A Comparative Study for Credit Card Fraud Detection System using Machine Learning (ML)

Devang Barot[1], Saket Swarndeep[2]

[1]Student of Master of Engineering, Ahmedabad, Dept. of Computer Engineering, L.J University, Gujarat, India.
[2]Assisstant Professor, Dept. of Computer Engineering and Technology, L.J University, Ahmedabad, Gujarat, India

---***---

Abstract - *There are many Credit Card Fraud Detection System in two days world. This paper is going to discuss about the various techniques used in Credit Card Fraud Detection and also how the datasets are chosen or pre-processed to build the Machine Learning, Deep Learning, Neural Network models. We will be going to discuss various models like neural networks, decision tree, logistic regression, Random Forest, Parallel Granular Neural Networks, Multivariate control chart , Gaussian Kernel, Meta-Learning, Computational Intelligence, Convolutional Neural Networks, Neural Network on the basis of Mining System, Self-Organizing Maps, Generative Adversarial Networks, Pipeling, Ensemble Learning, AdaBoost, Majority Voting, Deep Convolution Neural Network Model, Adversarial Learning, Fuzzy Clustering, Optimized Light Gradient Boosting, anti-k nearest neighbour, Calibrated Probabilities, bidirectional Long short-term memory (BiLSTM), bidirectional Gated recurrent unit (BiGRU), Genetic Algorithm, Class Balancing Techniques, Auto-Encoder, Restricted Boltzmann Machine, Cat Boost, Light Gradient Boosting Machine.*

***Key Words*: Credit Card Fraud Detection, Credit Card Frauds, Machine Learning, Deep Learning, Detection Methods, Classifiers**

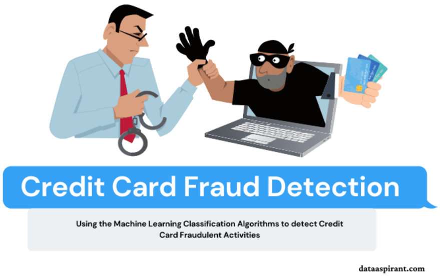
Credit Card Fraud Detection
Using the Machine Learning Classification Algorithms to detect Credit Card Fraudulent Activities
dataaspirant.com

Fig - 1: Credit Card Fraud Detection System [16]

1.INTRODUCTION

Credit Card had made daily life much easier. Daily payments can be done in no time but every coin has 2 sides all things all pros and cons. Credit card has Credit card frauds as the most important con. Credit card frauds can be virtual or physical. Credit card fraud is a growing menace these days. It is a process in which third party do the money transaction without permission or under observation of the card holder. So, to overcome these frauds there are many frauds detection system has been created by the use of Python, Machine Learning, Deep Learning. Credit Card Fraud Detection System is a system or an algorithm or combination of multiple algorithms which prevent the fraud transactions to be happening and if fraud transition happen it will inform the user about the fraud transaction is detected.

Fig - 2: Credit Card Frauds [15]

1.1 Machine Learning and Deep Learning Algorithms

Machine Learning: It is a branch of Computer Science which takes the previous data and learn from it and built a model on the bases of which we give the future predictions. Machine learning is taking over all the other techniques today world is using. Machine learning have various amount of algorithm which can help us in predictions.

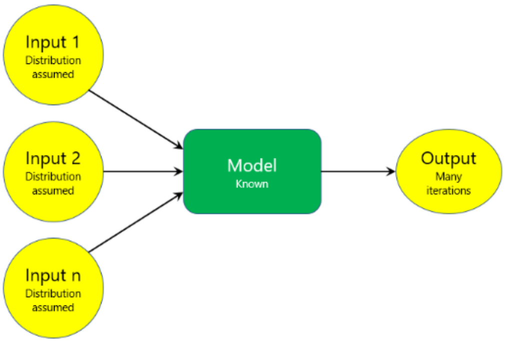

Fig - 3: Basic Model of Machine Learning [17]

Machine Learning has 3 main techniques they are:

1. **Unsupervised Learning: -** Unsupervised Learning is a technique which uses unlabelled data and learning do not take place under supervisor. Output is not known to user

2. **Supervised Learning: -**
   Supervised Learning is a technique which uses labelled datasets and learning takes placed under supervisor.
   Output is known to user.

3. **Reinforcement Learning: -**
   In this process negative and positive reward are given on the basis of the action and decision they take. Machine observes the rewards act accordingly.

Deep Learning: WE can say that the deep learning is the extended version of the machine learning or a part of machine learning where artificial neural network is used where extraction of high features takes place from the datasets where multiple layers of processes is used.

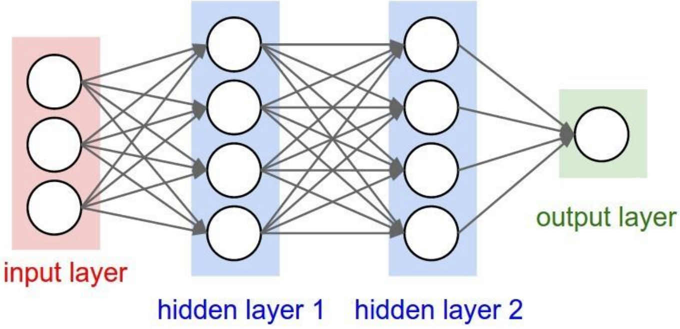

Fig - 4: Basic Model of Deep Learning [18]

1.2 Literature Survey

In [1], they talked about how to use meta learning for detection of fraud. the system they building has 2 important components which are Local Fraud Detection Agents and Meta Learning Agent. Local Fraud Detection Agents detect the intrusion by learning previous frauds in a single system. A generated new classifier agent is made up of 2 or more classifiers by meta learning agents.

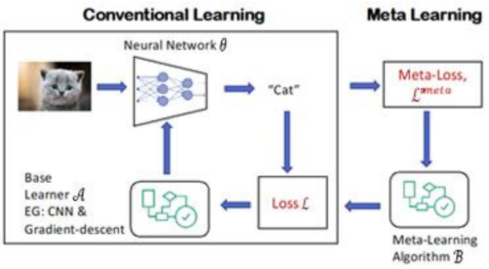
Conventional Learning
Meta Learning
Neural Network θ
"Cat"
Meta-Loss, $\mathcal{L}^{meta}$
Base Learner $\mathcal{A}$ EG: CNN & Gradient-descent
Loss $\mathcal{L}$
Meta-Learning Algorithm $\mathcal{B}$

Fig - 5: Basic Model of Meta Learning [19]

Meta learning gives you how to learn and combination and integration of numbers of separated learned classifiers or models. Multiple U.S banks contributed data for this fraud detection simulation. The database contains 500000 records and each record were having 30 fields. The data which was provided by the banks where labelled as the fraud transaction and non-fraud transaction. Data between January and October was taken as training data and validation in meta data was done in month of November. December's data was taken as testing data. They consider 42000 data randomly for training purpose and 4000 data from the November month for the meta learning validation. to test the data, they had taken 4000 records for testing purpose. They have use ID3 and CART. The learning process of both the algorithms are based on the decision trees. The process of getting base classifier for meta learning to use class-combiner. Experiment was caried out twice and 1600 times each combination was processed. The Data was distributed in the percentage of 50-50 fraud/non-fraud. The true positive rate generated was 80% and false positive was less than 16% and this distribution generated a maximum fraud detection rate and minimum amount of alarm rate. For the future aspects they gone be using sliding window for the selection of training data from the previous months.

Neural Networks [2] had also played an important role in Credit card fraud detection. We are going to discuss about conversation neural network and how it going to help in credit card fraud detection. Feature Matrix has been used for the abandoned transactions data. At first, they have given the small description about CNN-based fraud detection framework after getting idea about fraud detection Framework secondly, they who introduced us to the novel trading features and third step will be solving problem of credit card fraud detection the first two initial step is that the training part will be done offline and the prediction part will be online. When the transaction will arrive, the system will judge whether the following transaction is legitimate or fraudulent in no time. Following three initial steps will be taken and that is a feature selection feature transformation and classification module. CNN had been used because it is very convenient for the large size of data and also it is very helpful for avoiding the overfitting of the model. There are many applications of convolution neural network and two of them are image classification and speech signal processing. From the original attributes of transaction which generate a one dimensional which are then transformed into feature matrices

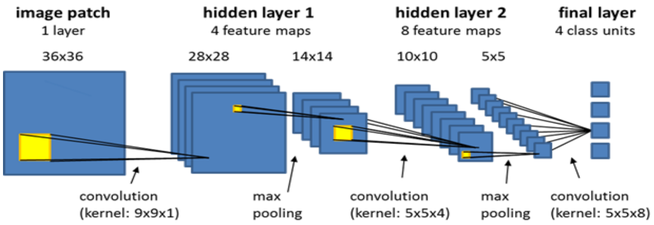

Fig - 6: Basic CNN Model [20]

We randomly select the samples which can be fraudulent or legitimate in order to generate heat maps. In the model there are six mean players. First layer content convolution layer which is then followed by sampling layer third layer is also called convolution layer and the last three contain all the connectivity which is named as a fully connection layer the data is taken from the traditional commercial banks and the data set contains to 260 million transaction records in which rest of the data is legitimate transaction and only 4000 transactions were fraudulent. Did to the data from January to December as a training data and the records of 11 word taken for the testing purpose. The results of CNN model were compared with the other algorithms and it is resulted that CNN model on various samples achieve the best performance from all of the other algorithms After the algorithm is process F1 score is decided on the basis of F1 score performance is evaluated of the model**.**

This paper [3] talks about how the data mining system can help in credit card fraud detection. The basic target behind this idea is to extract implicitly interesting and unknown knowledge from the database. The approximate number says that a Visa card and MasterCard users' loss approximately 700 million in US as a fraud credit card charge. Sing in the present tense feedforward network architecture are implemented in the CARDWATCH the cardboard system consists of five main models which are global constant module GCM Core Graphical User Interface Module GUIM Database Interface Module DBIM Learning Algorithm Library LAL Learning Algorithm Interface Module LAIM. Card watch is a fraudulent detection system. And talking in the present times only feed forward network architecture are implemented in garbage they have used 3-layer neural network functioning purpose. Auto associative network has been used for the training purpose in order to reproduce legal patent which is fresh and new but they cannot reproduce fraud patterns the major drawback of the system was they use one network for customer restrictions. They created a fake card holder in order to generate this user they have used 3 transaction generator inputs starting point of transaction consist of set or 323 transactions with number of three different purchase categories which have period of 365 days costly 264 transaction work given for the training purpose hence they have 3 purchase categories so the inputs were given in the unit of 7-7-7 in architecture of network RMSC was used to determine whether the transaction is legal or fraudulent after this system was tested it generate 85% of fraud detection rate and hundred percent of legal transaction identification rate this system has a GUI interface very friendly. For the future purpose the card watch will be extended for the use of general purpose of anomaly detection.

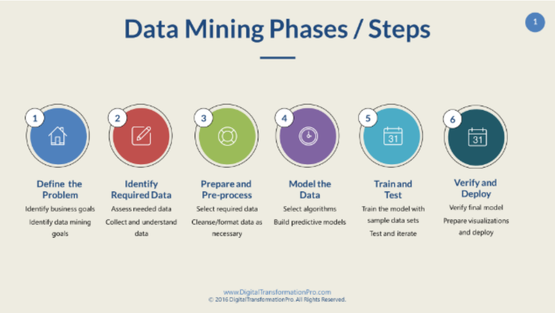
Data Mining Phases / Steps
1
1
Define the Problem
Identify business goals
Identify data mining goals
2
Identify Required Data
Assess needed data
Collect and understand data
3
Prepare and Pre-process
Select required data
Cleanse/format data as necessary
4
Model the Data
Select algorithms
Build predictive models
5
Train and Test
Train the model with sample data sets
Test and iterate
6
Verify and Deploy
Verify final model
Prepare visualizations and deploy
31
31
www.DigitalTransformationPro.com
© 2016 DigitalTransformationPro. All Rights Reserved.

Fig - 7: Data Mining Procedure [22]

When there is attack on machine learning algorithms and the way we are going to tackle that attack's this type of learning is called that was adversarial learning. In [4] adversarial learning is used for detecting the fraud. To generate a model of fraudster best strategy they have used game theoretical adversarial learning approach. For the classification of fraudulent and non-fraudulent transaction they have used Logistic regression. Test results shows that statistic model does not perform well while adversary aware classifier is better than static model. Adversary a classifier has increase under the curve score. They are using SMOTE in order to balance the class ratio by generation of synthetic instances of fraudulent transactions in the version of version sampling. The process is like ok choice between strategies are given opportunity is given to the classifier that it can utilize the same class a fire or Re train the classifier. ROC curve with adversarial learning had shown growth an area under the curve is went up to 0.78 to 0.84. It is also noticed that as the round proceeds performance of classifier.

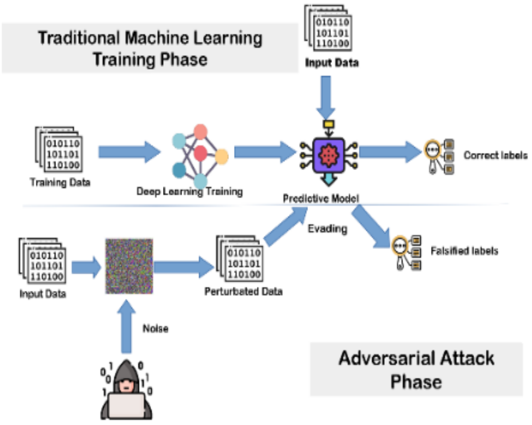

Fig - 8: Adversarial Learning [21]

This research paper [5] has use the hybrid approach in which day have use two methods which are fuzzy clustering and neural network. Clustering where data point belongs to one or more clusters is known as fuzzy clustering. Neural network consists of input layer hidden layer and output layer and also consists of nodes. Neural network act as a human brain. Because of overlapping nature of cluster boundaries, the usage of hard clustering is limited in physical world application. Due to unavailability of real-life credit set the data set has been developed by Panigrahi. The synthetic transaction is generated by use of Gaussian distribution that shows the behaviour of Genuine user as well and fraudulent user the Simulator reflects the real-life scenario those are usually seen in credit card transaction processing system. MATLAB- 2014 is used in the implementation of fraudulent detection system fuzzy c means algorithm module is provided input vectors as input. Suspicion score is calculated for each and every data point there in the cluster by the help of Euclidian distance. They have determined to threshold value which are lower threshold and upper threshold. The upper threshold value is said to 0.72 and lower threshold value is set to 0.28. If the going on transaction has a suspicion score value more than threshold value then it is as discarded from the cluster. Suspicion table contain values whose suspicion score lie between upper threshold and lower threshold. Learning takes place when the suspicion table are fed to the machine learning layer where SGC back propagation algorithm processes it. 5 hidden layer is used to train the network. Results keep getting better when the number of hidden layers is increases but as a consequence computation time also increases. The data sheet is divided into 3 categories it consists of 15% of validation 70% of training face and 15% of testing. When the algorithm is processed the results, we get our are 93.9 are correct classification transactions and 6.1% are incorrectly classified transactions. For the future purpose they will be experimenting different algorithms to.

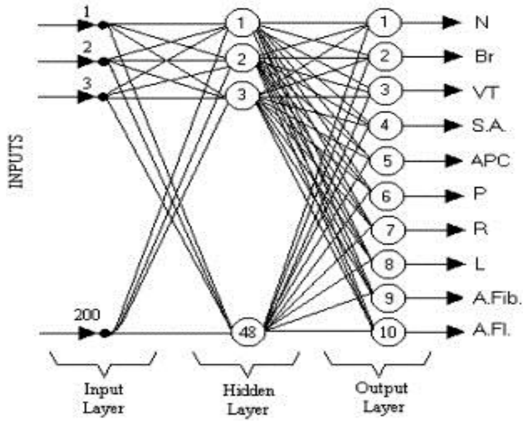

Fig - 9: Sample of Fuzzy Clustering and Neural Network [23]

In [6] order to integrate the parameters of light gradient boosting basin system hyperparameter optimization algorithm is used. This experiment was performed by the help of 2 real world public credit card transaction data set. This system discriminates between legitimate and fraudulent credit card transactions. The utilization to optimize parameter of light gradient boosting is the main contribution of this research. Intel Core i7 Processor is been used with 8GB RAM in this experiment techniques of machine learning are also used. 284807 credit card transaction records are contained by first data site which is owned in September 2013 in Europe. UCSD-FICO data mining contest 2009 data set is our second data set which contains e commerce transaction. Fivefold procedure was conducted using to Real world data. Cross validation process was employed to get the reliable comparison. This system achieves AUC 90.94% in data set 1 and 92.9% in data set 2. The value of recall score went up to 40.5% in data set 1 and 28.3% in data set 2. But this results it can be ensured that fraud detection rate went up to 40%. AUC score of RF algorithm stands on 2nd position by achieving 90.9 it % and 92.8%. SVM algorithm stands on the last position as it achieves the lowest area under the curve score of 47.8% and 70.90% for the data set 1 and data set 2.

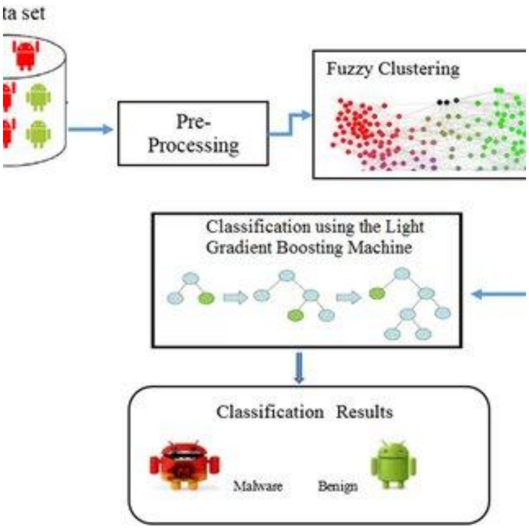

Fig - 10: Basic process using Light Gradient Boosting[24]

This paper [7] gives the information about how anti k-nearest neighbour algorithm can be used for the detection of the fraud. Traditional technique and modern techniques are 2 common forms of credit card fraud. Application fraud is type of traditional techniques and intercept fraud is a type of modern technique. This particular system uses trim outliner detection based on reversed k-nearest algorithm. There are two main procedures of this algorithm which are stream manager and the query manager. The incoming data stream object is received by the former procedure and the current window efficiently update it. We need to update knnlist and rknnlist to maintain current window perfectly. Random data set size is chosen which includes 10,000 multidimensional space points data which is uniformly distributed on different dimensions. The pros of this proposed model were the record of lost and stolen car features makes it handy to stop fraudulent transaction. Error detection in sequence of numbers hands detect invalid number easily buy credit card validation checks. Concluding this paper by letting all know that the number of scans is been reduced by this algorithm is only one. The proposed method is efficient and effective on both synthetic and real data set.

In [8] order to experiment contacts of credit card fraud detection 2 different methods of calibrating probability are used which aims to find the model that lessens the Real-World loss of credit card transactions. The first method includes of adjustment of probabilities on the parameters of difference in bad rate among the training and testing data sets and for the second method calibrated property are taken after the modification of receiver operating characteristic curve. Big European company had provided data set with the transaction between January 2012 to June 2013. State-of-the-art fraud system is implementing the current version of the system. Probability of random forest algorithm is used by the BMR bade use of Under sample and training data set RF algorithm is train by doing this observation of various positive base rates is possible. Scikit learn is implemented in order to use RF algorithm. Parameters of RF is tune in order to get good range of possibilities of estimates. For the construction purpose with BMR logistic integration and decision trees also used. In order to get better results, we found that BMR model is used. It is observed that when BMR model is used the fraud detection rate increased as well as precision was also maintained. Savings leads to 41.7%. LR-u-cal ROCCH-BMR is considered to be best model so far. Finally, 5820 euros rise in the model. 49.26% saving again the option of contact in every client. Paper is ended by saying that it only by use of raw possibilities bayes minimum risk are performed outperformed.

Machine learning and deep learning is a rising technologies in today's world. So, this paper [9] talks about how machine learning and deep learning can be implemented in the detection of fraud transactions. The data set for this experiment was provided by Kaggle. The model De used in this experiment BiLSTM- MaxPooling-BiGRU-MaxPooling is basically based on bi directional the memory and bidirectional Gate recurrent unit. Not only this day also applied some machine learning classifiers like naive base, voting, ada-boosting, random forest, decision tree and Logistic regression. One of the biggest problems to build a credit card fraud detection system is lack of good data sets. The data sets are highly in balance and contains not known fields that's why data pre-processing is needed. Some evaluation measures used in this experiment were catching rate, false alarm rate Matthew's correlation Coefficient balance classification. Best of performance is achieved by decision tree which is based on bagging classifier and results also shows that T2 do not perform better than OCVM. OCVM give the accuracy of 96.6% and it's FPR is 8.5% also its F-score is 100%. A data set contains 569875 labelled as legitimate transactions on the other hand there are 20663 transactions are fraudulent transactions. As we have a balance data three techniques have been used to resolve this problem SMOTE technique random over sampling, random under sampling. By doing hard voting with the help of under and over sampling the area under the curve that we achieve is 80% and 81%. Max pooling is applied to both the algorithms bidirectional Long short-term memory and bidirectional Gated Recurrent Units. By use of under sampling, random oversampling and SMOTE was not very promising. Thus, it is observed that better results are achieved by using deep learning rather than machine learning models. Area under the curve was 80% and 81% by the use of hard voting when we use machine learning classifiers by applying under Sampling and over sampling. In fact our model achieves the better results than machine learning model which achieves the area under the curve is equal to 91.37%.

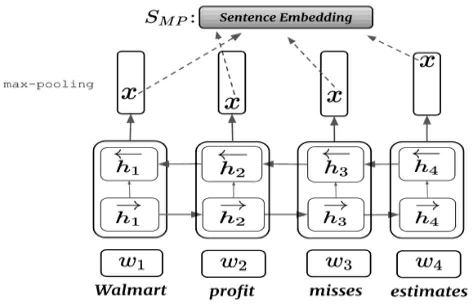

Fig - 11: BiLSTM – MaxPooling [25]

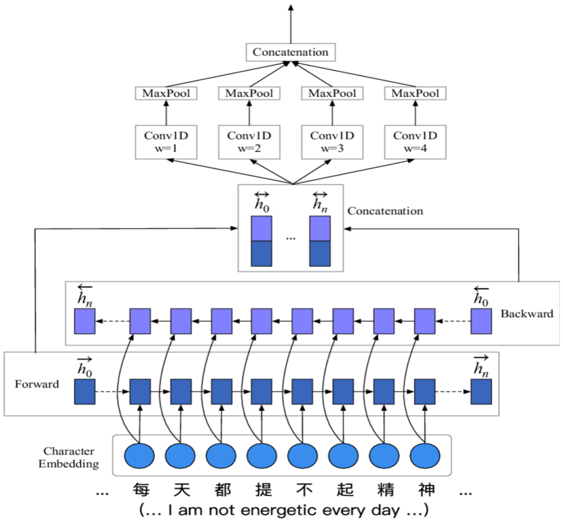

Fig - 12: BiGRU – MaxPooling [26]

As the ratio of RAW to normal transaction is very less so we should take care of the highly skewed nature of data. By doing this experiment [10] we came to know that random forest gives the more accurate result to find the normal transaction while neural network is good for detecting fraudulent transactions. One 12th of one percent transactions can be identified in today's fraud detection system. There are two major ways to fight against credit card frauds they are fraud detection and fraud prevention. Direct several fraud prevention techniques nowadays one of them is OTP, banking websites provide security questions. In this experiment they have used data which is publicly accessible. This data set contain numerical records. In this experiment we are going to keep best of both the algorithms so we can predict high accuracy. Now training data consists of 60% of normal transaction in 60% of fraudulent transaction for the cross validation the data is divided into 20% normal transaction and 20% fraudulent transaction while for the testing purpose for the data is divided into 20% of normal transaction and 20% of fraudulent transaction. Then for the training of the model we will first train the feedforward neural network on the entire training data. Then we will train another feed forward neural network of 60% it of fraudulent transaction and 60% of normal transactions on under sampling training data. Then again, they have trained same number of fraudulent transaction while half of the normal transaction. The next step will be training data will be trained by the random forest which consist of 300 decision trees. Same processor will be repeat again but random forest will have 400 decision trees. Then cross-validation will be applied in order to get tuning parameter of three models. The output received from the majority of classifier is used to test the testing data. The main aim of this experiment was to minimize be misclassification of fraudulent transactions.

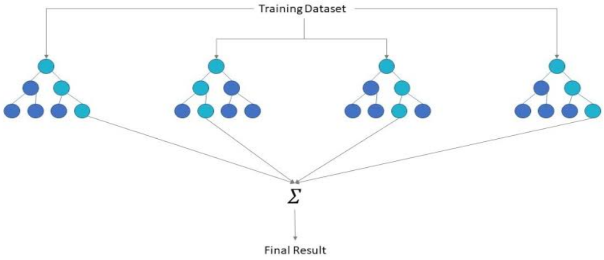

Fig - 13: Basic Idea for Random Forest [27]

Genetic algorithm is a new technology nowadays it's a means to obtained better solution and eliminate fraud transactions. In [11], it is discussed that how genetic algorithm can be used in purpose of fraud detection. Video Aar system is designed in a way that fraudulent rule sets are given to the system then rule engine is applied in which data sets is given from that step then we move to the next step where field and priority are given then the process data is given to the genetic algorithm. This specific system is built in the applet viewer user interface module.

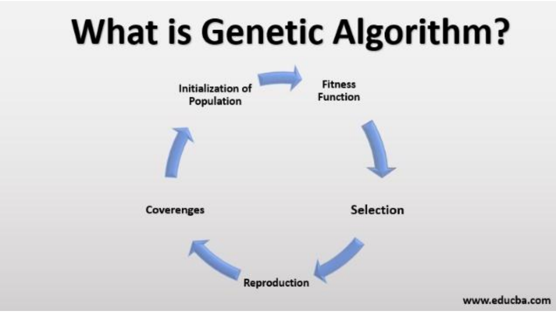

Fig - 14: Life Process of Genetic Algorithm [28]

This paper [12] shows how class balancing techniques helps in credit card fraud detection. three most popular solution R data level algorithm level and ensemble solutions. For the purpose of balancing of majority and minority classes sampling methods like over sampling under sampling is been implemented. Imbalance learning problem is the major issue which is to be solved first. Because of imbalance learning problem the ratio of finding fraudulent transaction to legitimate transaction will be very low. The system will follow this process firstly raw data is collected then that data is pre-process. Once the pre-processing is completed then data set is generated from that data. The data is given to the over Sampling and under sampling method. On the over sampling part SMOTE, SMOTE ENN, SMOTE TL, Safe SMOTE, ROS is applied on the data. On the other hand, on under sampling RUS, CNN, CNN TL, TL is applied. Then all the data is combined and given to the cost-sensitive methods and ensemble methods. On the cost sensitive method side, the support vector machine and C4.5 decision tree is applied on the data while on the ensemble method side Ada Boosting and bagging is applied on data. The process data now goes to the performance meter where you get the value of area under the R the ROC the curve, sensitivity, specificity, G-Mean. From all of the over sampling methods SMOTE ENN performance was better and also bagging use the better result from all the classifiers. In the following experiment it is observed that sampling take lesser time then under sampling when apply to the same model. The final results says that for over sampling SMOTE ENN perform best and for the under-sampling TL perform best.

In today's world making online fraud transaction is became very easy. In order to stop them this paper [13] has implemented deep learning methodologies which are auto-encoder and restricted Boltzmann machine. Fraudster continuously change their fraud patterns in order to not get detected. So we have to change the medium from offline to online fraud transaction detection using unsupervised learning.AE, RBM, H2O is used from the Google by deep learning. Three data sets were used which were from Germany, Australia, and Europe. For the calculation of nearest point KNN was used. Autoencoder is used for the detection of fraud. In order to encode and decode the output and input they have used the hyperbolic function. After doing all the calculations the auto-encoder give the area under the curve up to 0.9603 on the European data set which is suitable for large data sets on the other hand when auto-encoder and Boltzmann was applied on Australian and German data sets the results were not as expected so we can conclude that work on big data sets well and fine and do not work well on small data sets.

This paper [14] tells us about how Cat boosting and Light Gradient Boosting Machine (LGBM) can be used for credit card fraud detection. They had compared the performance of Auto-Encoder (AE), K-means clustering, Logistic Regression and Neural Network (NN) vs Cat boosting and Light Gradient

Boosting Machine (LGBM). In cat boosting parameter tuning is not needed and it can be run on the default's parameters. It does not require the conversion of categorical data to numerical data. basic benefit of using gradient boosting is it increase the accuracy and minimize the overfitting rate. LGBM is based on decision trees and classification of model maximized also reduce the usage of memory. Synthetic Minority Over Sampling (SMOTE), Logistic Regression and AE all have low amount of recall scores and less amount of robustness as it takes more time to compute and its inappropriate for the imbalance data. After implementation it is observed that Cat Boost is best for in term of accuracy and in case of large datasets LGBM is better suits. LGBM perform best among all of them and achieved the accuracy score of 99% while NN, Logistic Regression, AE, K-Means clustering, Cat Boost scores 96%, 77%, 96%, 93%, 98%

2. PROPOSE SYSTEM

As per the reference of the [6] and [15], Our propose model use Light Gradient Boosting Machine Learning (LGBM) as per the [6] and [15] perform far better than the other algorithms. Our system compares the XGBoosting, SMOTE, Light Gradient Boosting and finds the transactions are legitimate or fraudulent as shown in figure.

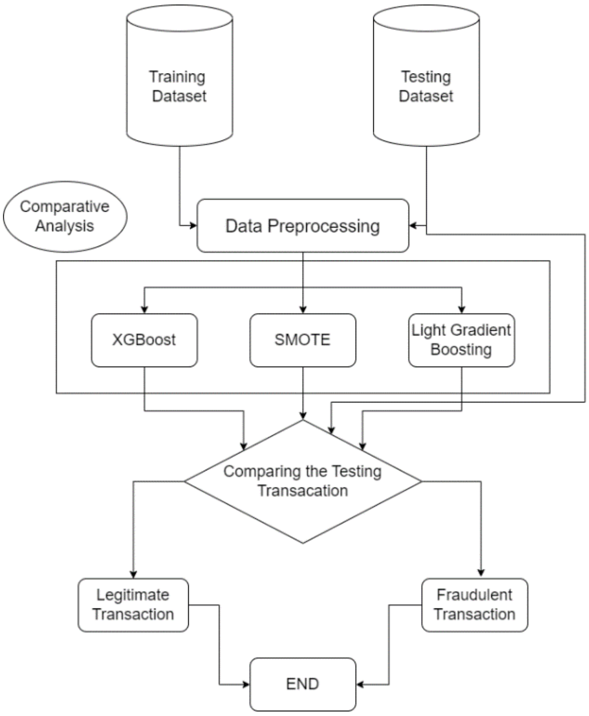

Fig - 14: Proposed Model

Step 1: Taking the Datasets and divide it into the training and testing sets.

Step 2: Then data is pre-processed in order to get required features.

Step 3: Providing training data to XGBOOSTING, SMOTE, LGBM to built a model.

Step 4: Comparing using testing data which perform better.

3. CONCLUSIONS

Technology growth is directly proposal to the growth of Credit Card Frauds. As for the future work we can apply deep learning techniques for detecting fraudulent transactions as deep learning is capable of making more powerful model as compare to machine learning.

REFERENCES

[1] Stolfo, S., Fan, D. W., Lee, W., Prodromidis, A., & Chan, P. (1997, July). Credit card fraud detection using meta-learning: Issues and initial results. In *AAAI-97 Workshop on Fraud Detection and Risk Management* (pp. 83-90).M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Fu, K., Cheng, D., Tu, Y., & Zhang, L. (2016, October). Credit card fraud detection using convolutional neural networks. In *International conference on neural information processing* (pp. 483-490). Springer, Cham.K. Elissa, "Title of paper if known," unpublished.

[3] Aleskerov, E., Freisleben, B., & Rao, B. (1997, March). Cardwatch: A neural network based database mining system for credit card fraud detection. In *Proceedings of the IEEE/IAFE 1997 computational intelligence for financial engineering (CIFEr)* (pp. 220-226). IEEE.

[4] Zeager, M. F., Sridhar, A., Fogal, N., Adams, S., Brown, D. E., & Beling, P. A. (2017, April). Adversarial learning in credit card fraud detection. In 2017 Systems and Information Engineering Design Symposium (SIEDS) (pp. 112-116). IEEE.

[5] Behera, T. K., & Panigrahi, S. (2015, May). Credit card fraud detection: a hybrid approach using fuzzy clustering & neural network. In 2015 second international conference on advances in computing and communication engineering (pp. 494-499). IEEE.

[6] Taha, A. A., & Malebary, S. J. (2020). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE Access, 8, 25579-25587.

[7] Ganji, V. R., & Mannem, S. N. P. (2012). Credit card fraud detection using anti-k nearest neighbor algorithm. *International Journal on Computer Science and Engineering*, *4*(6), 1035-1039.

[8] Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. (2014, April). Improving credit card fraud detection with calibrated probabilities. In *Proceedings of the 2014*

SIAM international conference on data mining (pp. 677-685). Society for Industrial and Applied Mathematics.

[9] Najadat, H., Altiti, O., Aqouleh, A. A., & Younes, M. (2020, April). Credit card fraud detection based on machine and deep learning. In *2020 11th International Conference on Information and Communication Systems (ICICS)* (pp. 204-208). IEEE

[10] Sohony, I., Pratap, R., & Nambiar, U. (2018, January). Ensemble learning for credit card fraud detection. In *Proceedings of the ACM India Joint International Conference on Data Science and Management of Data* (pp. 289-294).

[11] RamaKalyani, K., & UmaDevi, D. (2012). Fraud detection of credit card payment system by genetic algorithm. *International Journal of Scientific & Engineering Research*, *3*(7), 1-6.

[12] Sisodia, D. S., Reddy, N. K., & Bhandari, S. (2017, September). Performance evaluation of class balancing techniques for credit card fraud detection. In *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)* (pp. 2747-2752). IEEE.

[13] Pumsirirat, A., & Liu, Y. (2018). Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine. *International Journal of advanced computer science and applications*, *9*(1).

[14] A. A. Taha and S. J. Malebary, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine," in IEEE Access, vol. 8, pp. 25579-25587, 2020.

[15] AI Journey https://ai-journey.com/wp-content/uploads/2019/06/fraud-EMV-chip-credit-card.jpg

[16] Data Aspirant https://dataaspirant.com/wp-content/uploads/2020/09/1-Credit-card-fraud-detection-with-classification-algorithms.png

[17] Vortarus https://vortarus.com/wp-content/uploads/2018/12/simulation-diagram.png

[18] Malicksarr https://www.malicksarr.com/wp-content/uploads/2021/06/Deep-Learning-Definition.png.jpg

[19] Code Ground https://cdn.codeground.org/nsr/images/img/blog-thumb23.jpg

[20] Ecognition https://docs.ecognition.com/Resources/Images/ECogUsr/UG_CNN_scheme.png

[21] Medium https://miro.medium.com/proxy/1*8FhisenG1AsVv-MxRpVYZg.png

[22] Digital Transformation Pro https://digitaltransformationpro.com/wp-content/uploads/2017/06/Datamining-1024x576.png

[23] Els-cdn https://ars.els-cdn.com/content/image/1-s2.0-S0010482505000417-gr4.jpg

[24] Research Gate https://www.researchgate.net/publication/345040132/figure/fig1/AS:952564933750788@1604120586852/The-proposed-approach-for-Android-malware-classification_Q320.jpg

[25] Research Gate https://www.researchgate.net/publication/330008974/figure/fig4/AS:709745916776451@1546228021348/BiLSTM-max-pooling-The-network-performs-a-polling-operation-on-top-of-each-word-hidden.ppm

[26] Research Gate https://www.researchgate.net/profile/Wenpeng-Lu/publication/331459358/figure/fig3/AS:850162641534980@1579705977589/Network-architecture-of-BiGRU-CNN.png

[27] IBM https://1.cms.s81c.com/sites/default/files/2020-12-07/Random%20Forest%20Diagram.jpg

[28] edu CDA https://cdn.educba.com/academy/wp-content/uploads/2019/09/What-is-Genetic-Algorithm.png