An Ameliorated method for Fraud Detection using Complex Generative Model: Variational Autoencoder

Kaithekuzhical Leena Kurien, Ajeet Chikkamannur

Abstract*: *Perpetrating fraud for financial gain is a known phenomenon, in this fast-growing adoption of smart phones and increased internet penetration, embracing digital technology. Evolution of financial transactions over the years, from paper currency to electronic media, leading the way in the form of credit cards or interbank electronic transactions. Consumers trending towards e-commerce hasn't deterred criminals, but considered this as the opportunity to make money through defrauding methods. Criminals are rapidly improving their fraud abilities.

The current Supervised and Unsupervised Machine Learning Algorithm approaches to the discovery of fraud are their inability to learn and explore all possible information representation. The proposed system, VAE based fraud detection, which uses a variational autoencoder for predicting and detecting of fraud detection. The VAE based fraud detection model consists of three major layers, an encoder, a decoder and a fraud detector element. The VAE-based fraud detection model is capable of learning latent variable probabilistic models by optimizing the average value of the information observed. The fraud detector uses the latent representations obtained from the variational autoencoder to classify whether transactions are fraud or not. The model is applied on real time credit card fraud dataset. The experimental results show that, implemented model perform better than supervised Logistic Regression, unsupervised Autoencoders or Random Forest ensemble model.

Keyword*: *Fraud detection, credit card, machine learning, generative models, Variational Autoencoder.

I. INTRODUCTION

The Technology is advancing everyday and this change in neoteric methods in technology has major influence on diverse areas of ecommerce and social media. As many users proliferate social media, the ecosystem is fuelled by different types of users, with intensions good and bad. In this day and age, credit card is one of the most widely used transaction method. The greater than before popularity of credit card is mainly due to the ease of transaction, purchasing goods at the comfort of our homes, saving time , the increasing popularity of network banking and mobile banking. In the digital world, the increased online shopping and payment leads to hacking and fraudulent transactions.

Fraud Facts 2019[1] published by UK Government discusses various fraud types occurred due to digital revolution and the statistics show the large amount of revenue loopholes in the present digital ecommerce system and explains the ways to combat fraud and advises users safe digital transactions and focuses on how false transaction cause loss of revenue to various financial institutions in United Kingdom. Due to the dynamic evolving nature of fraudster, finding a pattern in fraud detection is difficult .The fraudsters are wise and knowledgeable and they often cleverly use innovative ways to commit fraud transactions to escape law. The machine learning approach of fraud detection has delivered promising results in recent times due to large computing power and ability to handle large datasets. The supervised approach of machine learning detects fraud, but is unable to tackle the dynamic nature of fraudster. The unsupervised approach of machine learning is able to detect all the unseen anomalies in the data and able to tackle the dynamic nature of fraudster. The unsupervised deep neural network also detects fraud efficiently. Recent times generative model algorithms have given excellent results and the biggest advantage is they work with a sample of data and explore or generate all possibilities within the distribution which is relevant in area of fraud detection.

II. RELATED WORK

The challenge of fraud detection in credit card domain is is similar to other anomaly detection areas like spam detection [2]and cancer detection[3][4] due to the imbalanced dataset nature where around 99 percent of data would be of one class and less than one percent would be of another class. The skewed nature of dataset of is challenging and difficult to detect and predict.

The earlier studies of fraud detection used supervised, unsupervised and ensemble classification and regression algorithms. The supervised algorithms [5] used labeled data to classify whether the transactions in credit card were fraudulent or not. The algorithms used were Support Vector Machine, Random Forest and Logistic Regression.

Revised Manuscript Received on December 22, 2019.

* Correspondence Author

Ms Kaithekuzhical Leena Kurien *, Computer Science and Engg, R.L Jalappa Institute of Technology, VTU, Bengaluru ,India. Email: lina.shibu@gmail.com

Dr Ajeet Chikkamannur Prof & HOD, Computer Science and Engg, R.L Jalappa Institute of Technology, VTU, Bengaluru, India Email: ac.ajeet@gmail.com

The comparison between the supervised and ensemble algorithms showed that Random Forest showed better results in predicting whether the transactions are fraud or not. The unsupervised algorithms of clustering and auto-encoders [6] were applied and the result were encouraging. The deep learning neural network algorithms are able to learn high level features in better way than traditional machine learning algorithms.

Khattar[6] uses multimodal variational auto-encoder in fake news .The text and images were two modes passed on the encoder and decoder. The latent representation holds the learned features. Multimodal variational autoencoder showed better results and have used convolutional neural network.

Quoc Phong[7] uses deep learning algorithms on network anomalies on NetFlow records. The different attacks on the network are anomalies which can be detected and predicted. The variational autoencoder based framework is scalable on size of data and feature dimension. The unsupervised learning of Variational Autoencoder showed better results in identifying Dos,spam attacks.

Ruoyu Deng[8] proposes FraudJudger ,a fraud detection model based on behavior of users on unlabeled data. The model uses Adversarial autoencoder which merges operation and transaction data which are converted to latent representation by adversarial autoencoder which are used to classify the users.

Yvan [9]evaluated automated feature engineering in fraud detection in credit card domain using Hidden Markov Model. The Hidden Markov Model uses likelihood of a transaction to a sequence of past transactions. The findings from Hidden Markov Model are used as extra features in a Random Forest for detection of fraud. The model shows better results in auc-roc curve and the paper also addressed missing value issues in credit card fraud detection

Ping Jiang [10]shows autoencoder neural network applied on credit card dataset and as the dataset is imbalanced ,oversampling is performed on the dataset to obtain balanced dataset. The evaluation parameters of roc-auc curve on autoencoder are good.

Jinwon An,,Zhiqiang Wan[11][12]implemented variational autoencoder which is a generative model using probabilistic function. The anomaly detection on fraud dataset is difficult as the dataset is skewed and the results obtained from the model is good.

III. EXISTING APPROACH

The two main types of learning are supervised approach and unsupervised approach. The supervised algorithm uses labeled data .The unsupervised algorithm can learn without labeled data. They can find unknown patterns in the data.

A. **Supervised Learning:** A well labeled training data is used to infer and predict unforeseen patterns in the data. [13]From the training data, the features are extracted and the machine learning algorithms are applied and modeled to classify whether the particular event occurs or not. The supervised algorithms are Logistic Regression, Decision Tree, Naive Bayes.

B. **Unsupervised Learning :** The input data is present and the data is not labeled. The unsupervised algorithms are applied to the unlabeled training data to explore and examine patterns in the data. The two types of unsupervised algorithms are Clustering and Association. Clustering algorithms process the data and can group the data into clusters .The algorithms on themselves help identify the clusters. Association rules of if- then-else are written for each use case .The unsupervised models are K-Means, Autoencoders ,Hierarchical clustering, K-NN.

C. **Ensemble Models :** It is a process by which multiple models are strategically generated and combined to solve a computational intelligence problem. The different ensemble learning models[14] are Bagging, Boosting, Ada-boost algorithm .In this paper, Ensemble model Random Forest comparison is shown.

IV. PROPOSED METHODOLOGY:UNSUPERVISED DEEP LEARNING MODEL:VARIATIONAL AUTOENCODERS

Variational Autoencoders (VAEs) are generative models used for generating fictional human faces ,artificial music and artwork. Kingma et al. and Rezende et al defined generative models Variational autoencoders (VAEs) in 2013.[15]It learns from latent variables and corresponding inference models using stochastic gradient descent. Stochastic gradient descent [16]randomly selects small sample of data iteratively, unlike gradient descent which works on entire dataset.

Variational Autoencoders functionally also try to reconstruct the input as normal autoencoders , but with the additional constraint that the latent representation learns the probability distribution parameters of the input than the encoding of the input, hence called the "Variational". The advantages of learning the distribution are by explicitly modeling the data and noise generation processes, they can learn to separate the two, making it more robust. Secondly, the latent space can become more interpretable if disentanglement constraints are applied. Third advantage is new samples can be generated by sampling latent vectors and passing them through the layers of decoder.

It is a principled generative model. The input data is mapped to latent space using neural net and the latent space has posterior distribution p(x1) and prior distribution p(x) are modeled as Gaussian distribution. The latent space has mean and covariance vector and force it to be unit normal distribution using KL divergence. The random sample from latent space distribution is assumed to generate data similar to training data (X).The latent space vector is mapped to input image using decoder. The reconstructed output is assumed to correspond to mean of Gaussian that leads to reconstruction loss.

Each iteration only one sample is randomly selected from latent space is used. The variational autoencoder is capable of learning probabilistic latent variable models by optimizing a bound on the marginal likelihood of the observed data.

The encoder layer is a neural network that accepts the all 30 attributes as input and passes to the next Dense Layer of Sequential Keras model with 15 attributes .The next Dense Layer accepts 10 attributes and the output is passed to 7 attribute dense layer. The fifth layer converts it to two dimension mean and covariance of size two variables.

The implementation of VAE based model for fraud detection is using python with keras and tensorflow as backend.

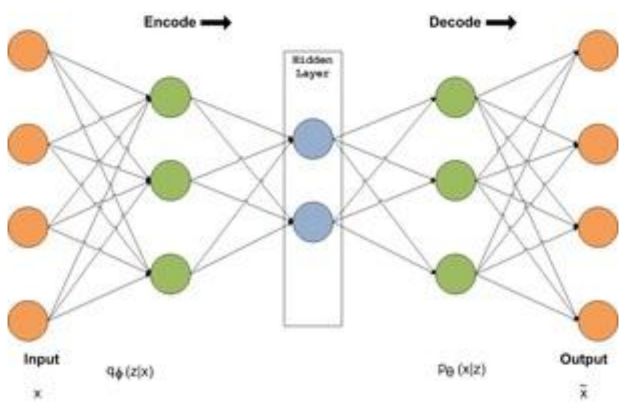

Fig .1.Diagram of Variational AutoEncoder

The Variational autoencoder has three parts ,encoder, decoder and loss function. The encoder is a network which takes the input and outputs the feature vector. Its input is a data point x, its output is a hidden representation z, and it has weights and biases θ[17].The encoder accepts the input x with n dimensions and 'encodes' into latent space which is lower dimension and stochastic. The encoder gives output result parameters to q$\theta(z/x)$ which is Gaussian probability density.

The decoder is a network with the same network structure as encoder but in opposite orientation that takes the feature vector from the latent vector. Its input is the representation z, it outputs the parameters to the probability distribution of the data, and has weights and biases ϕ. The decoder is denoted by p$\emptyset(x/z)$. The loss function of the variational autoencoder is the negative log-likelihood with a regularizer. The total loss is then $\sum_{i=1}^{N} li$ for N entire data points. The loss function *li* for data point *xi* is:

$$li(\theta,\phi)=-\mathrm{E}_{z\sim q\theta(z|xi)}[\log p\phi(xi|z)]+\mathrm{KL}(q\theta(z|xi)||p(z)) \quad (1)$$

The next term is called the regularizer, Kullback-Leibler divergence between the encoders distribution qθ(z⁄(x))and p(z).It is a measure of how much close value q is to p.

The first term is called the reconstruction loss, or expected negative log-likelihood of the i-th data point in x. The expectation is taken with respect to the encoder’s distribution over the representations. This term encourages the decoder to determine to reconstruct the data. Poor reconstruction will incur a large cost in reconstructive loss function.

V. VAE BASED FRAUD DETECTION

The novel deep learning VAE model of 12 layers is proposed to detect fraud in credit card data. It has 3 major layers.

- Encoder Layer: This layer encodes the information which is numeric data type into intermediate latent vector.

- Decoder Layer: This layer reconstructs back the original data from latent vector.

- Fraud detector: This layer uses the learned shared representation (latent vector) to predict if a transaction is fraudulent or not.

A.Encoder : The inputs to the encoder are the attributes of credit card transactions and it outputs a latent vector representation of the feature learnt from the data. The following are the layers defined at the encoder end.

Table 1: Encoder and Layers Description

Sr No	Layer Type	No of attributes
1	Input Layer	30
2	Dense Layer1	25
3	Dense Layer 2	15
4	Dense Layer3	10
5	Dense Layer 4	7
6	Latent Dimension	2

B. Decoder

The architecture of the decoder is similar to that of the encoder but reversed. The objective of the decoder is to reconstruct original information from the sampled latent version.

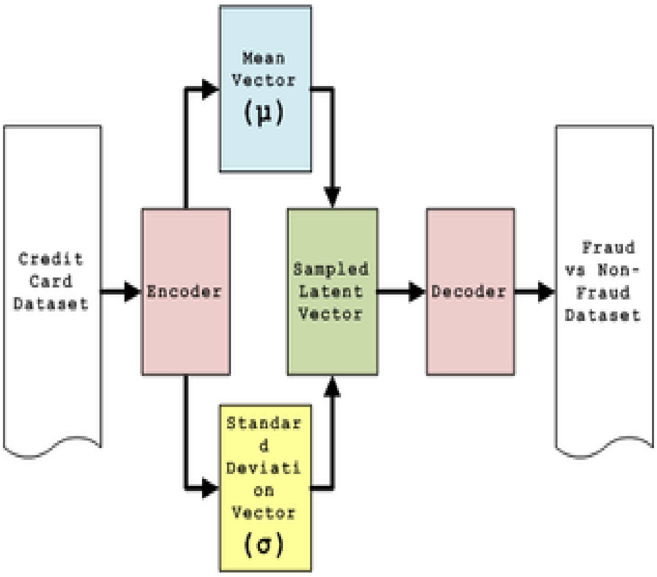

Fig.2. Block Diagram of VAE-Based Fraud detection

C. Fraud Detector

Fraud Detector takes latent representation as input and aims to classify whether the transactions are fraudulent or not.

The reconstruction loss and KL divergence loss are added and optimized in Variational Autoencoder models. The probability distribution parameters (µ and s) approximate to the target distribution (Normal distribution) by reducing the Kullback-Leibler Divergence.

VI. DATASET AND EVALUATION

The problem statement is to illuminate fraud in credit card transactions.

The dataset consists of credit card transactions made by European cardholders in September 2013.

(https://www.kaggle.com/mlg-ulb/creditcardfraud). [19] The duration period for the dataset is two days. There are 492 fraud transactions from 284,807 transactions. The dataset is extremely skewed and the positive class (frauds) account for 0.172% of all transactions.

The columns in the dataset are numerical data and are PCA transformed due to confidentiality issues. There are 30 columns in the dataset out of which features V1, V2, ... V28 are the principal components obtained with PCA. The 'Time' and 'Amount' column have not been PCA transformed. The column 'Time' contains the seconds elapsed between each transaction and the first transaction in the dataset. The feature 'Amount' is the transaction Amount. It can be observed that Amounts in fraudulent transactions were always below 2,500. The column 'Class' is the response variable. It takes value 1 in case of fraud and 0 otherwise.

A. Algorithm VAE Based Fraud detection

Algorithm: VAE based Fraud detection

Input: The credit card dataset

Output: Fraud/Non - Fraud Transactions

- Input Raw Dataset
- Visualize Preprocessed Features and examine co-relation between the attributes
- Randomly sample a small subset of data as training data and testing data
- Apply Variational Autoencoder generative algorithm with

  1. Encoder neural network and its layers
  2. Decoder neural network and its layers
  3. Latent Dimension size specification

- Compare VAE based Fraud detection results vs Logistic Regression vs Random Forest vs Autoencoders

B. Implementation and Steps in the Proposed System

- Input the dataset and Visualize the features in the dataset

The credit card dataset is input to the system and features are analyzed.

Out[11]:

Time	V1	V2	..	V28	Amt	Class
0.0	-1.359807	-0.072781		-0.021053	149.62	0
0.0	1.191857	0.266151		0.014724	2.69	0
1.0	-1.358354	-1.340163		-0.059752	378.66	0
1.0	-0.966272	-0.185226		0.061458	123.50	0
2.0	-1.158233	0.877737		0.215153	69.99	0

[5 rows x 31 columns]

Fig .3. The sample dataset

The features are visualized and in the diagram the clear distinction of fraud and non fraud transactions are observed.

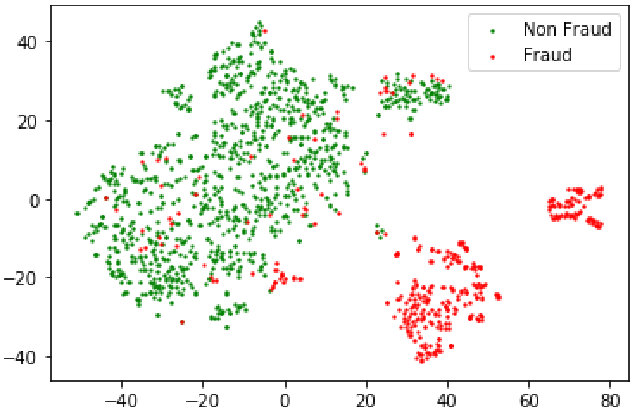

Fig .4. Visualizing the features

- Splitting Training Dataset and Testing Dataset .The training set has a combination of 2000 non-fraud transactions and the entire fraud transactions .The dataset is extremely skewed and imbalanced with0.172% fraud transactions. Hence approximately 300-400 are fraud transactions which are also added to training set. The testing set consists of 0.25% transactions.
- Train a Variational Autoencoder with 12 layers total in encoder and decoder and Fraud detector .

☐ Encoder: The input to the encoder is the sequential list of credit card transactions T = [T1 T2 ... Tn], where n is the number of transactions in the sample. Each transaction Ti ∈ T is passed onto multiple layers in the encoder .To extract the features from the numeric content of transaction data in the encoder, tensor flow probability layers are used. The encoder is a Keras Sequential [20] model with dense layers. In the last, outputs of dense layers are passed to multivariate to separate mean and covariance matrix. The final distribution also adds regularization term to the loss. Specifically, the KL divergence is added between the encoder and the prior to the loss.

The VAE is trained with 2000 rows non-fraud transactions and fraud transactions. The prior for the latent variables is set to be a random unit multivariate normal vector of the latent dimension. The latent dimension is set to 2 with two latent vectors.

□ Decoder: The decoder is same as reversed encoder .The output of the decoder are real values and have normal distributions.

□ Fraud detector: The output of the encoder neural network gives latent mean with dimension [2,2].

- Visualize Latent Representations of Mean and Standard Deviation

The plots of latent distribution parameters are shown below. The grouping of fraud and non fraud transactions are shown evidently.

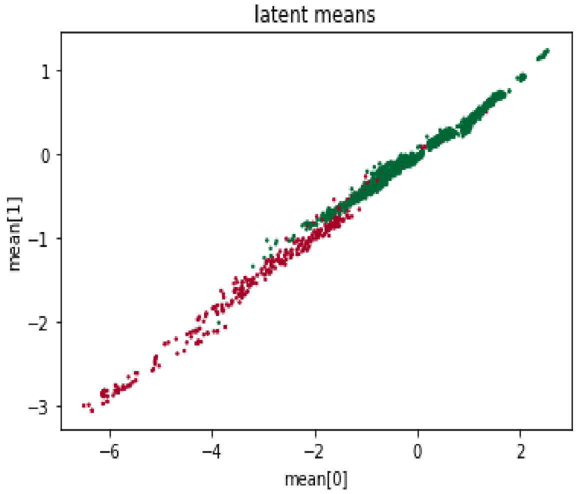

Fig.5. Plot showing latent means with red color indicating fraud and green non-fraud transactions.

The standard deviations plot with red values indicating fraud transactions tend to have higher values indicating outliers and are also scattered.

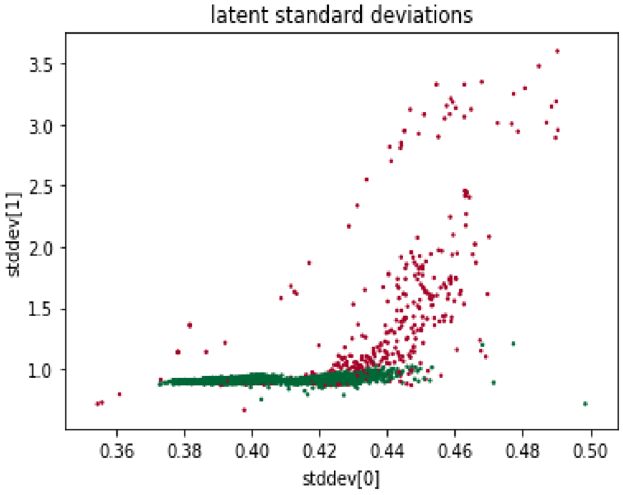

Fig.6. Plot showing standard deviations with red indicating fraud and green showing non fraud transactions

C. Hyper parameters Tuned

The hyper parameters tuned in VAE-Based Fraud detection are:

1. Latent dimension: The Latent dimension used is 2.The model was also tested for Latent dimension with 3 dimensions each of mean and standard deviation. The model gave better results with latent dimension of 2.

2. Number of Epochs: The numbers of epochs tested were 50,100,150,200.

3. Patience: This attribute stops after specified iterations after achieving convergence

4. Encoder /Decoder Layers: The model was tested with 4,5 and 6 layers.

5. Batch size: The batch size was tested for 128,256 respectively.

6. Input data: The generative models randomly selects a small subset of data and explores the complex patterns of possibilities of fraud .The input data size was tested on 1500,2000 and 2500 non fraud transactions with entire fraud transactions which is 0.176% of entire transaction set.

VII. RESULT AND DISCUSSION

A.Metrics used: The Auc-Roc curve is Area Under Curve and Receiver Operator Characteristics. It is an important metric used to perform evaluation of a classification model. Auc-Roc curve shows excellent results in measuring models performance for imbalanced datasets. The imbalanced datasets with class 0 with more than 99% and less than one percent values as class1are challenging for the metrics to evaluate the classification model. Auc-Roc curve provides better evaluation results at imbalanced datasets. Auc-Roc curve is the metrics used for measuring the performance of VAE based fraud detection.

Roc is a probability curve [21] and Auc is the degree of separation between the two classes. The higher value of Auc means the model is able to distinguish 0s as 0s and 1s as 1s.

The output of the matrices depend on the results obtained by True positive (TP), True Negative (TN), false positive (FP), false negative (FN). [22] The transaction cases which are not fraud and the system model has predicted as not fraud as True Positive (TP). The transaction cases which are fraud and the system model has predicted as fraud as True Negative (TN). The transaction cases which are fraud and the system model has predicted as not fraud as False Positive (FP). The transaction cases which are not fraud and the system model has predicted as fraud as True Negative (TN). The ROC Curve, relative characteristic curve is plotted with true positive rate (TPR) against false positive rate (FPR).

Retrieval Number: B10051292S19/2019©BEIESP
DOI: 10.35940/ijitee.B1005.1292S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The True positive rate is calculated as the ratio of true positive cases system has identified with actual positive cases. The False positive rate is calculated as the ratio of false positive cases system has identified with negative actual cases.

B. Comparison of VAE Based Fraud detection Vs Supervised ,Unsupervised and Ensemble Models

The results of generative model VAE Based fraud detection on test set were better than Random Forest and Autoencoders.

The ROC-AUC Curve using VAE based Fraud detection is 97.07 %.

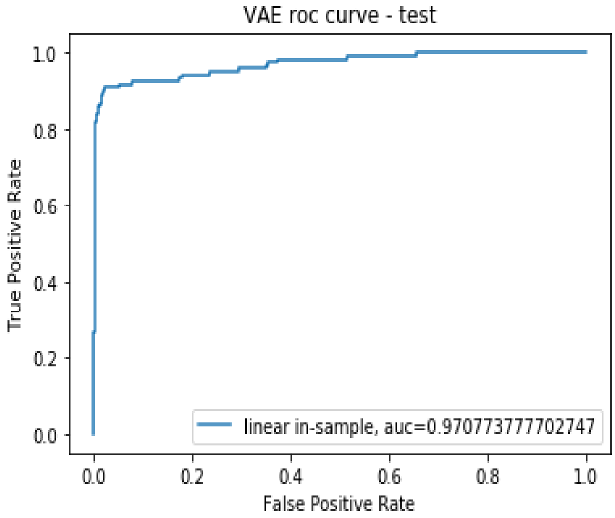

Fig.7. showing Roc-auc curve on test data of VAE-Based Fraud detection.

The ROC-AUC curve using simple Autoencoders deep neural network are shown below.

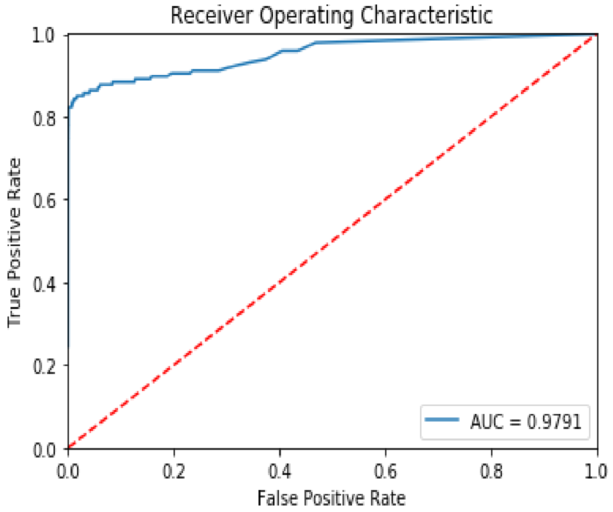

Fig.8. Results of Roc-auc curve on Autoencoders

The ROC-AUC curve using Random Forest Ensemble model is shown below.

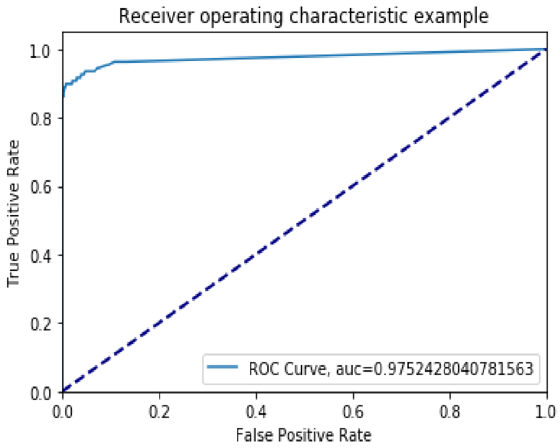

Fig.9. showing Roc-auc curve on test data of Random Forest.

The results of Supervised machine learning algorithm of Logistic Regression [23][24] is evaluated using ROC-AUC curve.

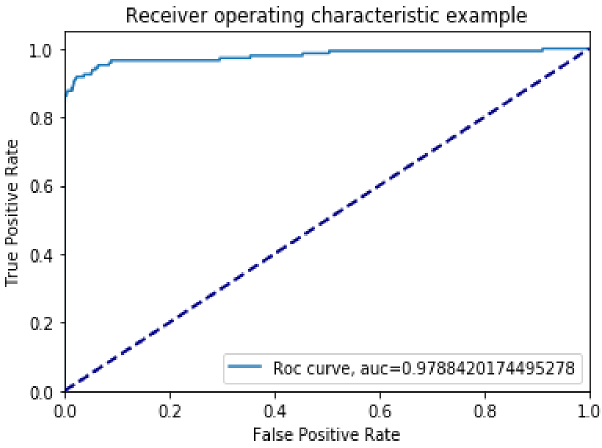

Fig.10. showing Roc-auc curve on test data of Logistic Regression

VIII. CONCLUSION

The threat of fraud in credit card transactions is always looming large and many companies are taking appropriate timely measures to tackle it. Machine learning algorithms [25][26] are the most appropriate solution to the problem of fraud detection. The generative models are able to generate all possible complex patterns or distributions within a small subset of data. Thus the dynamic evolving natures of fraudsters are tackled in a better way. The results of Variational autoencoder with a small subset which is randomly selected gave promising result as compared to supervised, unsupervised and semi-supervised deep learning algorithms with a much larger randomly selected dataset .

REFERENCES

1. Fraud The Facts 2019 The definitive overview of payment industry fraud ,2019[Accessed Oct 15th,2019 20:50]
2. Machine learning for email spam filtering: review, approaches and open research problems, Emmanuel Gbenga Dadaa,Joseph Stephen Bassia Haruna Chiroma Shafi'i Muhammad Abdulhamid Adebayo Olusola Adetunmbid Opeyemi Emmanuel Ajibuwae, ,Proceedings in Heliyon, Volume 5, Issue 6, June 2019

3. Early Detection of Breast Cancer Using Machine Learning Techniques ,M. Tahmooresi, A. Afshar, B. Bashari Rad, K. B. Nowshath and M. A.,2018
4. Breast Cancer Diagnosis Using Deep Learning Algorithm, Naresh Khuriwal ,Dr Nidhi Proceedings in International Conference on Advances in Computing ,Communication Control and Networking Proceedings in Journal of Telecommunication, Electronic and Computer Engineering,2018
5. Detection and prediction of credit card fraud transactions using machine learning, Kaithekuzhical Leena Kurien & Dr. Ajeet Chikkamannur, IJESRT,2019
6. MVAE: Multimodal Variational Autoencoder for Fake News Detection by Dhruv Khattar,Jaipal Singh Goud,Manish Gupta,Vasudeva Varma ,2019,International Institute of Information Technology,Hyderabad,
7. GEE: A Gradient-based Explainable Variational Autoencoder for Network Anomaly Detection,Quoc Phong Nguyen,Kar Wai Lim,Dinil Mon Divakaran,Kian Hsiang Low,Mun Choon Chan, arXiv.org ,March 2019.
8. FraudJudger: Real-World Data Oriented Fraud Detection on Digital Payment Platforms,Ruoyu Deng,Na Ruan, arXiv.org ,Sep 2019,
9. Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs,Yvan Lucas,Pierre-Edouard Portier,L ea Laporte,Liyun,He-Guelton3, Olivier Caelen3, Michael Granitzer2, and SylvieCalabretto, arXiv.org ,Sep 2019.
10. Adapting to Concept Drift in Credit Card TransactionData Streams Using Contextual Bandits and Decision Trees,Dennis J. N. J. Soemers,1 Tim Brys,1 Kurt Driessens,2 Mark H. M.Winands,2 Ann Now´e11.1Vrije Universiteit Brussel, 2Maastricht University,2018,Proceedings from The Thirtieth AAAI Conference on Innovative Applications of Artificial Intelligence (IAAI-18)
11. Credit Card Fraud Detection Using Autoencoder Neural Network,Ping Jiang (M.Eng),Jinliang Zhang (M.Eng),Junyi Zou (M.Eng),University of Western Ontario,2019
12. Variational Autoencoder based Anomaly Detection using reconstruction by Jinwon An, Sungzoon Cho Proceedings in 2015-2 Special Lecture on IE
13. Variational Autoencoder Based Synthetic Data Generation for Imbalanced Learning by Zhiqiang Wan, Yazhou Zhang, and Haibo He
14. https://www.guru99.com/supervised-vs-unsupervised-learning.html [Accessed Oct 16th,2019 10:50]
15. http://www.scholarpedia.org/article/Ensemble_learning [Accessed Oct 16th,2019 10:55]
16. https://www.geeksforgeeks.org/ml-stochastic-gradient-descent-sgd/ [Accessed Oct 16th,2019 10:58]
17. An Introduction to Variational Autoencoders ,Diederik P. Kingma,Max Welling, ,arXiv ,December 2017
18. https://jaan.io/what-is-variational-autoencoder-vae-tutorial/ [Accessed Oct 16th,2019 09:30]
19. https://towardsdatascience.com/intuitively-understanding-variational-autoencoders-1bfe67eb5daf [Accessed Oct 15th,2019 20:50]
20. http://www.scholarpedia.org/article/Ensemble_learning [Accessed Oct 16th,2019 09:32]
21. https://www.kaggle.com/mlg-ulb/creditcardfraud [Accessed Oct 16th,2019 09:35]
22. https://medium.com/tensorflow/variational-autoencoders-with-tensorflow-probability-layers-d06c658931b7 [Accessed Oct 16th,2019 09:37]
23. https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5 [Accessed Oct 16th,2019 11:50]
24. https://developers.google.com/machine-learning/crash-course/classification/roc-and-auc [Accessed Oct 17th,2019 20:50]
25. A Survey of Fraud detection techniques in Social Media,Leena Shibu, Dr.Ajeet Chikkamannur,IJETM,2014
26. A Survey on Methodology of Fraud Detection using Data Mining, Leena Shibu, Dr.Ajeet Chikkamannur,IJTSRD,2017
27. Benford’s Law and Deep Learning Autoencoders :An approach for Fraud Detection of Credit card Transactions in Social Media, Kaithekuzhical Leena Kurien, Dr. Ajeet Chikkamannur, IEEE International Conference (RTEICT-2019)May 2019, to be published.

AUTHORS PROFILE

Ms Kaithekuzhical Leena Kurien received her M.Tech. degree in Computer Science and Visvesvaraya Technological University, India. Currently pursuing Ph.D in Visvesvaraya Technological University with research center as R.L Jalappa Institute of Technology, her research is focused on Fraud detection in Social Media. Her research interests are Artificial Intelligence, Machine Learning, Generative Models, Object Oriented System Development and Database Management Systems. Published number of papers at National and International repute and taught many undergraduate courses.

Dr Ajeet A. Chikkamannur received his Ph.D. and M. Tech. Degree in Computer Science & Engineering from Visvesvaraya Technological University Belagavi in 2013 and 2001 respectively. Currently, he is working as Professor and Head, CSE Programme and Research Centre at Department of Computer Science and Engineering, R L Jalappa Institute of Technology, Doddaballapur, Bangalore. His research interests are Software Engineering, Reverse Engineering, Database Management Systems, Object Technology and IOT. He teaches several courses to Academia. He has organized conferences and delivered keynote, invited talks at conferences. Published number of papers at National and International repute. Awarded with best teacher.