INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 8, Issue 5 - V8I5-1146)
Available online at: https://www.ijariit.com

Credit Card Fraud Detection and Classification by Optimize Features and Deep Learning

Razia Seema
raziaseema1819@gmail.com
Himachal Pradesh Technical University, Hamirpur, Himachal Pradesh

Kumari Archana
niralaarchana.1991@gmail.com
Himachal Pradesh Technical University, Hamirpur, Himachal Pradesh

ABSTRACT

Traditionally, rule-based systems have been the primary instrument for detecting fraud in today's financial systems, with fraud specialists defining the rules based on prior instances and outcomes. If a new transaction meets one or more of the previously established criteria, an alert is triggered, indicating that the new transaction may be fraudulent. For previously known fraud tendencies, the rule-based method is effective. Before adding a new rule to the current rule set, a sufficient number of fraudulent transactions must have happened that fit the rule. During this time span, fraud techniques may evolve, resulting in the induced rule expiring. Thus, the emphasis should be on using prior transactions that follow a rule-based approach in conjunction with an unsupervised method that detects previously unknown fraud activity. There is a need to use fraud detection systems that are capable of keeping up with the cardholder's updated spending behaviour. The detection process's goal is to identify as much fraud as possible while reducing the false positive rate, which has a negative effect on cardholder satisfaction as the cost of providing more false alarms increases. To accomplish this approach, the threshold value is determined at the account level of the cardholder by evaluating the probability sequence of previous and new incoming transactions. Additionally, identified fraudulent transactions are labelled in the database for future analysis in the event that additional assessment is required.

Keywords: *Deep learning, Fraud, Detection, Classification*

1. INTRODUCTION

Knowledge discovery is an activity that generates knowledge by disclosing it or deriving it from previously collected data. Then, knowledge is structured via indexing knowledge components, content-based filtering, and the establishment of connections and relationships between the elements. As a result, consumers have access to this information to aid in their decision-making process. The term "knowledge discovery" refers to the process of extracting useful information from data, whereas "data mining" refers to a specific stage of this process.

The knowledge discovery process is an interactive and iterative that involves the following steps:

1. To comprehend the application domain: This requires considerable previous knowledge and an understanding of the application's objectives.
2. Target data set: Choosing a data set or data samples for discovery.
3. Data organisation and pre-processing: To eliminate noise, to determine methods for dealing with omitted data fields, to account for temporal progression information, and to map missing and unknown values.
4. Data Reduction and Prediction: Identifying valuable characteristics of data and using techniques to minimise the effective number of variables under consideration.
5. Choosing Data Mining Functions: Choosing data mining functions such as summarization, classification, regression, and clustering depending on the data models.
6. Algorithm selection: Algorithm selection includes statistical algorithms, envisage approaches, divergence trend analysis, and decision tree analysis. Numerous methods may be used in various combinations based on the data models.
7. Data Mining: The use of computer methods to the discovery of patterns in data that have been represented in a specific form or collection of representations. A pattern that is both attractive and confident enough may be regarded as knowledge.
8. Interpretation: Interpreting the found patterns and, if necessary, returning to any of the preceding stages, as well as possible visualisation of the extracted patterns, eliminating duplicate or unsuitable patterns, and translating the relevant patterns into user-friendly language.

9. Making Sense of Found Information: Integrating discovered knowledge into the performance system, acting on it, or just recording it for future reference.

In this present era, current generation are highly influenced by the conception, named as "Digitalization". This insight of digitalization is playing highly important role in every sector of the banking, financial, insurance and other economic sectors. Normally, moving towards to digitalization is important for the Indian banking sector as it plays a most significant role in financial inclusion, which is mostly disturbed for offering the best services to customers with a prospect for gaining more in the future [4]. Generally, online banking is a familiar standard for transferring currency from one account to another account. Online banking is getting fame gradually, which increases online transaction with enhanced facilities in various domains such as insurance premium, online reservation for buses, railways, utilities bill payments, such as electricity, house and water taxes, online shopping and so on [8]. Online banking performances are continually increasing. On the other hand, this development has also one major drawback such as an increase in fraudulent activities [6]. Online banking is also named e-banking or internet banking and it developed quickly in precedent years [9] [18]. In the recent days, internet banking is an essential service even for the common people. Electronic banking is a novel banking service, which permits people for interacting with their banking accounts through the internet. Electronic banking provides various banking services, such as Automatic Teller Machine (ATM) services, Electronic Transfer of Funds (EFT), direct deposit Automatic Bill Payment (ABP), and so on [60]. Moreover, this method is a better advantageous medium for the financial association. However, this banking method is inexpensive, while compared with the customary banking method and it provides custom comfort and flexibility. This enhanced development of the online banking system experienced various challenges because of risk and attacks of fraud data settlement [61]. In this modern world, hackers utilize various approaches for violating the security of e-banking. Online application providers in business-to-business segments and business-to-customer segments are increased tremendously, consequently the fraudulent activities and attacks also increased proportionally. In this context, there is an essential need of strong authentication strategies during online transactions. With the advancement and availability of information andcommunication systems raised the demand for numerous advanced techniques to facilitate Security of cryptographic systems in more sophisticated manner [9]

2. LITERATURE REVIEW

Darwish, S. M. [14] designed a semantic fusion method for fraud detection. This method developed a semantic fusion method by integrating the artificial bee colony algorithm (ABC) and k-means algorithm. In the ABC, the inability in handling the real cluster was eliminated by combining the global search with the neighbourhood search. The relevant features were determined using the rule engine and the unified frame was developed by combining the ABC optimizer and k-mean classifier with the optimized classifier. The behaviour of the customer like the frequency usage, geographical locations, and book balance was considered for determining the fraudulent. This method improved the accuracy in classification and convergence speed but the computational complexity was high.

Patidar, R., and Sharma, L. [15] developed a hybrid method by integrating the Genetic Algorithm and neural network (GANN) for fraud detection in credit cards. The training of the neural network was done for determining the parameters, like type of the network, weight, number of nodes, and layers using the BPN. This method used the fact that the success rate was high for the talented person. This method provided accurate detection of the fraud in the credit card. However, this method failed to determine the transactions in the credit card in advance.

Fu, K. *et al.* [3] designed a Convolutional Neural Networks (CNN) for the detection of fraud in the credit card. In this method, the intrinsic patterns were learned from the labelled data for determining the behaviour of fraud. Then, the feature matrix was obtained from the available transaction data. After that, the latent patterns set were obtained for the samples using CNN. This method predicted the credit card fraud accurately but the complexity in the computation is a major concern.

Zhang, X. et al. [8] developed a homogeneity-oriented behaviour analysis (HOBA) for the detection of fraud in the credit card. The variables of the features used for the detection of credit card fraud were generated using HOBA. The behaviour in the transaction was analysed using deep learning methods. The performance was determined by considering the false- positive rates. This method provided good performance by reducing the losses in the fraud and reducing the regulatory costs. However, this method failed to reduce the cost of computation which is increased due to the increase in the variable set.

Darwish, S.M. et al. [15] designed a credit card fraud detection method by the analysis of the behaviour of the user. This method provided two-level tracking of the credit card. The precision of the method was improved using the ABC algorithm and k-means algorithm. Initially, normal behaviour was determined for the reliability of the fraud. Then, the fraudulent data were classified using the rule-based engine by finding the deviations from the normal data. The first-level classification was performed using the k-means algorithm whereas the second-level classification was done using the ABC algorithm. The k-means algorithm failed to evaluate the actual clusters which were overcome by the ABC algorithm. Finally, the KNN algorithm was used for the transaction matching and the closeness distance was evaluated using the incoming transaction. However, this method required the extra rules for enhancing the accuracy in the rule engine.

Kim E. *et al.* [43] developed a deep learning and hybrid ensemble method for the detection of fraud in the credit card. The champion-challenger framework was used for the comparison of both the methods in which the challenger stands for the deep learning method and the champion stands for the hybrid ensemble method. The data analysis and the established standard were used for developing the challenger and champion method. Both models were evaluated by determining the constraints in the fraud detection system. Post-launch and offline testing were used in the method for determining the winning model. This method failed to collaborate with experts in a particular domain.

Fiore U, *et al.* [31] modelled a fraud detection method in credit cards using the Generative Adversarial Networks. The Generative Adversarial Networks were trained for mimicking the minority class examples for improving the effectiveness of the classifier. The minority class examples were fused into augmented training set from the training data. This method solved the class imbalance problem besides improving the performance of the detection of fraud in the credit card. However, this method failed to provide maximum sensitivity.

3. PROPOSED WORK

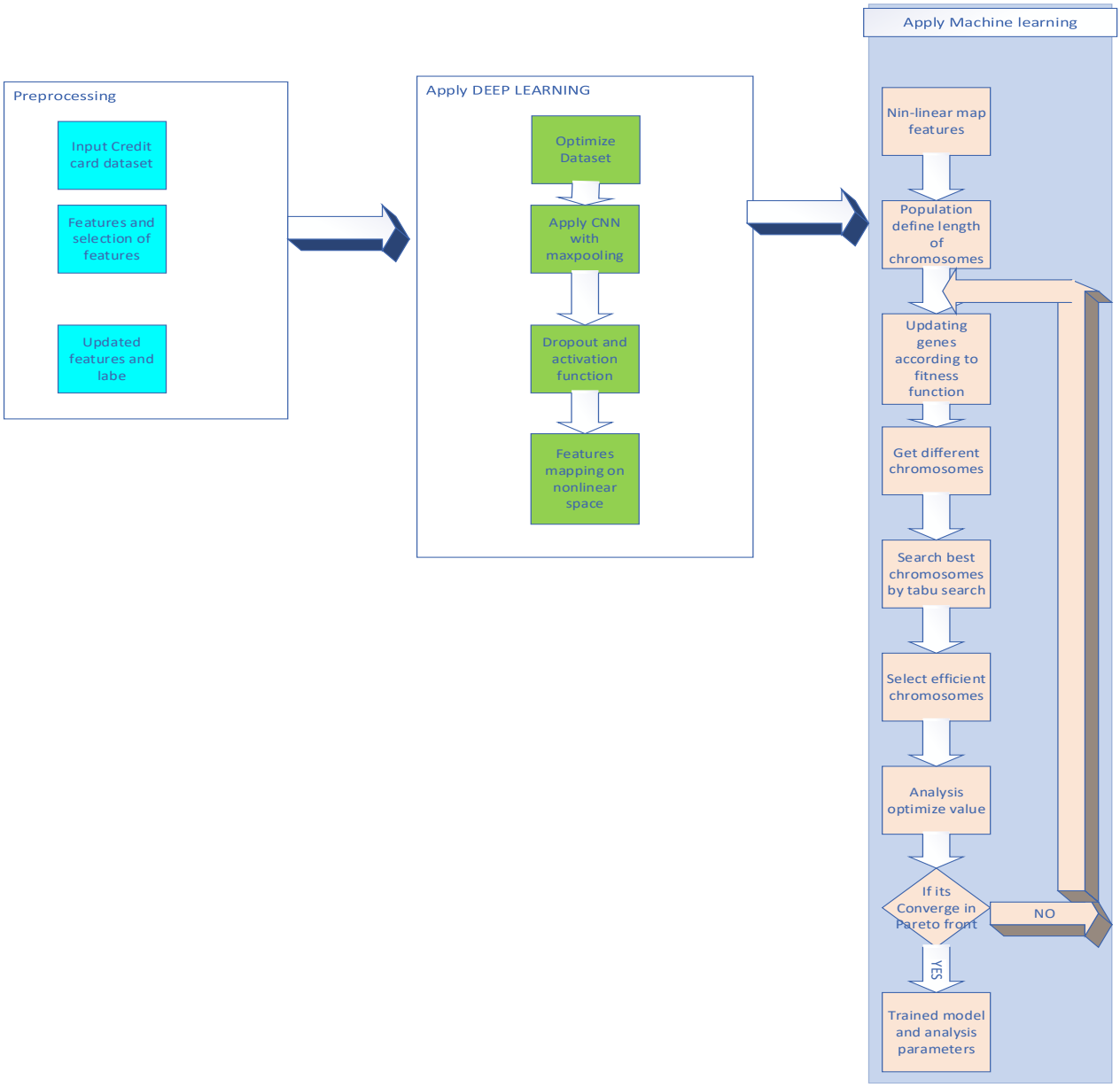

Fig 4.1 Proposed Flow chart

• Two methods are suggested in the proposed strategy, both of which are based on feature improvement. CNN's first attempt utilises a map in non-linear space. Utilize statistical factors such as mean and variance in the second.
• Using ensemble learning techniques, enhance the categorization or identification of cars.
We suggested two ensemble learning-based methods.

1. Divide data into two parts: 80% for training and 20% for testing.2. Begin training with a convolutional layer and map non-linear features.
3. When doing convolution, utilise pooling and Relu layers to map features. Four convolutional layers are used.
4. After four layers, we get a matrix, which is flattened by the thick layer.
5. This vector is used as a feature set for an additional tree classification algorithm. This additional tree classifier use an ensemble method in conjunction with decision trees to create a classifier model.
6. After 20% of the information is used as a test set, the classifier model is used to predict or identify vehicle type.
7. Using response analysis, determine the precision, recall, and accuracy of the suggested model.
8. Input sensor data and split it into two groups of 80% training and 20% testing.
9. Begin training with a convolutional layer and map non-linear features.
10. When doing convolution, utilise pooling and Relu layers to map features. Four convolutional layers are used.

11. After four layers, we get a matrix, which is flattened by the thick layer.
12. These features are then fed to an ensemble learner composed of KNN, decision trees, and MLP.
13. After 20% of the dataset is used as a test set, the classifier model is used to predict or identify the kind of vehicle.
14. Using response analysis, determine the precision, recall, and accuracy of the suggested model.

Extra tree classifier

It is a decision tree ensemble and is similar to other decision tree ensemble techniques such as bootstrap aggregation (bagging) and random forest. Extra Trees generates a huge number of unpruned decision trees from the training set. In the case of regression, predictions are produced by averaging the predictions of decision trees; in the case of classification, they are determined via majority voting. The Extra Trees method samples characteristics at random at each split point in a decision tree. Unlike random forest, which employs a greedy algorithm to determine the optimum split point, the Extra Trees method randomly chooses a split point.

a) Architecture of Deep RNN classifier

Then feature *A* acquired from the wrapper model is fed as input to Deep RNN classifier for achieving detection process. Deep RNN [73] consists of different hidden layers in network model. It is more successful and efficient to represent certain functions than considering other classifiers. Accordingly, recurrent connections are available among hidden layers. However, it achieves the process of detection with varying length of features under sequence of information. It considers the input of next state with the output obtained from previous state.

Due to the recurrent layers, the performance can be effectively increased. Figure 4.2 portrays the structure of Deep RNN classifier.

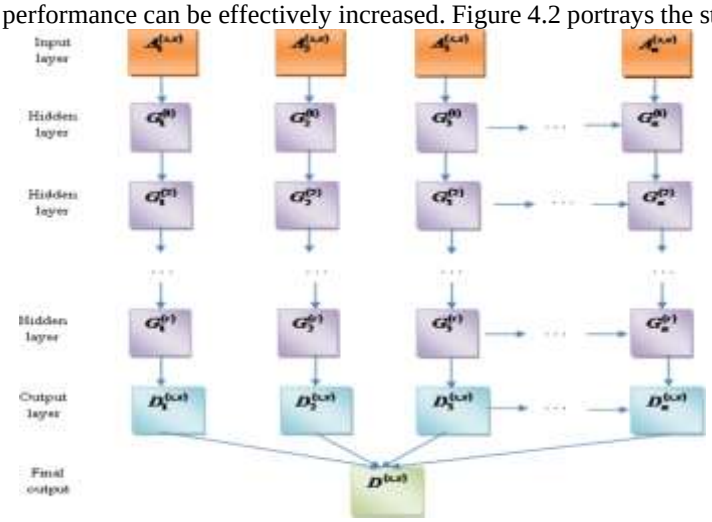

Figure 3.2. Structure of Deep RNN classifier

4. RESULT AND ANALYSIS

Analysis using synthetic data from financial payment system database

In this section, comparative analysis of developed approach using synthetic data from financial payment system database with respect to various feature size is described.

Figure 6.1 displays the comparative analysis using accuracy through changing training data percentage with respect to financial payment system dataset. For 70% of training data, accuracy of present GBDT, majority voting + Adaboost, random forest methods and developed HGW- Deep stacked auto encoder, HWO- Deep RNN and SpiHWO- deep RNN is 0.786, 0.806, 0.829, 0.857, 0.870 and 0.880. Similarly, accuracy of the present fraud detection techniques, namely GBDT is 0.887, majority voting + Adaboost is 0.877, random forest is 0.882, developed HGW based Deep stacked auto encoder is 0.896, developed HWO- Deep RNN is 0.919 and developed SpiHWO- Deep RNN is 0.951 for 90% of training data.

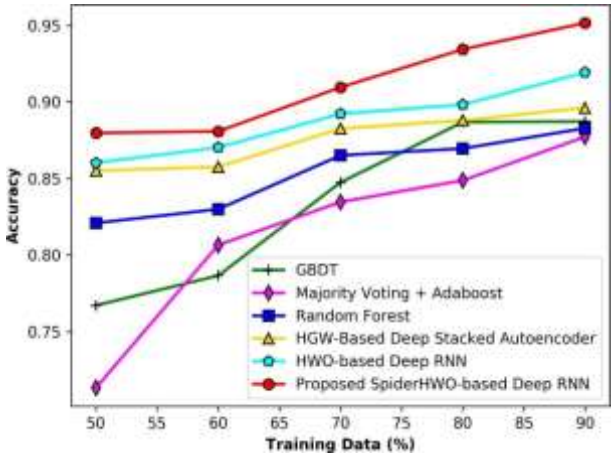

Figure 4.1 Comparative analysis with respect to accuracy

Figure 4.1 portrays comparative analysis with respect to sensitivity by varying training data percentage based on financial payment system dataset. The sensitivity value of present fraud detection techniques, such as GBDT is 0.698, majority voting + Adaboost is 0.682, random forest is 0.690, developed HGW- Deep stacked auto encoder is 0.725, developed HWO- Deep RNN is 0.740 and developed SpiHWO- Deep RNN is 0.781, when training data percentage is 70%. Likewise, for 90% of training data, sensitivity of present GBDT, majority voting + Adaboost, random forest methods and developed HGW- Deep stacked auto encoder, HWO- Deep RNN and SpiHWO- deep RNN is 0.716, 0.734, 0.737, 0.752, 0.764 and 0.792.

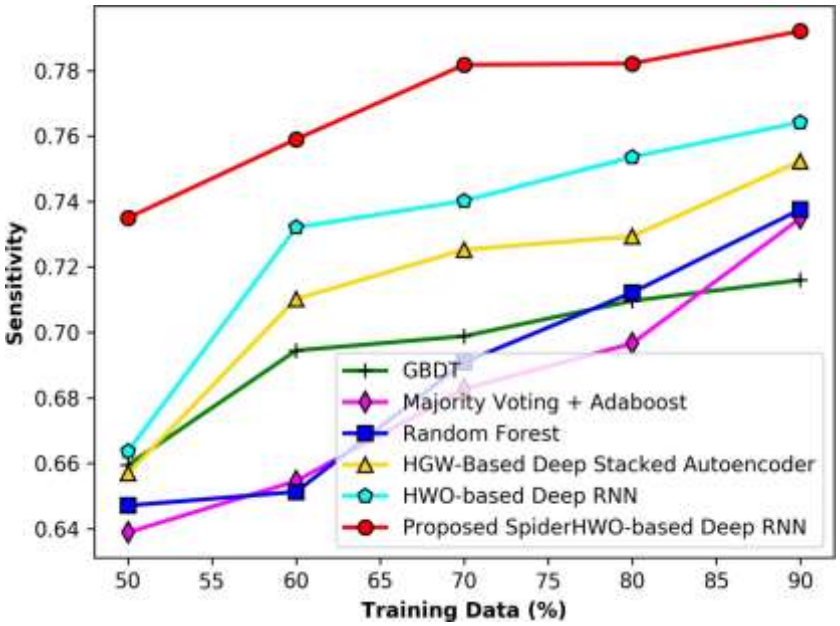

Figure 4.2 Comparative analysis with respect to sensitivity

Figure 4.3 displays the comparative analysis based on specificity through changing training data percentage with respect to financial payment system dataset. For 70% of training data, specificity of present GBDT, majority voting + Adaboost, random forest methods and developed HGW- Deep stacked auto encoder, HWO- Deep RNN and SpiHWO- deep RNN is 0.939, 0.949, 0.957, 0.957, 0.969 and 0.980. In the same way, specificity of present fraud detection techniques, namely GBDT is 0.966, majority voting + Adaboost is 0.962, random forest is 0.974, developed HGW- Deep stacked auto encoder is 0.976, developed HWO- Deep RNN is 0.994 and developed SpiHWO- Deep RNN is 0.9, while training data percentage is 90.

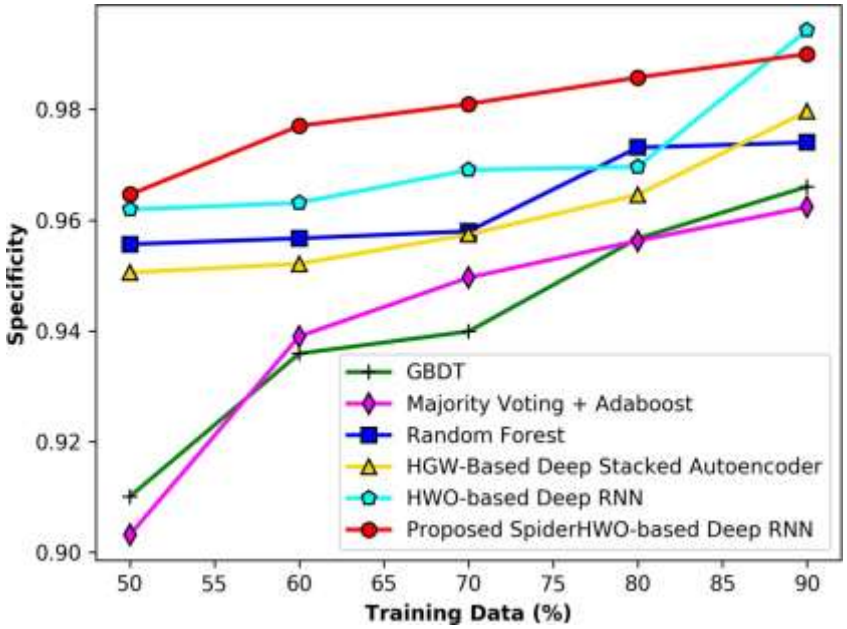

Figure 4.3 Comparative analysis with respect to specificity

5. CONCLUSION

This research presents three contributions for effective fraud detection in the financial sector. The first contribution is to present HGW-Deep Stacked Auto Encoder for performing fraud detection. Here, the training of Deep stacked autoencoder is done by the proposed HGW which is devised by combining HHO and GWO. The proposed HGW- Deep stacked autoencoder offers an optimal solution in discovering frauds with fitness function and adapts minimal error and computes optimal solution using iterations. The imperative features are chosen using the transactional data as the features improved detection rate and accuracy. The chosen features offer imperative information and make the detection more effective. Thus, the efficiency of fraud detection is verified and

recognized from legitimate ones. The second contribution is to devise HWO- Deep RNN for performing fraud detection. Here, the proposed HWO is established by combining HHO and WWO. Moreover, the chasing style, operational features, and cooperative behaviour of water waves made the proposed HWO produce the best solution in contrast to the fitness measure

6. REFERENCES

[1] Srivastava A, Kundu A, Sural S, Majumdar A, "Credit card fraud detection using hidden Markov model", IEEE Transactions on dependable and secure computing, vol.5, no.1, pp.37-48, February 2008.

[2] Fiore U, De Santis A, Perla F, Zanetti P, Palmieri F, "Using generative adversarial networks for improving classification effectiveness in credit card fraud detection", Information Sciences, vol.479, pp.448-55, April 2019.

[3] Syeda M, Zhang Y Q, Pan Y, "Parallel granular neural networks for fast credit card fraud detection", In proceedings of IEEE World Congress on Computational Intelligence, vol.1, pp.572-577, May 2002.

[4] Russell S and Norvig P, "Artificial intelligence: a modern approach", 3rd edn,

[5] Prentice Hall, 2010.

[6] Deshmukh A and Talluru L, "A rule-based fuzzy reasoning system for assessing the risk of management fraud", Intelligent Systems in Accounting, Finance & Management, vol.7, no.4, pp.223-41, December 1998.

[7] Altman E I, Marco G, Varetto F, "Corporate distress diagnosis: Comparisons using linear discriminant analysis and neural networks (the Italian experience)", Journal of banking & finance, vol.18, no.3, pp.505-29, may 1994.

[8] Phua C, Alahakoon D, Lee V, "Minority report in fraud detection: classification of skewed data", Acm sigkdd explorations newsletter, vol.6, no.1, pp.50-9, June 2004.

[9] Fan W, Miller M, Stolfo S, Lee W, Chan P, "Using artificial anomalies to detect unknown and known network intrusions", Knowledge and Information Systems, vol.6, no.5, pp.507-27, September 2004.

[10] Neill, D.B and Moore A.W, "Rapid detection of significant spatial clusters", In: Proc. of the 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 256–265, 2004.

[11] Brause R, Langsdorf T, Hepp M, "Neural data mining for credit card fraud detection", In Proceedings 11th International Conference on Tools with Artificial Intelligence, pp.103-106, November 1999.

[12] Zhou Z H and Liu X Y, "Training cost-sensitive neural networks with methods addressing the class imbalance problem", IEEE Transactions on knowledge and data engineering, vol.18, no.1, pp.63-77, December 2005.

[13] Huang C L, Chen M C, Wang C J, "Credit scoring with a data mining approach based on support vector machines", Expert systems with applications, vol.33, no.4, pp.847-56, November 2007.

[14] Awoyemi J O, Adetunmbi A O, Oluwadare S A, "Credit card fraud detection using machine learning techniques: A comparative analysis", In proceedings of 2017 International Conference on Computing Networking and Informatics (ICCNI), pp.1-9, October 2017.

[15] Fu, K., Cheng, D., Tu, Y., and Zhang, L., "Credit Card Fraud Detection Using Convolutional Neural Networks," Lecture Notes in Computer Science, pp.483– 490, 2016.

[16] Yang, Y. and Zhu, H., "A Study of Non-Normal Process Capability Analysis Based on Box-Cox Transformation", In proceedings of 3rd International Conference on Computational Intelligence and Applications (ICCIA), IEEE, pp. 240-243, July 2018.

[17] Ravisankar P, Ravi V, Rao G R, Bose I, "Detection of financial statement fraud and feature selection using data mining techniques", Decision support systems, vol.50, no.2, pp.491-500, January 2011.

[18] Jurgovsky J, Granitzer M, Ziegler K, Calabretto S, Portier P E, He-Guelton L, Caelen O, "Sequence classification for credit-card fraud detection", Expert Systems with Applications, vol.100, pp.234-45, June 2018.

[19] Kraus M and Feuerriegel S, "Decision support from financial disclosures with deep neural networks and transfer learning", Decision Support Systems, vol.104, pp.38-48, December 2017.

[20] Saia R, "A discrete wavelet transform approach to fraud detection", In proceedings of International Conference on Network and System Security, pp.464- 474, August 2017.

[21] Dal Pozzolo A, Boracchi G, Caelen O, Alippi C, Bontempi G, "Credit card fraud detection and concept-drift adaptation with delayed supervised information", In proceedings of 2015 international joint conference on Neural networks (IJCNN), pp.1-8, July 2015.

[22] Kamaruddin S and Ravi V, "Credit card fraud detection using big data analytics: use of PSOAANN based one-class classification", In Proceedings of the International Conference on Informatics and Analytics, pp.1-8, August 2016.

[23] Bolton R J and Hand D J, "Statistical fraud detection: A review", Statistical

[24] science, vol.235, pp.49, August 2002.

[25] Bahnsen A C, Aouada D, Stojanovic A, Ottersten B, "Feature engineering strategies for credit card fraud detection", Expert Systems with Applications, vol.51, pp.134-42, June 2016.

[26] Han F, Yao H F, Ling Q H, "An improved evolutionary extreme learning machine based on particle swarm optimization", Neurocomputing, vol.116, pp.87- 93, September 2013.

