

Credit Card Fraud Detection Using Federated Learning Techniques

R. Suvarna¹, Dr. A. Meena Kowshalya²

¹PG Scholar, Department of Computer Science and Engineering, Government College of Technology/Anna University, Coimbatore, Tamilnadu, India

²M.E, Ph.D, Assistant Professor, Department of Computer Science and Engineering, Government College of Technology/Anna University, Coimbatore, Tamilnadu, India

ABSTRACT

Frauds in Credit cards have become more usual in today's generation and many cases have been reported in the past with the increase in cybercrimes. Though there exist numerous techniques to detect online credit card fraudulence, deep-learning and federated learning techniques can efficiently detect accurate fraudulence. This paper exploits two unsupervised learning algorithms namely Auto encoder and Restricted Boltzmann Machine (RBM) implemented over a federated learning framework to predict number of credit card fraudulent users. - time European credit card dataset with 284,807 transactions are used to find the number of fraudulent users. The decentralized federated learning framework is compared against centralized approach. The average accuracy using federated learning for Auto encoder and RBM is 88% and 94% respectively and 99% and 92% using centralized deep learning approach. Federated Learning ensured high differential privacy compromising accuracy.

Keywords : Credit Card Fraud, Auto Encoder, Restricted Boltzmann machine, Federated learning, decentralized model

I. INTRODUCTION

Federated learning is a new branch in AI (Artificial Intelligence) that has opened eyes for a new era of Machine Learning. Federated Learning aims to train Machine Learning algorithms, for instance deep neural networks, on multiple local data containing local nodes without exchange of samples. The general principle is to generate a global model. It can exploit both decentralized data and decentralized computing power that can achieve more personalized experience without compromising on user privacy through homomorphic encryption. Federated Learning algorithms use a server where the encrypted train data is loaded. The data can be split into any number of chunks and can be given to different local nodes for training. The trained data is driven into the central server which will update itself with the trained data. The main difference between Federated Learning and distributed learning lies in the properties of the local datasets where distributed learning aims at training homogeneous datasets whereas Federated Learning aims to train heterogeneous datasets. Few examples of future federated learning are self-driving connected cars that leverages federated learning for safe driving, Credit card Fraud detection, healthcare for improving privacy. The advantages of using Federated Learning are to form smarter models with lower latency, less power consumption and improved privacy. It also has the ability to decouple which helps in the need to store the data in the cloud.

Federated Learning involves the following steps.

Step 1: Starts by training a generic machine learning model (dataset) in the server.

Step 2: The dataset in the server is sent to other multiple devices known as federated clients.

Step 3: The clients train the heterogeneous data and communicate it back to the central server.

Step 4: The new shared model is again sent back to the clients.

This cycle repeats again and again which helps the central server to get better and to make it more personalized.

This paper aims to detect the Credit card Fraudulence using Federated Learning algorithms namely Auto Encoder (AE) and Restricted Boltzmann Machine (RBM) in a federated learning set up. This paper uses a real time European dataset which consists of 2, 86,486 transactions with 32 features. The metrics used to evaluate the model are AUC curve, Accuracy and Confusion Matrix. A brief comparison of using deep learning algorithms and Federated Learning algorithms are made.

II. RELATED WORK

In [1] the paper proposes two deep learning techniques to detect the credit card fraud detection using few parameters. The result shows the increased accuracy of the fraudulence but privacy is lagging.

In [2], Credit card fraudulence is detected using a federated learning method. This paper evaluates the credit card FDS (Fraud Detection System) with FFD (Federated Learning for Fraud detection) framework for real-time dataset. This has resulted in increasing the AUC test average which is 10% higher than the deep learning methods. Feature engineering strategies in [3] gives a brief explanation about the measures to evaluate a fraud detection model by proposing a new saving measure based on comparing the financial cost of an algorithm versus using no model. The results of the proposed features increase the performance by

252 and 287% respectively. In [4] Federated deep learning model is used towards efficient and privacy preserving strategies which introduces a new protocol which is efficient based on stochastic gradient descent method by integrating the additively homomorphic encryption with differential privacy. This work has resulted with high efficiency and high accuracy with non-private training model.

The survey in [5] depicts the different types of fraud such as bankruptcy fraud, counterfeit fraud, theft fraud, application fraud and behavioral fraud. With addition to this, the measures for the fraudulence is also predicted using decision tree, pair-wise matching, clustering techniques, neural network and genetic algorithms. The statistical summary of using different techniques is shown and compared. In [6] the first privacy preserving approach Verify Net that supports verification in the process of training neural networks has been proposed which is a federated learning approach. This resulted in high security of verify net and is shown to be supporting for users dropping out in training process.

Client Selection for federated learning in [7] proposes methods to select the client for federated learning with heterogeneous resources in mobile edge. This work aimed to enable privacy-preserving training a model working with heterogeneous clients in a cellular network. The paper proposes a new protocol, Fedcs which resulted in providing high performance Machine learning with shorter time. In [8] Training strategies in Gaming Approach on mobile devices in Federated learning is proposed to maximize the individual utility and the stability and equilibrium of the game are analyzed theoretically. The results of the accuracy and energy consumption metrics are depicted. In [9] a feature fusion approach is proposed to aggregate the features in both local and global models to achieve high accuracy at less communication cost.

The resultant of this work is depicted in reducing the number of communication rounds by more than 60%. Paper [10] analyses the features of fraud detection problem and creates a new model using Support Vector Machine algorithm based on PCA (Principle Component Analysis) and ICW-SVM. This model has proved to be more practicability and adaptability but selection of kernel function is lagged. In the survey [11], the fraud detection by applying Employing transaction aggregation strategy. Dataset partitioning and its usefulness is derived for more accurate accuracy.

The authors in [12] proposed a model of deep autoencoder and Restricted Boltzmann Machine (RBM) to detect fraudulence in credit card transactions. These two models were found to be accurate for large datasets. Techniques presented in [13] give a brief analysis on credit card fraud identification by using KNN and Outlier detection which eliminates the false alarm rate. Classification is done by KNN algorithm and by calculating its nearest point. Both supervised and unsupervised learning is detected using Outlier detection Due to its less memory requirements unsupervised learning is preferred to treat the dataset.

The author in [14] proposed a profiling method to detect the fraudulence in credit cards using Timelier fraud detection method which helps in minimizing the time detection between detection and fraud occurrence. From an individual credit card account the patterns are inherited in a time series manner. These patterns are used to reduce the time between when a fraud occurs and when it is finally detected. The results gained are more accurate in finding the credit card fraud in timelier manner. Survey presented in [15] explains about the credit card fraud detection techniques for different types of frauds. This survey results in identifying the user model that best identifies fraud cases.

The authors in [16] discuss the credit card fraud detection techniques by using Data Mining and Big

Data approaches which helps in understanding and working on how to safe guard the credit card. This technique helps to minimize risk and response time. Techniques proposed in [17] are genetic algorithm and scatter search where the limit of the card is assumed and taken as the misclassification cost. This technique calculates the available limit of card based on the fraudsters' usage of the available limit. The algorithms in [18] discuss the card payment system using genetic algorithm which is based on Data Mining. The optimal solution is established to generate the result using the genetic algorithm by developing a method of generating test data. The result predicts the fraudulent transactions and the results are based on the principles of this algorithm.

The method proposed in [19] are K-Clustering Model and Hidden Markov Model for understanding the sequence of transaction and for generating clusters by categorizing the card holder's profile as low, medium, high spending based on their spending behavior with the basement of amount. The models are found to be speeding in detecting fraudulence. The credit card fraudulences is detected if the incoming credit card transaction is not accepted by the trained HMM. Fraudulence detection of credit card in [20] is done by Decision tree and Support Vector Machine (SVM) models. Fraud detecting models are built by using seven classification methods. Comparing the models decision tree predicts credit card frauds more accurately than the other models for real time datasets. But, the number of frauds caught by SVM models are still far less than the number of frauds caught by decision tree methods.

Credit card fraud detection technique in [21] discusses the fusion approach using Dumpster-Shafer theory and Bayesian learning which is used to combine evidences. It determines the suspicion level of each incoming transaction based on the extent of its deviation from good pattern. These techniques results in learning the problem patterns more accurately. Fraudulent detection using Hybridization in [22] is proposed by BLAST-SSAHA technique where the two sequence alignment algorithms are joined together to analyze the profile, deviation and for synthetic transaction. This is more effective compared to the existing domains.

The authors in [23] use game-theoretic model which doubts and detects the next step of the fraudster. The author in [24] presents the automated credit card fraud detection by means of Bayesian and Neural Network models. These two techniques are applied to problems and significant results are obtained 10% and 15% of fraudulence were detected. By comparing the two methods it shows that Bayesian networks yields better result as compared to artificial neural network.

III. PROPOSED WORK

M-Commerce and E-Commerce are not new. The consumer orders the product via internet by using the credit card payment method. The issuing bank sends the transaction to the acquiring bank by sending the amount of money, date and time of payment. The credit card fraud detection system is used to validate the behavior of credit card. The credit card fraud system requests consumer's profile from the database to bring their behavior into the AE and RBM by using deep learning. Based on the AE, the acquiring bank transfers the input that is the amount of money, date and time etc. The AE uses past behavior to be trained first, and then uses the new coming transaction as a validation test for the transaction. AE does not use labeled transactions to be trained, because it is unsupervised learning. RBM uses all transactions that transfer from acquiring bank as visible input and is fed to the hidden node. After activation, the RBM reconstructs the model by transferring the new input from the activation function back to the visible function. If the transaction is fraudulent, the system will record the transaction as a fraud in the database and will reject it. The acquiring bank sends a SMS alert to the real consumer that the system suspects the transaction as fraudulent as shown in fig 1.

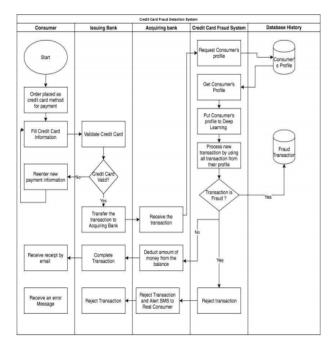


Fig 1. Architecture of fraud detection

This paper detects fraudulence by applying federated learning for training and testing of data. In Federated learning, there is a central server which contains the complete dataset, following with any number of local nodes that the user needs to process. We train and test the data by splitting it into 3 workers. The data is divided into three chunks and then fed into the 3 workers (local nodes) separately. The result of each local node is fed back into the central server, where the results are combined and a new model is formed and this cycle continues till the data are trained at its best level as shown in fig.2. Auto Encoder and RBM techniques are used to detect the fraudulence using a federated learning model. The main advantage of federated learning is that, it increases the privacy of the dataset and training and testing will be more accurate.

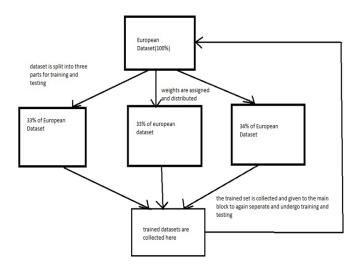


Fig 2. Architecture of federated learning.

For experimentation, a European dataset possessing cardholder information from September 2013. The dataset holds 284, 807 transactions with 31 features.

Auto Encoder:

The data is split into training and testing data. They are trained and tested through federated learning. The results of these data are given to the deep neural network and auto encoding is done. One input layer, 7 hidden layers and one output layer are chosen for the process. Forward feeding input layer is set with the bias of value 1. Activation is done in the hidden layer using relu and tanh (hyperbolic tangent function). Encoding and decoding is done in each of the hidden layer and the result is received in the output layer. The error from the output(if any) is detected. Back Propagation computes the error signal and propagates the error backward through network starting from the output layer. The bias in the hidden layer is ser as 1. The error is computed with the condition of the difference between the actual value and desired value. The process continues until it satisfies the output limit of 0 or 1. The factors are calculated such as model loss, recall and precision, ROC. Graphs are obtained for each factor and the accuracy is also plotted in the increasing manner.

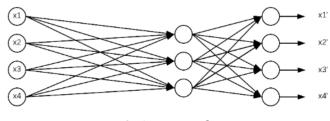


Fig 3. Auto encoder

Let v1, v2,....vn be the set of features, let w1,w2,....wn be the weights

The datas are trained and tested using federated learning.

X_train,X_test,y_train,y_test= train_test_split(x,y,test_size=0.2) Split into two workers Bobs_model = net() Alices_model = net()

Input the feature set and weights to the auto encoder neural network

Perform Activation function in hidden layer using tanh (tangent function)

Perform Encoding and decoding in the hidden layers ecoding

$$h(x) = g(a(x))$$

 $= tanh(Wx) \longrightarrow eqn.1$ Decoding $x^{\wedge} = O(a^{\wedge}(x))$ $= tanh(Wx * h(x)) \longrightarrow eqn.2$

Reconstructing the error by Backpropogation is done by finding the error rate of the feed forward output. To minimize the error they are fed to the output layer as input and the bias during backpropogation is set to 1 in the input layer. Backpropogation is used here since it updates the values automatically as it undergoes the process. The variation is obtained by finding the difference between the Actual error and desired error.

360

RBM:

The second technique applied is the RBM which is a different frame of network compared to other deep neural networks because it consists of only input layer and hidden layers and it does not consists of any output layer. The output is reconstructed back to the input having the bias of hidden layer as 1. The data is fed to the input layer with bias assumed to be 1 and then to the hidden node where activation is done using sigma (sigmoid function) and then the output is reconstructed. RBM reconstructs the model by transferring the new input from the activation function back to the output or visible function. During the activation function the energy along with the joint probability and entropy is calculated.

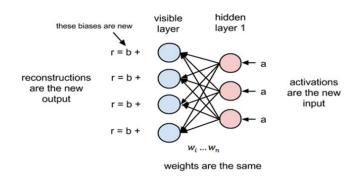


Fig 4. Restricted Boltzmann Machine

Let $\{v1, v2,...,vn\}$ be the set of features, let $\{w1,w2,...,wn\}$ be the weights

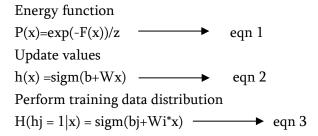
The datas are trained and tested using federated learning method.

X_train,X_test,y_train,y_test= train_test_split(x,y,test_size=0.2) Split into two workers Bobs_model = net() Alices_model = net()

Input the feature set and weights to the auto encoder neural network

Perform Activation function in hidden layer using sigm (sigma function)

Perform Activation in hidden layer with sigm(sigmoid function) and by finding free energy and uniform distribution



The reconstruction error is basically the mean squared of the difference between predicted and the actual data x. reconstructing the error by Backpropogation is done same as in AE but here in RBM it does not consist of output layer. The output for RBM is the value obtained during the reconstruction.

IV. EXPERIMENATAL RESULTS

Python libraries namely sklearn, numpy and tensor flow are used for data analysis, mathematical functions, classification, prediction and to obtain data flow graphs. The average accuracy of Auto encoder is 94% and RBM is 88% for European dataset respectively. The AUC curve achieved a result of 0.94. The model loss, recall and precision, recall and precision using threshold values and ROC is attained in the form of graphs. The confusion matrix is found for both the datasets on applying the two deep learning techniques.

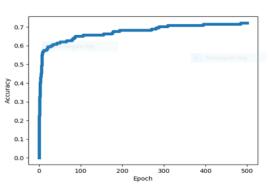
V. ACCURACY PERCENTAGE

| | DEEP | FEDERATED |
|---------|----------|-----------|
| | LEARNING | LEARNING |
| AUTO | 99% | 94% |
| ENCODER | | |
| RBM | 92% | 88% |

Table 1. Accuracy Percentage

361

AUTO ENCODER: ACCURACY:





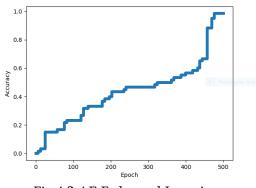
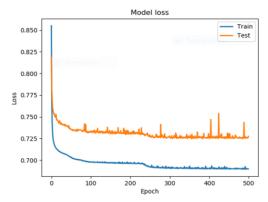


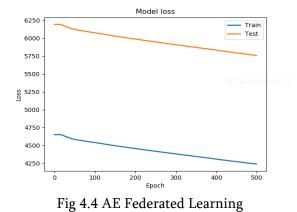
Fig 4.2 AE Federated Learning

The accuracy percentage for European and Australian datasets using Auto encoder is 73% and 99% respectively.

MODEL LOSS

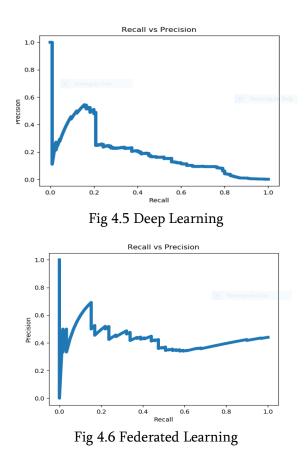






The Model loss for both the datasets is shown is figure 4.3 and 4.4 where the loss of model is graphed in the decreasing order.

RECALL AND PRECISION



The above shown graphs in figure 4.5 and 4.6 illustrate the recall and precision parameters for both the datasets.

RECALL AND PRECISION USING THRESHOLD

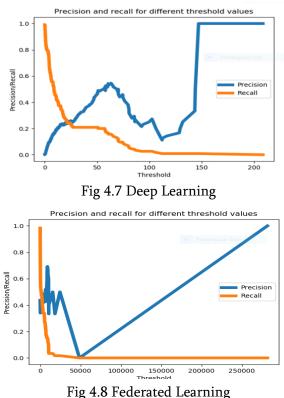


Fig 4.8 Federated Learning

The above shown graphs in figure 4.5 and 4.6 illustrate the recall and precision using the threshold values for both the datasets.

ROC

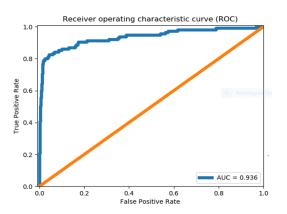


Fig 4.9 Deep Learning

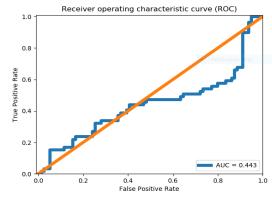


Fig 4.10 Federated Learning

The Receiver Operating Curve (ROC) for the both the datasets shown in figures 4.9 and 4.10 illustrates the performance of the classification model.

CONFUSION MATRIX

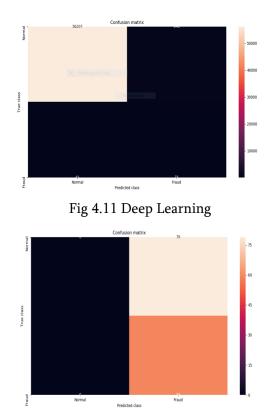


Fig 4.12 Federated Learning

The Confusion Matrix for both the datasets are obtained that specifies a table layout that allows visualization of the performance using auto encoder technique and it shows the number of normal transactions, fraud transaction and confusion matrix.

363



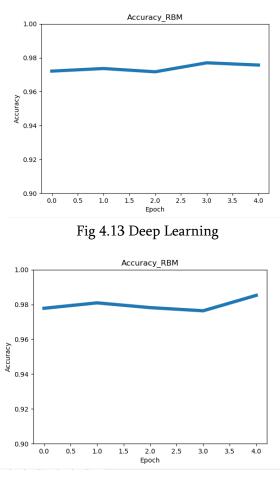
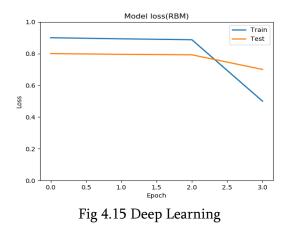


Fig 4.14 Federated Learning

The accuracy percentage for European and Australian datasets using RBM is 98% and 92% respectively.

MODEL LOSS



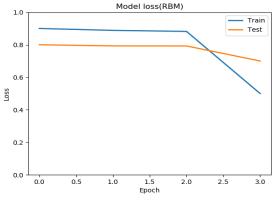


Fig 4.16 Federated Learning

The Model loss for both the datasets is shown is figure 4.15 and 4.26 where the loss of model is graphed in the decreasing order

RECALL AND PRECISION

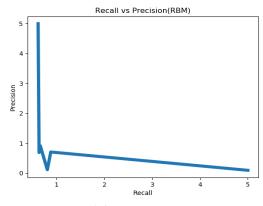
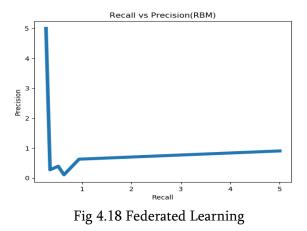
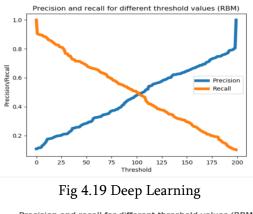


Fig 4.17 Deep Learning



The above shown graphs in figure 4.17 and 4.18 illustrates the recall and precision parameters for both the datasets.

RECALL AND PRECISION USING THRESHOLD



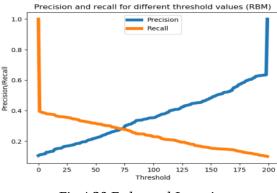
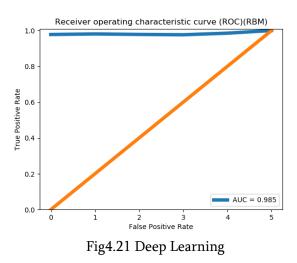


Fig 4.20 Federated Learning

The above shown graphs in figure 4.19 and 4.20 illustrates the recall and precision using the threshold values for both the datasets

ROC



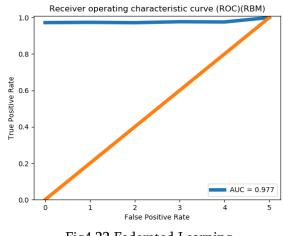


Fig4.22 Federated Learning

The Receiver Operating Curve (ROC) for the both the datasets shown in figures 4.9 and 4.10 illustrates the performance of the classification model.

CONFUSION MATRIX

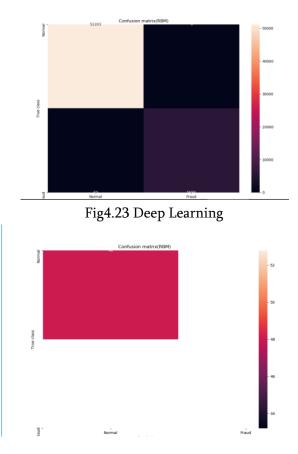


Fig4.24 Federated Learning

The Confusion Matrix for both the datasets are obtained that specifies a table layout that allows visualization of the performance using RBM technique and it shows the number of normal transactions, fraud transaction and confusion matrix.

VI. CONCLUSION

Fraud detection online is globally pandemic now-adays. As fraudsters create irregular patterns that match the original, there is a need of a stronger technique to detect online frauds preserving privacy of users. We have used unsupervised deep learning and federated learning techniques to detect online frauds ensuring privacy. Comparing the deep learning techniques without federated learning and with federated learning, the accuracy is being reduced using federated learning whereas the privacy has been increased when using federated learning. When comparing the two techniques with federated learning, RBM attains a higher efficiency with greater accuracy than Auto encoder whose accuracy is less because when comparing the original pattern and fraud pattern showing completely different patterns is considered to be genuine.

VII. REFERENCES

- [1]. Suvarna. R, Dr. A.Meena Kowshalya, 2020, Credit Card Fraud Detection Using Deep Learning Techniques, Journal of Web Engineering and Technology, sISSN: 2455-1880, Vol. 7, Issue 1, April.
- [2]. Wensi Yang, Yuhang Zhang, Kejiang Ye, Li Li, Cheng-Zhong Xu, 2019, Ffd: A Federated Learning Based Method For Credit Card Fraud Detection, Springer Journal Big Data 2019,LNCS 11514, pp. 18–32.
- [3]. Meng Hao, Hongwei li, Guowen Xu, Sen Liu and Haomiao Yang, 1 June 2016, , Feature engineering strategies for credit card fraud detection.
- [4]. Albertio, chiung, International Conference on Science and Technology on Communication Security Laboratory, 978-I-5386-8088-

9/19@IEEE, Towards Efficient and Privacypreserving Federated Deep Learning.

- [5]. Wei Yang Bryan Lim, Nguyen cong Luong, Dinh Thai Hoang, Yutao Jiao, Ying-Chang Liang, 26Sep 2019, International Conference on Science and Technology arXiv:1909.11875vl cs.NIFederated learning in Mobile Edge Networks: A Comprehensive Survey.
- [6]. Xu, Hongwei Li, Sen Liu, Kan Yang, Xiaodong, 2019, VerifyNet: Secure and verifiable Federated Learning, Guowen, China, Journal of Transaction pn Information Forensics and security, 1556-6013© IEEE.
- [7]. Takayuki Nishio, Ryo Yonetani, Japan, 2019, Client Selection for Federated Learning with Heterogeneous Resources in Mobile Edge, JST ACT-I Journal of Computer Science 978-1-5386-8088-9/19© IEEE.
- [8]. Yuze Zou, Shaohan Feng, Dusit Niyato, Yutao Jiao, Shimin Gong and Wenqing Cheng, 2019, Federated Learning: An Evolutionary Game Approach, International Conference on Internet of Things(iThings) and IEEE Green Computing and Communications(GreenCom) and IEEE Cyber 978-17281-2980-8, Physical and Social Computing(CPSCom) and IEEE Smart Data(SmartData), Mobile Device Training Strategies.
- [9]. Xin Yao, Tianchi Huang, Chenglei Wu, Ruixiao Zhang, Lifeng Sun, China, 2019, Towards Faster And Better Federated Learning: A feature Fusion Approach, International Conference on Compuer science and Engineering 978-1-5386-6249-6/19 © IEEE.
- [10]. Qibei Lu, Chunhua Ju, January 2011, Research on Credit Card Fraud Detection Model Based on Class Weighted Support Vector Machine, Journal of Convergence Information Technology, volume 6, Number 1.
- [11]. Sanjeev Jha, Montserrat Guillen, J. Christopher
 Westland, 2012, Employing transaction
 aggregation strategy to detect credit card fraud,

International Journal On Expert Systems with Applications 0957-4147.

- [12]. Apapan Pumsirirat, 2018, Credit Card Fraud Detection using Auto-Encoder and Restricted Boltzmann Machine, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 1.
- [13]. Detection N.Malini, Dr.M.Pushpa, 2017, Analysis on Credit Card Fraud Identification Techniques based on KNN and Outlier, 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEEICB17) 978-1-5090-5434-3© IEEE.
- [14]. Ekrem Duman a, M. Hamdi Ozcelik Dogus , Istanbul, Turkey b Yapi Kredi Bankasi, IT Department, Istanbul, Turkey , Detecting credit card fraud by genetic algorithm and scatter search.
- [15]. Venkata Ratnam Ganji Gudivada A.P,India. Credit card fraud detection using anti-k nearest neighbor algorithm, International Journal on Computer Science and Engineering (IJCSE).
- [16]. K.RamaKalyani, D.UmaDevi, Fraud Detection of Credit Card Payment System by Genetic Algorithm, International Journal of Scientific & Engineering Research Volume 3, Issue 7, July-2012 1 ISSN 2229-5518 IJSER.
- [17]. Mohd Avesh Zubair Kha1, Jabir Daud Pathan2, Ali Haider Ekbal Ahmed, 2014, Credit Card Fraud Detection System Using Hidden Markov Model and K-Clustering, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2.
- [18]. Y. Sahin and E. Duman ,2016, Detecting Credit Card Fraud by Decision Trees and Support Vector Machine, International Multiconference of Engineers and computer scientists 2011 vol1 IMECS 2011, March 16-18.
- [19]. Amlan kundu, suvasini panigrahi, shamik sural and arun k. majumdar, 2009, blast-ssaha hybridization for credit card fraud detection,

ieee transactions on dependable and secure computing, vol. 6, no. 4.

- [20]. Suvasini Panigrahi a , Amlan Kundu a , Shamik Sural a, A.K. Majumdar , 2019, Credit card fraud detection: A fusion approach using Dempster– Shafer theory and Bayesian learning
- [21]. Leila Seyedhossein, 2010, Mining Information from Credit Card Time Series for Timelier Fraud Detection, 5th International Symposium on Telecommunications (IST'2010).
- [22]. N.Malini, Dr.M.Pushpa, credit card fraud detection techniques by data mining and big data approach, International journal of research in computer applications and robotics issn 2320-7345 analysis.
- [23]. Shamik Sural2, and A.K. Majumdar, 2019, A Game-Theoretic Approach to Credit Card Fraud Detection Vishal Vatsa1.
- [24]. Priya Ravindra Shimpi, Prof. Vijayalaxmi Kadroli, 2015, Survey on Credit Card Fraud Detection Techniques, International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 4 Issue 11 Nov 2015, Page No. 15010-15015.

Cite this article as :

R. Suvarna, Dr. A. Meena Kowshalya, "Credit Card Fraud Detection Using Federated Learning Techniques", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 3, pp. 356-367, May-June 2020.

Journal URL : http://ijsrset.com/IJSRSET207380