the 1st international naiso congress on neuro fuzzy technologies (pp. 261-270).

[14]. Shen, A., Tong, R., & Deng, Y. (2007). Application of classification models on credit card fraud detection. In Service Systems and Service Management, 2007 International Conference on (pp. 1-4). IEEE.

[15]. West J, Bhattacharya M, Islam R. Intelligent financial fraud detection practices: An investigation. In International Conference on Security and Privacy in Communication Systems. Cham: Springer. 2014;186-203.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

[16]. Bose I, Wang J. Data mining for detection of financial statement fraud in Chinese Companies. In International joint Conference on e-Commerce, e-Administration, e-Society, and e-Education. International Business Academics Consortium (IBAC) and Knowledge Association of Taiwan (KAT). Taiwan; 2007.

[17]. Kirkos E, Spathis C, Manolopoulos Y. Data mining techniques for the detection of fraudulent financial statements. Expert Systems with Applications. 2007;32(4):995-1003.

[18]. Ravisankar P, Ravi V, Rao GR, Bose I. Detection of financial statement fraud and feature selection using data mining techniques. Decision Support Systems. 2011;50(2):491-500.

[19]. Bhattacharyya S, Jha S, Tharakunnel K. Data mining for credit card fraud: A comparative study.Decision Support Systems. 2011;50(3):602-613.

[20]. Pinquet J, Ayuso M, Guillen M. Selection bias and auditing policies for insurance claims. Journal ofRisk and Insurance. 2007;74:425-40.

[21]. Tasche D. A plug-in approach to maximising precision at the top and recall at the top. arXiv preprint arXiv:1804.03077; 2018.

BIOGRAPHY

- Jaiprakash is an M. Tech candidate at the Dr. Babasaheb Ambedkar Technological University, researching the subjects of AI, NLP, and social networks. He is a seasoned Data Scientist with over a decade of professional modeling experience and a passion for developing business ideas into implementable solutions by harnessing the power of Machine Learning and Technology.

  A multidisciplinary data scientist with extensive experience in machine learning and data engineering. He works with technologies such as Docker, TensorFlow, Spark, cloud environments, relational and graph databases, APIs, Python, and R stacks. He has prototyped, developed, and deployed real-world data applications for many of the most prominent Indian and global brands. He can be reached at jaiprakash.prajapati@outlook.com.