International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Credit Card Fraud Detection Using GSA

Ritu, Sudesh Nandal
Department of Electronics and Communication Engineering, Bhagat Phool SinghMahila Vishwavidalaya Khanpur Kalan , Sonepat , Haryana, India

ABSTRACT

Billions of dollars of loss are caused every year by fraudulent credit card transactions. The design of efficient fraud detection algorithms is the key for reducing these losses, and more and more algorithms rely on advanced machine learning techniques to assist fraud investigators. We found German credit card fraud detection database available publically which is having 1000 data points. This dataset is divided into 70/30 ratio for training and testing the neural network. The famous and efficient machine learning neural network algorithm is used to get a trained NN. This network is further updated for more classification accuracy using Gravitational Search Algorithm (GSA) which is an optimization algorithm. It tunes NN's weights and biases and check for the mean square error which is an evaluation parameter also in our work. Complete work is simulated in MATLAB R 2016a. Results are compared with previously used simulated annealing (SA) algorithm and proposed method is giving better results in term of area under curve (AUC) of ROC (receiver operating characteristics) and MSE.

Keyword: Fraud Detection , Gravitational Search Algorithm, Neural Network, Simulated Annealing

I. INTRODUCTION

1.1 The problem of Fraud Detection

Fraud is as old as humanity itself and can take a vast range of different forms. The latest technologies provide some extra method where in criminals can also devot fraud. The use of credit cards is regularly occurring in cutting-edge day society and credit scorecard fraud has kept on developing in current years. Financial losses due to fraud problem affect the traders banks and person customers. Additionally Fraud may effect the reputation and image of merchant inflicting non-financial losses. For example, if a cardholder is sufferer of fraud with a certain enterprise, he may additionally not accept as true with their enterprise and select a competitor [1].

To minimize the fraud cases, it is divided into two process i.e. fraud prevention and fraud detection. Fraud prevention refers to dam fraudulent transations at supply. Fraud detection is where successful fraud transaction are identified. Technologies which have been used that allow you to prevent fraud are Address Verification Systems (AVS), Card Verification Method (CVM) and Personal Identification Number (PIN). AVS includes verification of the deal with zip code of the customer even as CVM and PIN involve checking of the numeric code keyed by the patron [2]. For prevention functions, financial establishments undertak all transactions with rule primarily based filters and data mining methods as neural networks [3].

Fraud detection is, given a hard and fast of credit score card transactions, the manner of figuring out if a new legal transaction belongs to the magnificance of fraudulent or proper transactions. A Fraud Detection System (FDS) need to no longer handiest stumble on fraud instances efficiently [4]. Enhancement in fraud detection system provides a fee- effective system in the sense that the price invested in transaction screening ought to now not be higher than the loss because of frauds. Bhatla suggests that screening of only 2% of transactions can bring about decreasing fraud losses accounting for 1% of the entire cost of transactions. However, an assessment of 30% of transactions could reduce the fraud losses appreciably to zero 06%, however increase the prices exorbitantly. In order to minimize prices of detection it's far vital to apply professional regulations and statistical based models (e.g. Machine Learning) to make a first display among

authentic and capability fraud and ask the investigators to review most effective the cases with excessive risk [5].

Typically, transactions are first filtered by using checking a few important situations (e.g. sufficient stability) and then scored with the aid of a predictive model. The predictive model scores each transaction with excessive or low risk of fraud and those with excessive danger generated signals. Investigators test these indicators and offer remarks for each alert, i.e. actual advantageous (fraud) or false high-quality (true). These feedbacks can then be used to improve the model. As discussed in paper[6][7], Machine Learning (ML)efficiently discover fraudulent patterns and predict transactions which are maximum probable to be fraudulent. ML strategies consist in inferring a prediction version on the basis of fixed examples. In the domain of fraud detection, using learning techniques is attractive for some of motives. First, they allow to discover patterns in high dimensional records streams, i.e. Transactions arrive as a non-stop stream and each transaction is defined by the way of many variables. Second, fraudulent transactions are often correlated each through the years and area. For examples, fraudsters commonly try to dedicate frauds in the equal store with different cards within a brief term. Third, gaining knowledge of strategies may be used to discover and version current fraudulent strategies as well as perceive new techniques associated to uncommon conduct of the cardholders. Predictive fashions primarily based on ML strategies and also able to automatically combine investigators' feedbacks to improve the accuracy of the detection, while in the case of professional machine, such as investigators feedbacks require rules revision that may be tedious and time ingesting [8].

When a fraud can't be avoided, it is desirable to detect it as rapidly as possible. In both cases prevention and detection, the trouble is magnified by some of domain constraints and characteristics. Firstly, care should be taken not to prevent too many valid transactions or incorrectly block genuine playing cards. Customer infection is to be prevented. Secondly, maximum banks technique full-size numbers of transactions of which handiest a small fraction is fraudulent, often less than 0.1%. Third, simplest a restricted wide variety of transactions may be checked by means of fraud investigators, i.e. we can't ask a human individual to check all transactions separately if it is fraudulent or no longer. In other phrases corporations and public establishments need computerized systems able to help fraud detection [9]. Typically, transactions are first filtered by checking some essential conditions (e.g. sufficient balance) and then scored by a predictive model. The predictive model scores each transaction with high or low risk of fraud and those with high risk generate alerts. Investigators check these alerts and provide a feedback for each alert, i.e. true positive (fraud) or false positive (genuine). These feedbacks can then be used to improve the model.

Credit card frauds may additionally occur in numerous methods [9], simply to mention a few, we are able to have stolen card fraud, cardholder-not-present fraud and application fraud:

- Stolen card fraud is the most commonplace type of fraud wherein the fraudster typically attempts to spend as a whole lot as possible and as fast as feasible. The detection of this sort of fraud normally is based on the discovery of a sudden usage sample of the credit score card (typically unexpectedly crucial) with appreciate to the not unusual exercise.
- Cardholder-now not-present fraud is frequently found in e-business. Here the fraudster wishes the records about a credit score card but now not the cardboard itself. This fraud demands a activate detection due to the fact that, in contrast to the preceding case, the reputable card owner is not conscious that his very own facts have been stolen.
- Application fraud corresponds to the software for a credit card with fake non-public records. This sort of fraud takes place extra rarely when you consider that it may be detected throughout the application by checking the data of the applier, contrary to different frauds that can't be anticipated.

II. PROPOSED WORK

In the proposed set of rules, agents are taken into consideration as objects and their overall performance is measured by their hundreds. All these objects appeal to each other by means of the gravity force, and this force causes a global motion of all items in the direction of the objects with heavier loads. Hence, hundreds cooperate using an immediate shape of conversation, through gravitational force. The heavy hundreds – which correspond to correct solutions –

flow more slowly than lighter ones, this guarantees the exploitation step of the set of rules. In different phrases, every mass affords an answer, and the set of rules is navigated by using nicely adjusting the gravitational and inertia loads. By lapse of time, we anticipate that hundreds be attracted with the aid of the heaviest mass. This mass will present a most reliable solution within the search area. The GSA could be taken into consideration as an isolated machine of hundreds. It is sort of a small synthetic world of hundreds obeying the Newtonian laws of gravitation and movement. More precisely, masses obey the following laws: Law of gravity and Law of motion.

A neural community is a system of hardware and/or software patterned after the operation of neurons in the human mind. Neural networks also called artificial neural networks are an expansion of deep gaining knowledge of technologies. Commercial programs of these technologies generally consciousness on fixing complicated signal processing or pattern popularity troubles.
Neural Networks, with their tremendous capability to derive which means from complicated or obscure facts, is wont to extract designs and find developments which could be too complicated to be noticed with the help of either humans or completely different laptop computer techniques. a talented neural community is notion of as AN "expert" within the class of statistics it has been given to investigate.

The credit card fraud detection is emerging risk field with more and more presence of user's on internet. With the introduction of Digital India movement, online payments and money transfer is increased. This all raises a group of people who defraud the online activities. So the need of credit card fraud detection and prevention is utmost required. In our work we proposed a novel algorithm to detect the credit card fraud. The method is using machine learning algorithm as main along with evolutionary optimization algorithm to improve the performance of neural network (NN). Neural Network is also an iterative process which changes its input weights and biases to achieve the minimum mean square error (MSE). It is using feedback propagation loop which is using Lquenberg algorithm. This algorithm iterates locally which means it doesn't guarantee the convergence of all minima points. it may skip some combinations of input weights and biases which may reduce the MSE more. To avoid this issue we have adapted the optimization method named Gravitational Search Algorithm (GSA). It is based on the movement of celestial bodies and position of these agents is input weights and biases in our case. The output of NN is calculated by formula in 1.

$$output = input * IW_i + B_i \qquad (1)$$

where IW_i are the input weights and B_i are the biases. The number of input weights and biases depends upon the number of hidden layers. The GSA algorithm is supposed to tune these values. For this purpose first the Neural network is created in MATLAB. That network will be used further for optimization algorithm. We have use the German dataset downloaded from UCI machine learning repository. This dataset contains 20 attributes along with a label of good and bad. If label is 1, those attributes are for non fraud case and vice versa. In out proposed algorithm of optimized neural network we need the numeric dataset, so this dataset in numeric format is also available on the same web link.

A complete step by step algorithm is explained below.

Step1. Load the German credit card fraud dataset in numeric format and divide that into random 70/30 ratio for training and testing of neural network.

Step2. Generate the NN script to create and train the network whose weights and biases are to be optimised.

Step3. Initialise the GSA parameters like number of iterations, number of agents, initial G0 and alpha. Pass the previously created network into GSA to get the dimension of weights and biases.

Step4. Randomly initialise the new input weights and biases to give an initial seed to GSA optimisation. These must be within a boundary as given in next chapter.

Step5. Call the objective function to update the neural network's weights and biases and calculate the MSE for those values by using the testing dataset.

Step6. To update the random positions of agents, force and mass has to be calculated by using the equations

$$F_{ij}^{d}(t) = \mathrm{G(t)}\frac{M_{pi}(t)\times M_{aj}(t)}{R_{ij}(t)+\varepsilon}{}_{\mathrm{i}}X_j^d(t) - X_i^d(t)),\mathrm{(t)} \qquad (2)$$

$$m_{it} = \frac{fit_i(t) - worst(t)}{best(t) - worst(t)} \quad (3)$$

the respective notations are given in previous chapter

Step7. The new updated position is obtained from the formula

$$X_i^d(t+1) = X_i^d(t) + V_i^d(t+1) \quad (4)$$

The velocity in this case is calculated by using acceleration which is based on force and mass calculated in previous step.

Step8. For this new updated position or values of weights and biases, objective function is again called and MSE is saved.

Step9. The weights and biases for which minimum of MSE is obtained out of previous two set of values, is further considered for updating.

Step10. This process continues till all iterations are not completed.

Step11. The final minimum MSE is obtained and weights ad biases set for them is used as final NN weights and biases which gives less MSE than conventional NN and Simulated Annealing tuned NN.

III. IMPLIMENTATION AND SIMULATION RESULT

In our work we have proposed the optimization algorithm i.e. GSA optimisation as decribed earlier to optimise the combination of NN weights and biase to minimise MSE in detcetion for creadit card fraud. The proposed work is implemented in MATLAB. MATLAB provides a user interface platform to design script. A lot of inbuilt functions in it makes the use easier and saves our time to build our code from scratch. During the GSA implementations we have to provide the input of number of agents, total number of iterations and range to the GSA script. The values of these inputs are tabulated in Table 1.

Table 1: input variables set in GSA optimization

Input	Value
Total number of agents	10
Total iterations0	**50**
Range	[-1,1]

We trained and optimized the network for proposed GSA algorithm and compared the results with SA tuned NN and conventional NN as available with MATLAB's toolbox which is using Lquanberg algorithm. A neural network with 1 hidden layer and 20 hidden neurons is created as shown in figure 1.

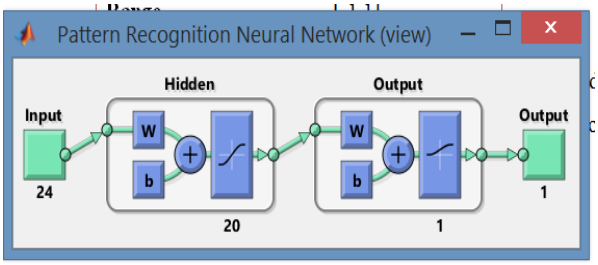

Figure 1: NN with one hidden layer and 20 neurons

This network is further optimized with proposed GSA and previous work of SA (Simulated Annealing). Both are optimization algorithms and an optimization work is judged on the basis of optimization curve between number of iterations and fitness function output. Ideally it must be exponentially decreasing and then consistent after particular number of iterations with no more decrease in slope of curve. Since MSE should be least for our case as it is a type of error, so optimization graph with least slope will be considered best optimization. A comparison between GSA and SA optimization for our application is shown in figure 2.

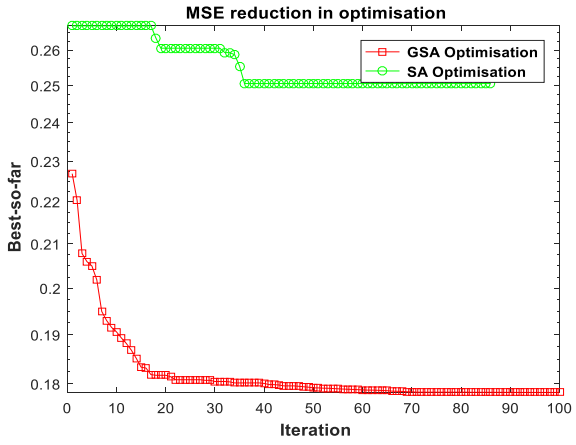

Figure 2: Optimization curve comparison of GSA with SA

The GSA trained NN is settled at MSE of 0.18 while SA tuned NN settled at 0.25 unit MSE. In this case 28% reduction in the GSA tuned MSE is achieved. The results obtained i.e. number of correct classified fraud cases or good cases are evaluated by Receiver Operating Characteristic Curve (ROC) which is plotted for binary classification task. It is a plot between true positive rate and false positive rate. It was first introduced in world war II to detect the enemy tank's position on radar. Later it was used in psychology testes and in machine learning. In machine learning the true positive rate are sensitivity and recall which is formulated as

$$SensitivityorTPR = \frac{TP}{TP + FN}$$

Where TP is true positives and FN is false negative and false positive rate is fall out probability. Area under this curve is used to determine for the accuracy of classification. The maximum area under ROC is 1.The intercept of the ROC curve with the line at 45 degrees orthogonal to the curve is the balance point where TPR and FPR are equal i.e TPR=FPR. The ROC curve for our case is shown in figure 3.

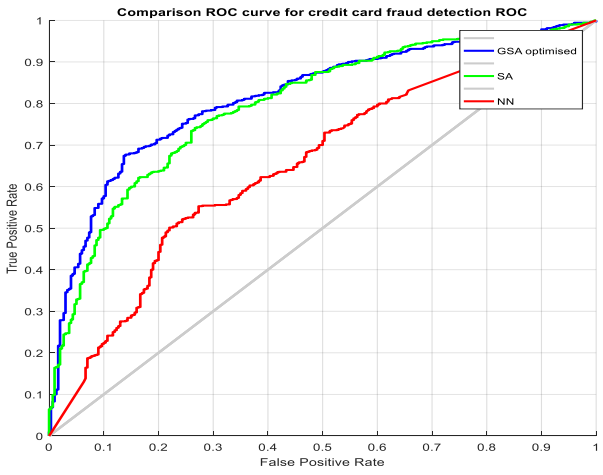

Figure 3: ROC curve for credit card fraud detection for GSA tuned NN, SA tuned NN and NN

The area under curve is highest for our proposed optimization GSA tuned NN. An improvement of 13.43% is occurred than SA and 25 % from NN with LM back propagation.

Table 2: Comparison of Area Under Curve (AUC) for three Algorithm

NN AUC	SA AUC	GSA AUC
0.6536	0.7974	0.8166

Figure 4 shows the confusion matrix plot for these algorithms. In the field of machine learning and specifically the problem of statistical classification, a confusion matrix, also known as an error matrix, is a specific table layout that allows visualization of the performance of an algorithm, typically a supervised learning one (in unsupervised learning it is usually called a matching matrix). Each column of the matrix represents the instances in a predicted class while each row represents the instances in an actual class (or vice-versa).The name stems from the fact that it makes it easy to see if the system is confusing two classes (i.e. commonly mislabeling one as another).

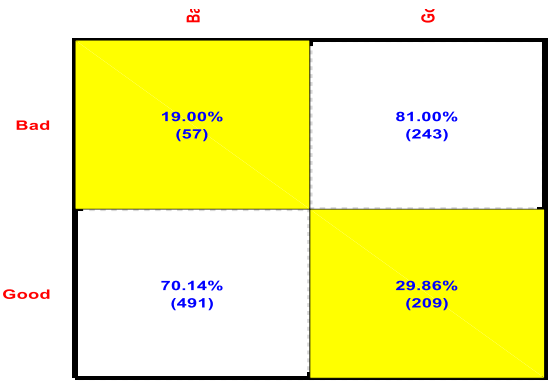

Figure 4: Confusion matrix for GSA tuned NN algorithm

The mean square error is calculated for each final tuned set of weights and biases of NN. The lesser is MSE, better is classification accuracy. A vector of combined weights and biases for all these three cases are not shown because of large dimensions. The MSE for GSA tuned NN is least as shown in bar graph in figure 5, followed by SA tuned NN and then conventional NN. Previous researcher has proved that SA optimized Neural Network classifies better than NN with LM feedback algorithm and our proposed GSA optimization performed well than SA by 4%.

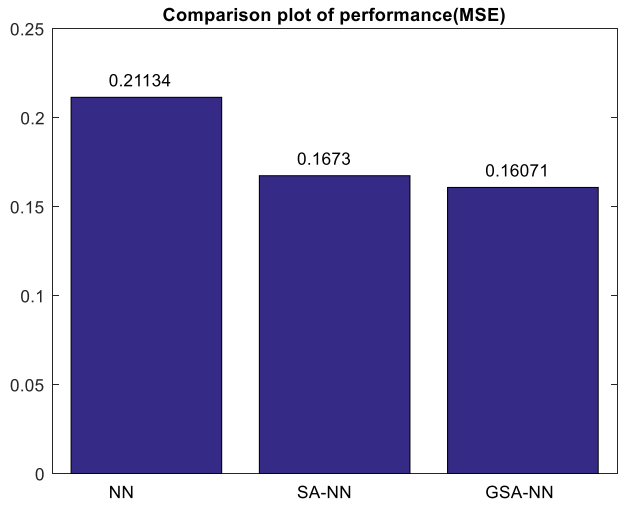

Figure 5: MSE comparison between GSA tuned NN, SA tuned NN and NN

Table 3 shows the percentage improvement of all evaluation parameters over other algorithms.

	GSA vs SA (%)	**GSA vs NN (%)**
AUC	13.43	25
MSE	4	24

IV. CONCLUSION

The findings in this work highlight the fraud detection improvement that a meta-learning strategy can provide when it is used in conjunction with an established neural network fraud detection system. The principles of neural networking are motivated by the functions of the brain especially pattern recognition and associative memory. The neural network recognizes similar patterns, predicting future values or events based upon the associative memory of the patterns it has learned. The advantages neural networks is that these models are able to learn from the past and thus, improve results as time passes. They can also extract rules and predict future activity based on the current situation. By employing neural networks effectively, banks can detect fraudulent use of a card, faster and more efficiently. Neural network is tuned with gravitational search algorithm and compared with SA tuned NN. The improvement in accuracy and mean square error is noticed in purposed optimization. GSA is performing well because it's a global meta optimization technique and SA is local optimization algorithm which converges prematurely unlike GSA. our system achieves the 13.43 % of more area under curve than SA and 4% less MSE than SA tuned neural network. This percentage improvement is more if purposed method is compared with conventional neural network. The improvement in AUC reaches up to 25% and MSE decreases up to 24%. The dataset used for this purpose is downloaded from UCI machine repository which is having 20 attributes including the actual label of fraud or non fraud. This data considers the user's bank account status in multiple levels, his credit history, whether married/divorced/live in etc., employed/self employed etc. These kind of attributes serve the purpose of training the neural network.

V. FUTURE SCOPE

In future, work on the algorithm can be done which aware users with the type of fraud with which they are victim of. In other words again classification of type of frauds to aware the users and to help credit card companies to build prevention measures. Unavailability of real time data and testing on real time data is still not done. More confidence in the algorithm can be built up if it can be tested for real time data and also on a large data set used for training.

VI. REFERENCES

[1]. Raghavendra Patidar, Lokesh Sharma," Credit Card Fraud Detection Using Neural Network", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume1, Issue-NCAI2011, Page No. 32-38 June 2011

[2]. V. Bhusari, S. Patil," Study of Hidden Markov Model in Credit Card Fraudulent Detection ", International Journal of Computer Applications (0975 – 8887) Volume 20– No.5, Issue-5, Page No. 33 April 2011

[3]. Dr R.DHANAPAL , GAYATHIRI.P," Credit Card Fraud Detection Using Decision Tree For Tracing Email And Ip ", IJCSI International Journal of Computer Science Issues,Volume 9,Issue 5, No 2,Page No. 406-412 September 2012

[4]. X.Y. Liu, J. Wu, and Z.H. Zhou. Exploratory under sampling for class-imbalance learning.

Systems, Man, and Cybernetics, Part B: Cybernetics,Volume 39,No. 2, Page No. 539–550, 2009.

[5]. Vijayshree B. Nipane, Poonam S. Kalinge, Dipali Vidhate, Kunal War, Bhagyashree P. Deshpande,"Fraudulent Detection in Credit Card System Using SVM & Decision Tree", IJSDR, Volume 1, Issue 5,Page No. 896-901 2016.

[6]. Mohamed Hegazy, Ahmed Madian, Mohamed Ragaie,"Enhanced Fraud Miner: Credit Card Fraud Detection using Clustering Data Mining Techniques", Egyptian Computer Science Journal (ISSN: 1110 – 2586) Volume 40 – Issue 3, Page No. 72-81 September 2016

[7]. Azeem Ush Shan Khan, Nadeem Akhtar and Mohammad Naved Qureshi,"Real-Time Credit-Card Fraud Detection using Artificial Neural Network Tuned by Simulated Annealing Algorithm", Proc. of Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC, Page No. 114-121, 2014

[8]. L.U. Oghenekaro, C. Ugwu,"A Novel Machine Learning Approach to Credit Card Fraud Detection ", International Journal of Computer Applications (0975 – 8887) Volume 140 – No.5, Page No. 45-50, April 2016

[9]. Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, "Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning," Special Issue on Information Fusion in Computer Security, Volume 10, Issue no 4, Page No. 54-363, October 2009

[10]. Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K.Majumdar, "BLAST-SSAHA Hybridization for Credit Card Fraud Detection," IEEE Transactions On Dependable And Secure Computing, Volume 6, Issue no. 4, Page No.309-315, October-December 2009.

[11]. Sunil Bhatia1, Rashmi Bajaj2, Santosh Hazari3, "Analysis of Credit Card Fraud Detection Techniques," International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013) Volume 5, Issue no. 3,Page No. 1302-1307,March 2016.

[12]. L. Lei, "Card Fraud Detection by Inductive Learning and Evolutionary Algorithm," 2012 Sixth International Conference on Genetic and Evolutionary Computing, Kitakushu, 2012, Page No. 384-388.

[13]. M. Lotfi Shahreza, "Anomaly detection using a self-organizing map and particle swarm optimization," Volume 18, Issue 6, Pages 1460–1468, December 2011.

[14]. Nader Mahmoudi , Ekrem Duman, "Detecting credit card fraud by Modified Fisher Discriminant Analysis," Expert Systems with Applications, Volume 42, Issue 5, , Pages 2510–2516,1 April 2015.

[15]. Jarrod West and Maumita Bhattacharya, "Intelligent Financial Fraud Detection: A Comprehensive Review," Computers & Security (2015),Volume 57, , Pages 47–66, March 2016.