http://communications.science.ankara.edu.tr

Commun.Fac.Sci.Univ.Ank.Series A2-A3
Volume 66, Number 1, Pages 82-94 (2024)
DOI: 10.33769/aupse.1361266
ISSN 1303-6009 E-ISSN 2618-6462

Research Article; Received: September 15, 2023; Accepted: October 30, 2023

A MACHINE LEARNING-BASED FRAMEWORK USING THE PARTICLE SWARM OPTIMIZATION ALGORITHM FOR CREDIT CARD FRAUD DETECTION

Abdullah Asım YILMAZ[1]

[1]Department of Computer Engineering, Atılım University, Ankara, TÜRKİYE

ABSTRACT. The detection of fraudulent activities in credit cards transactions presents a significant challenge due to the constantly changing and unpredictable tactics used by fraudsters, who take advantage of technological advancements to evade security measures and cause substantial financial harm. In this paper, we suggested a machine learning based methodology to detect fraud in credit cards. The suggested method contains four key phases, including data normalization, data preprocessing, feature selection, classification. For classification artificial neural network, decision tree, logistic regression, naive bayes, random forest while for feature selection particle swarm optimization is employed. With the use of a dataset created from European cardholders, the suggested method was tested. The experimental results show that the suggested method beats the other machine learning techniques and can successfully classify frauds with a high detection rate.

1. Introduction

Since the inception of credit cards and online payment systems, numerous individuals have discovered ways to deceive and unlawfully obtain credit card details in order to make unauthorized purchases. Consequently, a significant volume of fraudulent transactions occurs on a daily basis. In response, banks and e-commerce platforms are actively working to detect and prevent such fraudulent activities. They are leveraging deep learning (DL) and machine learning (ML) techniques to detect and halt fraudulent transactions before they are approved [1]. With the advancement of cutting-edge technology and global communication, fraudulent activities have been on the rise at an alarming rate [2]. As indicated by

Keywords. Credit card fraud detection, machine learning, particle swarm optimization.
abdullah.yilmaz@atilim.edu.tr-Corresponding author; 000-0002-3014-609X.

the Global Payments Report of 2015, credit cards emerged as the most widely utilized payment method worldwide in 2014 when compared to alternatives like e-wallets and bank transfers [3]. To conduct fraudulent actions using credit card services, cybercriminals usually target large-scale transactional services. Fraud using credit cards refers to transactions performed on atypical transaction patterns, inactive card, or unauthorized card use. [4]. Broadly speaking, credit card fraud can be classified into three main categories. These are conventional frauds (such as fake and stolen cards), merchant-related frauds (including merchant triangulation and collusion) and online frauds (involving counterfeit merchant websites) [5].

ML, a subset of Artificial Intelligence, has emerged as a prominent and widely discussed field in recent years. It has attracted significant attention, and numerous companies are now actively considering investments in machine learning to enhance their services. Machine learning involves employing a range of computer algorithms and statistical modeling techniques to enable computers to perform tasks without relying on explicit programming instructions [1]. Data mining refers to the procedure of extracting meaningful and insightful patterns from extensive collections of data, with the goal of uncovering descriptive, predictive, and valuable models [6]. By employing statistical and mathematical techniques, data mining techniques have the capacity to extract valuable information from large datasets. In the context of credit card fraud detection (CCFD), these techniques can be utilized to differentiate between normal and suspicious credit card transactions by identifying distinct characteristics [7]. On the other hand, ML is centered around learning and developing models to classify, cluster, or perform other tasks, rather than solely discovering valuable information like data mining [6]. Machine learning techniques have found extensive application across various domains in computer science. These domains include spam filtering, credit scoring, web search algorithms, recommendation systems, targeted advertising, fraud detection, classification problems and numerous other areas [8-12]. Machine learning classifiers function by constructing models based on sample inputs and utilizing them to make predictions or decisions, as opposed to relying solely on fixed program instructions. A wide range of machine learning approaches exists, each designed to address diverse and heterogeneous problems [13]. The model obtained would acquire knowledge from the "training data" and utilize that experiential knowledge to make predictions or carry out actions. DLs, which are a branch of ML, involve the use of artificial neural networks. Various methods such as restricted Boltzmann machines, recurrent neural networks, deep belief networks, generative adversarial networks, long short-term memory networks and convolutional neural networks are employed. A well-trained neural network would possess the ability to capture distinct relationships throughout the entire dataset [1].

2. Related Work

Awoyemi et al. [14] conducted a comparative analysis of different ML methods on credit card fraud dataset of European cardholders. In this study, it is used a hybrid sampling technique to solve the dataset's imbalance. The authors of study considered Naive Bayes (NB), K-Nearest Neighbors (KNN), and Logistic Regression (LR) ML methods and the implementation of the study was performed using the Python scripting language. Here, accuracy is used as the main metric value to measure how well each machine learning approach performs. According to the obtained empirical testing results, it was observed that LR, KNN, and NB each achieved accuracy levels of 54.86%, 97.69%, and 97.92%. In spite of the relatively strong performance of the KNN and NB, the authors did not take into account the possibility of utilizing a feature selection method.

Pumsirirat and Yan [15] proposed deep learning model to detect credit card fraud. The authors' goal is to concentrate on fraud cases that can't be identified using supervised learning. In this paper, proposed model was created using restricted Boltzmann machine and auto-encoder. In this study, the authors used tensor flow library from Google to implement their deep learning model include AE and RBM. According to the experimental results obtained on the datasets, suggested model produce high accuracy and Area Under Curve (AUC) score for huge fraud datasets. Sahin et al. [16] proposed a new cost-sensitive decision tree method to construct an fraud detection system for credit card transactions. This method uses support vector machines (SVM) and decision trees (DT). In this study, proposed method is compared with traditional classification models on a real world credit card dataset. The accuracy and true positive rate of the results show that the proposed method works better than other well-known methods.

Varmedja et al. [17] suggested CCFD approach utilizing ML on a credit card fraud dataset [18]. In order to solve the problem of imbalance of classes on CCFD dataset, the authors used synthetic minority oversampling technique (SMOTE). Multilayer perceptron, NB and RF ML techniques were employed to to assess the performance of suggested approach. According to the empirical results, the RF algorithm achieved the best fraud detection rate with 99.96% accuracy compared to MLP and NB ML methods.

3. Proposed Model for Credit Card Fraud Detection

This section presents the suggested framework for fraud detection. The suggested model for detecting fraud is ML-based and contains an optimized feature selection. This feature selection process provides with particle swarm optimization (PSO) algorithms. The suggested system's methodology, as shown in Figure 1, include four primary stages, namely, data normalization, data preprocessing, feature selection, and classification. First, data normalization is accomplished for to normalize the data in the training dataset. Second, the fraud detection data is pre-processed. SMOTE is used in this stage so as to sort out the class imbalance problem on the fraud detection data [19]. Third, feature selection operation is performed using PSO in order to get more accurate results in the classification process. Lastly, ML-based algorithms are used in order to carried out the classification processes.

For classification DT, RF, LR, Artificial Neural Network (ANN), and NB while for feature selection GA and PSO is employed in proposed method. The proposed method was tested using a dataset generated from European cardholders. The empirical results demonstrate that the suggested method beats the other machine learning techniques and can successfully classify frauds with a high detection rate.
An overview of the suggested model and the literature consulted for the suggested method are the two subsections that make up the remaining portion of this section. The model overview section first provides a detailed description of the proposed fraud detection framework for detecting fraud. Second, the literature consulted for the suggested method explain used feature selection technique and machine learning techniques that were employed in the proposed method.

3.1. **Overview of proposed model for fraud detection.** Figure 1 shows the architecture of the suggested methodology. In the first step, minimum-maximum scaling algorithm is utilized to normalize the fraud detection dataset in normalized data block (NDB) [20]. The mathematical formulation of minimum-maximum scaling algorithm is shown in Equation (1). In order to provide that each of the input values fall inside a predetermined range, scaling operation is performed. Second, NDB's normalized data is used to implement the PSO algorithm in PSO feature selection block (FSB). PSO creates candidate feature vector (FCV) an at each iteration of the PSO FSB. This FCV an is then used to test the trained models and train the models.

$$f_s = \frac{f - \min(f)}{\max(f - \min(f))} \tag{1}$$

3.2. **Literature Consulted for the Suggested Model.** The literature that was consulted in order to create the suggested fraud detection method is reviewed in this part, which is two subparts. First part provides a detailed explanation of the feature selection technique, and five well-known machine learning-based algorithms are described in second part.

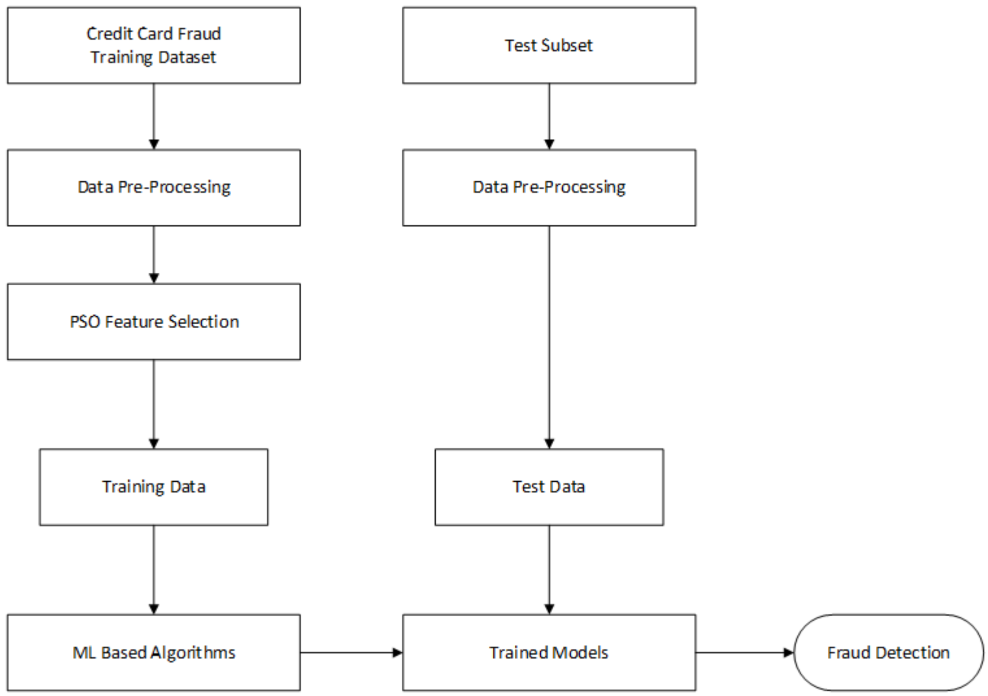

FIGURE 1. Architecture of the proposed framework.

3.2.1. *Feature Selection Methods*. PSO is an optimization method that draws inspiration from the group behavior of fish schools and flocks of birds. It aims to find ideal answer to issue by improving a group of potential solutions called particles through their cooperation and communication [21]. In PSO, particles represent potential solutions and move through a multi-dimensional search space. While particle's velocity dictates the magnitude and direction of motion, its position represents answer. According to their personal experience and the best experience of the entire group, particles modify their placements and velocities as they move through the search space [22]. The algorithm, whose flowchart is shown in the Figure 2, begins by initializing particles with random positions and velocities. Particles change their positions and velocities during each iteration using both the best position discovered by all other particles in the group (global best) and their individual best position (local best). This update is influenced by individual

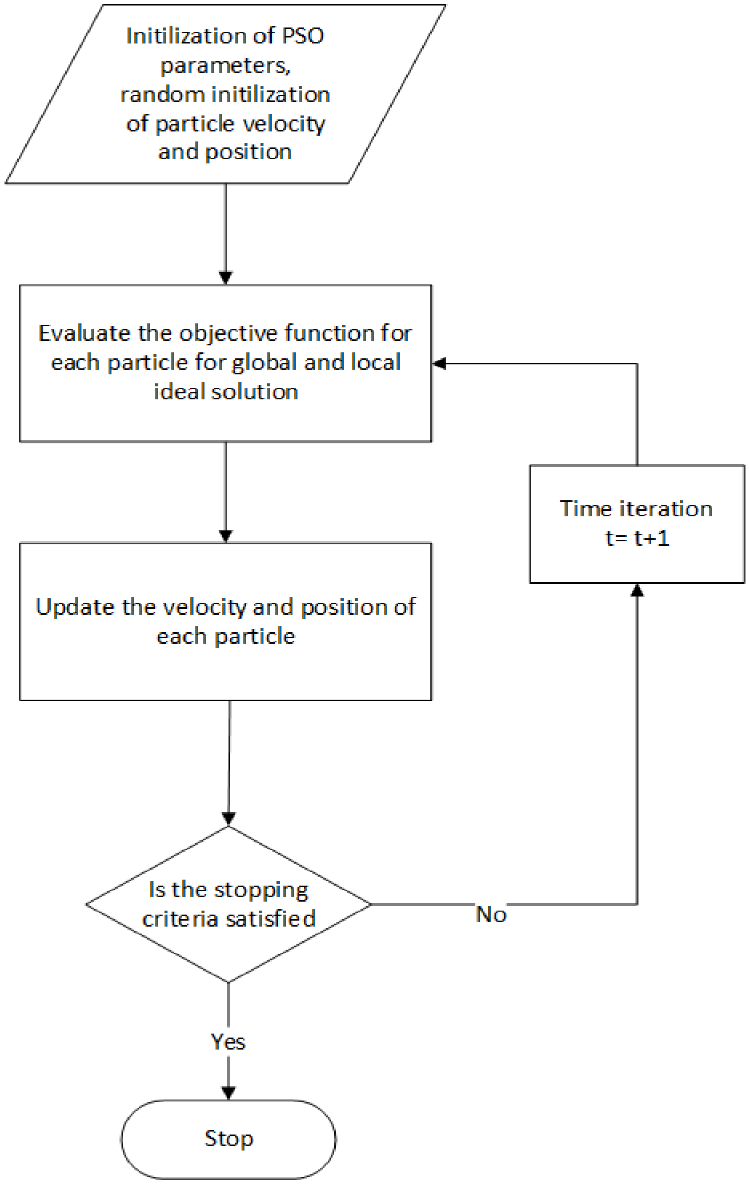

FIGURE 2. Flowchart of basic PSO algorithm.

experiences and the collective behavior of the group [23]. Social component and cognitive component are the two primary parts of the velocity update equation in PSO. The social component pulls particles in the direction of the ideal position discovered by any particle in the group, while the cognitive component directs particles toward their ideal position. These components balance exploration and exploitation, enabling efficient search in the solution space [24]. PSO iterates till a criterion for termination is satisfied, such as the required fitness value has been attained, and reaching a maximum number of iterations. The final positions of particles represent optimized solutions, or the best solution found [25]. PSO has been successfully used in various optimization problems [11], including function optimization, parameter tuning, neural network training, and feature selection.

3.2.2. *Machine Learning-Based Algorithms.* Despite its name, the Generalized Linear Models approach known as Logistic Regression is often referred to as Maximum Entropy. In this approach, a logistic function is used to characterize the probabilities that describe the potential outcomes of a single experiment. When there are one or more arguments, the output or result is determined using the logistic regression approach. The binary form of the output value is [26], which is either 0 or 1.

The data is divided using a condition in the Decision Tree classification. Data that meet the requirement are put in one class, while the rest are put in the other class. This procedure is iterative. There are various techniques for separation. These include similarity-based multi-attribute splitting, which compares terms in the document with predetermined words, and single-attribute splitting, which looks for the presence or absence of particular words for classification [27].

A learning technique for classification and regression is the Random Forest classification algorithm. Numerous decision trees are built throughout the training stage. To classify the fresh incoming state, the new state is sent to each of the trees. Each tree does categorization, and as a result, outputs a class. Based on majority vote, the output class is selected while taking into account the maximum number of related classes that the different trees can produce. The Random Forest approach is simple to understand and apply for both experts and laypeople, requiring little research and programming. Even those with little experience in statistics can use it with ease [28].

To extract features from a linear combination of data is the basic goal of the artificial neural networks technique and then model this obtained information as a nonlinear function of the features. Neural networks appear as a network diagram in which nodes are connected to each other in certain ways. Nodes are arranged in a layer. Architecturally, neural networks consist of three layers: hidden, ouput and input layer. Neural networks come in two varieties, namely, feedforward and feedback. Since the nodes are connected in only one direction in feedforward neural networks, this type of neural network is more suitable for sentiment analysis studies. Each link between nodes has a weight value that was determined by using the gradient descent approach to minimize the error function. A mathematical model that provides a value in two steps makes up a neuron. The weighted sum of the neuron input is determined in the first phase, and then an activation function is applied to this sum to produce output. With the use of input data from the complete network, the activation function, which is inherently nonlinear, can anticipate a previously learnt nonlinear function [29].

The NB approach is a classification algorithm based upon theorem of Bayes that has been utilized often in recent sentiment analysis studies. The assumptions made by naive Bayes classifiers are that the components (properties) of a given class are unrelated to one another in affinity. When attempting to divide the text into more than one class, the Naive Bayes approach is frequently utilized. [30].

4. Experimental Results and Discussions

The datasets used, the experimental findings, a review of the suggested model, and implementation specifics are all presented in this section. Python programming was used to carry out the proposed methodology's implementation. We used a personal PC with a 4.2 GHz Intel Core i5 11400H processor and 64 GB of RAM to carry out our studies. Additionally, a Linux system served as the setting for our tests.

4.1. **Dataset.** In our experimental studies, we utilize a fraud detection dataset, which consists credit card operations made by European cardholders. The total number of transactions in this dataset is 284807, with 0.172% of those transactions being fraudulent. This dataset contains 30 features, include (V1,..,V28), amount, and time. The dataset's attributes are all quantitative in type. The class (type of transaction) is represented by the last column. Here, zero value denotes non- fraudulent transaction while one value denotes fraudulent transaction. For purposes of data integrity and security, the features V1 through V28 are not named.

4.2. **Results and discussions.** Understanding the yield and performance of machine learning techniques requires an understanding of the assessment criteria used for classification processes. Evaluation metrics distinguish between model outcomes and explain how well the classification model performs [31]. Therefore, the suggested method's classification performance was indicated using accuracy, f-score, specificity, sensitivity metrics. The formulas in Table 1 were used to calculate these evaluation indicators. True negative, true positive, false negative, and false positive are represented in this table by the letters TN, TP, FN, and FP, respectively.

The experiments were run on a dataset of fraud [18]. FV = a1, a2, a3 was used in the classification procedure. The DT, RF, LR, ANN, and NB algorithms were trained and tested for each feature vector in FV. Tables 2, 3, and 4 provide the results. Both RF and ANN algorithms achieved the best test accuracy of 99.89% using a1, as shown in Table 2. However, in terms of precision, the RF approach produced the best results. Table 3's findings from the a2 test show that the RF method, with an accuracy of 99.88%, is the best model. The results that were attained when employing a3 are shown in Table 4. RF obtained 94.35% precision, 82.63 f-score and 99.92% accuracy rate for fraud detection in this case. a3 achieved the best outcomes when compared to a1, a2, and a3 results. Furthermore, the NB showed poorer performance concerning f1-score, precision and recall when compared to the results shown in Tables 2, 3, and 4.

To assess the effectiveness of the suggested paradigm, a comparison with other methodologies that are currently in use was also made. The accuracy values for both the proposed network and the other existing approaches are shown in Table 5. This table demonstrates with accuracy metric values that proposed method given and the majority of the suggested ML approaches that were applied outperformed suggested current methods in [33, 32, 17, 14]. Furthermore, the RF (implemented with v5) is the most accurate classifier in terms of classification. With an impressive accuracy of 99.92%, this model was able to detect credit card fraud.

TABLE 1. Assessment metrics formulations.

Evaluation metric	**Formula**
Sensitivity	TP / (TP+FN)
Accuracy	(TP+TN) / (TP+TN+FP+FN)
F-score	2*TP / (2*TP+FP+FN)
Specificity	TN / (TN+FP)

TABLE 2. Results of classification for feature vector a1.

Model	**Accuracy (%)**	**Recall (%)**	**Precision (%)**	**F-score (%)**
ANN	99.89	76.24	81.27	80.24
DT	99.87	74.12	74.34	68.66
NB	97.08	86.58	8.96	16.74
RF	99.89	75.56	88.49	82.57
LR	99.88	62.36	79.47	58.12

TABLE 3. Results of classification for feature vector a2.

Model	**Accuracy (%)**	**Recall (%)**	**Precision (%)**	**F-score (%)**
ANN	99.85	63.67	73.86	70.72
DT	99.81	66.28	61.52	57.45
NB	97.56	78.97	10.66	19.44
RF	99.88	74.26	83.73	79.36
LR	99.79	51.04	76.97	51.36

TABLE 4. Results of classification for feature vector a3.

Model	**Accuracy (%)**	**Recall (%)**	**Precision (%)**	**F-score (%)**
ANN	99.12	78.52	17.72	23.30
DT	99.81	73.34	68.65	69.51
NB	99.55	61.85	20.58	29.75
RF	99.92	73.36	94.35	82.63
LR	99.74	53.66	41.27	46.96

TABLE 5. Comparison with existing methods.

Model	**Accuracy (%)**
IF [14]	58.83
DT [32]	95.50
DT [34]	97.08
LR [33]	97.18
SVM [32]	97.50
LR [32]	97.70
NB [17]	99.23
PSO -NB (Proposed a3)	99.55
PSO-DT (Proposed a1)	99.87
PSO-LR (Proposed a1)	99.88
PSO-RF (Proposed a3)	**99.92**

5. CONCLUSION

ML-based technique for detecting credit card fraud was put out in this study. Using machine learning approaches, we provide a framework for fraud detection that incorporates improved feature selection. With PSO algorithms, this feature selection procedure is provided. Four primary processes make up the approach of the suggested system: data normalization, data preprocessing, feature selection, and classification. In order to normalize the data in the training dataset, data normalization is first completed. The data from the fraud detection procedure is then pre-processed. Third, feature selection operations are carried out utilizing PSO to produce more accurate classification results. In the output phase, a classifier based on ML (DT, RF, LR, ANN, NB) is used to perform the classification operations.

Three optimal feature vectors were produced when our suggested model was applied to the dataset of credit card transactions made by European cardholders. The experimental findings showed that the GA-RF (using v3) obtained an overall ideal accuracy of 99.92% using the PSO-selected features. Additionally, utilizing v1, other classifiers like the GA-DT were able to attain an astounding accuracy of 99.87%. Results from this study were better than those from earlier studies using similar techniques. In later studies, we intend to compare the results of more models and employ other global and metaheuristic search techniques for feature selection. We also intend to use several datasets to test the suggested strategy.

Declaration of Competing Interests The authors declare no conflict of interest.

References

[1] Raghavan, P., El Gayar, N., Fraud detection using machine learning and deep learning, *Int. Conf. on Comput. Intelligence and Knowledge Economy (ICCIKE)*, (2019), 334-339, https://doi.org/10.1109/ICCIKE47802.2019.9004231.

[2] Sisodia, D. S., Reddy, N. K., Bhandari, S., Performance evaluation of class balancing techniques for credit card fraud detection, *IEEE Int. Conf. on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, (2017), 2747-2752, https://doi.org/10.1109/ICPCSI.2017.8392219.

[3] WorldPay, Global payments report preview: The guide to the world of online payments, (2015). Available at: http://offers.worldpayglobal.com/rs/850-JOA856/images/GlobalPaymentsReportNov2015.pdf. [Accessed August 2023].

[4] Federal Trade Commission, Consumer sentinel network - data book for January, (2022). Available at: https://www.ftc.gov/. [Accessed August 2023].

[5] Bhatla, T. P., Prabhu, V., Dua, A., Understanding credit card frauds, *Cards Business Rev.*, 6 (2003), 1-15.

[6] Sahin, Y., Duman, E., Detecting credit card fraud by decision trees and support vector machines, *Int. MultiConf. of Engineers and Computer Scientists (IMECS)*, (2011), 1-5.

[7] Elkan, C., Magical thinking in data mining: Lessons from COIL challenge 2000, *ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining*, (2001), 426-431, https://doi.org/10.1145/502512.502576.

[8] Yilmaz, A. A., Guzel, M. S., Bostanci, E., Askerzade, I., A novel action recognition framework based on deep-learning and genetic algorithms. *IEEE Access*, 8 (2020), 100631-100644, https://doi.org/10.1109/ACCESS.2020.2997962.

[9] Aslan, Ö., Yilmaz, A. A., A new malware classification framework based on deep learning algorithms, *IEEE Access*, 8 (2021), 87936-87951, https://doi.org/10.1109/ACCESS.2021.3089586.

[10] Yilmaz, A. A., Guzel, M. S., Bostanci, E., Askerzade, I., A vehicle detection approach using deep learning methodologies, *Int. Conf. on Theoretical and Applied Computer Science and Engineering (ICTACSE)*, (2018), 64-71.

[11] Yilmaz, A. A., A novel hyperparameter optimization aided hand gesture recognition framework based on deep learning algorithms, *Trait. Du Signal*, 39 (3) (2022), 823-833, https://doi.org/10.18280/ts.390307.

[12] Yilmaz, A. A., Intrusion detection in computer networks using optimized machine learning algorithms, *Int. Informatics and Software Engineering Conf. (IISEC)*, (2022), 1-5, https://doi.org/10.1109/IISEC56263.2022.9998258.

[13] Yee, O. S., Sagadevan, S., Ahamed Hassain Malim, N. H., Credit card fraud detection using machine learning as data mining technique, *JTEC*, 10 (1-4) (2018), 23-27.

[14] Awoyemi, J. O., Adetunmbi, A. O., Oluwadare, S. A., Credit card fraud detection using machine learning techniques: A comparative analysis, *Int. Conf. on Computer Networks and Information (ICCNI)*, (2017), 1-9, https://doi.org/10.1109/ICCNI.2017.8123782.

[15] Pumsirirat, A., Liu, Y, Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine, IJACSA, 9 (1) (2018), 18-25, https://doi.org/10.14569/IJACSA.2018.090103.

[16] Sahin, Y., Bulkan, S., Duman, E., A cost-sensitive decision tree approach for fraud detection, *Expert Syst. Appl.*, 40 (15) (2013), 5916-5923, https://doi.org/10.1016/j.eswa.2013.05.021.

[17] Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M., Anderla, A., Credit card fraud detection-machine learning methods, *Int. Sympos. INFOTEH-JAHORINA*, (2019), 1-5, https://doi.org/10.1109/INFOTEH.2019.8717766.

[18] Kaggle Datasets: The credit card fraud detection dataset, (2013). Available at: https://www.kaggle.com/mlg-ulb/creditcardfraud. [Accessed August 2023].

[19] Guo, S., Liu, Y., Chen, R., Sun, X., Wang, X. X., Improved SMOTE algorithm to deal with imbalanced activity classes in smart homes, *Neural Process. Lett.*, 50 (2) *(2019)*, 1503-1526, https://doi.org/10.1007/s11063-018-9940-3.

[20] Jain, A., Nandakumar, K., Ross, A., Score normalization in multimodal biometric systems, *Pattern Recognit.*, 38 (12) (2005), 2270-2285, https://doi.org/10.1016/j.patcog.2005.01.012.

[21] Khan, S. U., Yang, S., Wang, L., L. Liu., A modified particle swarm optimization algorithm for global optimizations of inverse problems, *IEEE Trans. Magn.*, 52 (3) (2016), 1-4, https://doi.org/10.1109/TMAG.2015.2487678.

[22] Selvi, V., Umarani, R., Comparative analysis of ant colony and particle swarm optimization techniques, *IJCA*, 5 (4) (2010), 1-6, https://doi.org/10.5120/908-1286.

[23] Shi, Y., Eberhart, R. C., Empirical study of particle swarm optimization, *Proceedings of the 1999 Congress on Evolutionary Computation (CEC99)*, (1999), 1945-1950, https://doi.org/10.1109/CEC.1999.785511.

[24] Krohling, R. A., Gaussian swarm: A novel particle swarm optimization algorithm, *IEEE Conf. on Cybernetics and Intelligent Systems*, (2004), 372-376, https://doi.org/10.1109/ICCIS.2004.1460443.

[25] Bai, Q., Analysis of particle swarm optimization algorithm, *Comput. Inf. Sci.*, 3 (1) (2010), 180-184, https://doi.org/10.5539/cis.v3n1p180.

[26] Tyagi, A., Sharma, N., Sentiment Analysis using logistic regression and effective word score heuristic, *IJET*, 7 (2) (2018), 20-23, https://doi.org/10.14419/ijet.v7i2.24.11991.

[27] Kaur, H., Mangat V., A survey of sentiment analysis techniques, *Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, (2017), 921-925, https://doi.org/10.1109/I-SMAC.2017.8058315.

[28] Mamtesh, M., Mehla, S., Sentiment analysis of movie reviews using machine learning classifiers, *IJCA*, 182 (50) (2019), 25-28, https://doi.org/10.5120/ijca2019918756.

[29] Hemmatian, F., Sohrabi, M. K., A survey on classification techniques for opinion mining and sentiment analysis, *Artif. Intell. Rev.*, 52 (3) (2019), 1495-1545, https://doi.org/10.1007/s10462-017-9599-6.

[30] Alsaeedi, A., Khan, M. Z., A study on sentiment analysis techniques of twitter data, *IJACSA*, 10 (2) (2019), 361-374, https://doi.org/10.14569/IJACSA.2019.0100248.

[31] AnalyticsVidhya: Important model evaluation error metrics, (2019). Available at: https://www.analyticsvidhya.com/blog/2019/08/11important-model-evaluation-error-metrics. [Accessed August 2023].

[32] Khare, N., Sait, S. Y., Credit card fraud detection using machine learning models and collating machine learning models, *IJPAM*, 118 (20) (2018), 825-838.

[33] Seera, M., Lim, C. P., Kumar, A., Dhamotharan, L., Tan, K. H., An intelligent payment card fraud detection system, *Ann. Oper. Res.*, 8 (2021), 1-23, https://doi.org/10.1007/s10479-021-04149-2.

[34] Dornadula, V. N., Geetha, S., Credit card fraud detection using machine learning algorithms, *Procedia Comput. Sci.*, 165 (2019), 631-641, https://doi.org/10.1016/j.procs.2020.01.057.