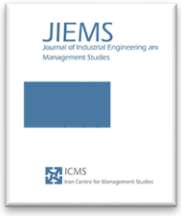
Vol. 11, No. 2, 2024, Pages 97-104

JIEMS
Journal of Industrial Engineering and Management Studies

journal homepage: www.jiems.icms.ac.ir



Hyperparameter Optimization based on grid search to detect fraud transactions in the banking industry

Maryam Asadi[1], Hassan Farsijani [2*]

[1] Faculty of Management, Department of Information Technology Management, Islamic Azad University, North Tehran Branch, Tehran, Iran

[2] Department of Management and Accounting, Shahid Beheshti University, Tehran, Iran

Received: Sep 2023-25/ Revised: Jun 2024-22/ Accepted: Dec 2024-10

Abstract

The ever-increasing volume and number of transactions in the bank make the fraud monitoring and detection process very complicated, costly, and time-consuming. In recent years, the development of new technologies has opened many ways for fraudsters and criminals to commit fraud. In this research, data mining methods are investigated in order to detect fraud in bank transactions. In order to detect fraud in bank card transactions, which are very unbalanced data types, the optimization of the support vector machine algorithm with hyperparameter techniques is presented and simulated on the Kaggle website data set, which includes bank card transactions, in the Python software environment has taken. The presented model benefits from bank transaction data and has the ability to extract complex patterns. As an effective optimization method, grid search technique intelligently adjusts the parameters of the support vector machine algorithm. The results of the model evaluation show that the support vector machine has a significant improvement in the detection of fraud patterns according to the criteria of accuracy and correctness. The combination of support vector machine and grid search technique as an innovative solution can help to improve the security of bank transactions in the digital age. In this research, hyperparameter optimization and smote balancing methods were used to reduce the number of false alarms. The proposed model can be commercialized and connected to the electronic banking system, online or offline, to detect fraudulent actions in transactions. The proposed model can be commercialized and connected to the electronic banking system, online or offline, to detect fraudulent actions in transaction.

Keywords: Optimization, Grid Search, Fraud, Support Vector Machine, safe Transaction.

Paper Type: Original Research

1. Introduction

One of the critical challenges of electronic banking is fraud in transactions, which can cause significant losses to banks and reduce trust in electronic banking. With the flourishing of the credit card business and Internet technology, the risk of fraudulent credit card transactions is ever-increasing due to the complex information involved in the credit card business. (Ni, Li, Xu, Wang, & Zhang, 2023) Fraud detection is one of the services of electronic banking. Analyzing the characteristics of a bank transaction can reveal the hidden pattern of fraud in it. The extraction of these patterns requires the use of knowledge discovery techniques such as machine learning. The dynamic shopping patterns of credit card holders and the class imbalance problem have made it difficult for ML algorithms to achieve optimal performance (Mienye & Sun, 2023). In this research, we propose a novel model for detecting fraud in the banking system. The novel model has two stages: balancing and classification of information. Although technology has made banking easier for customers, it has opened new avenues for fraud. Credit card fraud is a serious worldwide problem (Voican, 2021). Financial fraud statistics show that account fraud, credit card fraud, insurance fraud, and other fraudulent practices cost institutions and consumers millions of dollars annually. Detecting financial fraud is essential to minimize the risk to institutions. Fraudsters can drain personal accounts or charge thousands of dollars from credit cards. Even worse, organized crime rings can run elaborate schemes and steal millions of dollars. Financial and monetary institutions are looking for acceleration and speed of action in recognizing the activities of fraudsters and fraudsters. Credit card frauds comes under financial frauds that must be prevented and detected in a very short time (Sadgali, Sael & Benabbou, 2018). It is due to its direct effect on serving the clients of these institutions, reducing operational costs, and remaining a reliable and credible financial services provider. Therefore, it is inevitable to use fraud detection techniques to prevent fraudulent actions in

*Corresponding Author: h-farsi@sbu.ac.ir

banking systems, especially electronic banking. By applying cognitive computing technologies to raw data processing, it is possible to predict fraud in a large volume of transactions. This is why machine learning is used to prevent financial fraud. At the core of machine learning is a three-stage cycle that includes training, testing, and predicting. Machine Learning (ML) is a sub-field of Artificial Intelligence (AI) that allows computers to learn from previous experience (data) and to improve on their predictive abilities without explicitly being programmed to do so (Burkov, 2019). Cycle optimization makes more accurate predictions and can be used in specific applications. One of the methods is to use the parameter setting technique to reach hyperparameters. Improving the performance of machine learning methods, which can be done by adjusting its hyperparameter, is very important (Wu, Chen, Zhang, Xiong, Lei & Deng, 2019). Therefore, in this study, an approach with optimization of grid search is proposed. Hyperparameter optimization plays a vital role in the prediction accuracy of machine learning algorithms (Patel & Singh, 2013). The grid search technique has been used to optimize the support vector machine algorithm. In this research, by using the programming facilities of the Python environment, the proposed method was implemented on the data set related to bank fraud and based on various tests and according to various indicators such as accuracy, sensitivity and accuracy, the proposed method was evaluated. To analyze its effectiveness in fraud detection.

2. Literature Review

Electronic banking is a type of banking where all money transfers and banking processes are managed over the internet and electronically, without the need for customers to be physically present at the bank. Electronic banking utilizes advanced hardware, software, networking, and telecommunications technologies. In other words, electronic banking involves the use of advanced software and hardware technologies based on networking and telecommunications for the electronic exchange of financial resources and information, without the need for customers to be physically present at bank branches. The most important advantages of electronic banking are: the ability of customers to receive banking services without physical presence with secure communication, using the Internet to provide banking operations and services and to apply changes to all types of customer accounts, directly providing new and traditional banking services and operations to customers from through card-to-card electronic mutual communication channels. Nowadays, the use of online transactions has become very common and as a result, the cases of online fraud have also increased. Fraudsters have become very adept at discovering and exploiting flaws in systems that make managing fraud in the banking and financial industry extremely difficult. Fraud in electronic banking has become a challenge around the world, as many banks have gone bankrupt and many of their customers' assets have been lost. On the other hand, criminals are trying to reduce fraud detection by using new techniques to steal bank and customer assets. Fraud in electronic banking occurs when a fraudulent person commits bank fraud using the Internet. Fraud and fraudulent activities have disastrous financial consequences. Financial fraud is a fundamental problem that affects both the financial sector and daily life and plays an important role in influencing the integrity and trust in the financial sector as well as the cost of living of people (Choi and Lee, 2018). Attention of financial transactions, they are exposed to the risk of financial fraud. (West and Bhattacharya, 2016), by applying cognitive computing technologies in raw data processing, predicted frauds in a large volume of transactions. That is why to prevent fraud in business finance, machine learning is used. Banks can use machine learning to analyze unstructured information, such as monitoring social media and scrutinizing customer accounts to identify anomalies. Data mining is very important for e-commerce and provides valuable knowledge to the company. For this reason, researchers are looking for efficient data mining techniques in order to discover and extract knowledge from huge amounts of data and information. In this section, we present the work done in the field of fraud detection in transactions for better performance. Patel, Rinky, et al. & Singh, D. K. (2013) Used Genetic Algorithm to detect credit card fraud. Using the Genetic Algorithm, they minimized the number of false alarms. Instead of maximizing the number of correctly classified transactions, they defined an objective function where the costs of misclassification are variable, and thus correctly classifying some transactions is more important than correctly classifying other transactions. Pouramirarsalani et al. (2017) presented a novel approach based on neural network and reinforcement learning method with the aim of detecting fraud in electronic banking. Benchaji et al. (2019) use Genetic Algorithm to improve the classification of unbalanced datasets for credit card fraud detection. The K-means algorithm is used to cluster and group the sample minority type, and in each cluster used the Genetic Algorithm to obtain new samples and build an accurate fraud detection classification. Ojugo et al. (2021) propose a spectral clustering combination of modular neural network trained with Genetic Algorithm for fraud detection in credit card transactions. The results show that the hybrid model effectively differentiates between benign and genuine credit card transactions with a model accuracy of 74%. Tiwari et al. (2021) compared a number of data mining algorithms for fraud detection. These algorithms include hidden Markov model, decision trees, logistic regression, SVMs, Genetic Algorithm, neural networks, random forests, and Bayesian network. A comprehensive analysis of different techniques is presented in this research. Seera et al. (2021) applied 13 machine learning and

statistical models to credit card fraud detection. In this research, a statistical hypothesis test was used to evaluate whether the aggregate features identified by a Genetic Algorithm can provide better detection power compared to the original features. Ileberi et al. (2016) propose a credit card fraud detection engine based on ML machine learning using GA Genetic Algorithm for feature selection. After selecting the optimized features, the proposed detection engine uses the following ML classifiers: decision tree, (DT, random forest), (RF, logistic regression), (LR), (artificial neural network), (ANN) (NB) to verify the performance, the proposed credit card fraud detection engine is evaluated using a dataset generated from European cardholders. The dynamic purchasing patterns of credit card holders and the problem of class imbalance make it difficult for machine learning algorithms to achieve optimal performance. (Maini, 2023) In detecting fraud, the goal is to correctly classify transactions into legitimate and fraudulent. In this field, a lot of research has been done so far, however, the optimization of meta-parameters using meta-heuristic techniques, in less time and with more accuracy, is still IT is the concern of many organizations. Investigating the types of frauds in electronic banking and finally providing an optimal solution to deal with the threats will help financial institutions to move towards risk-free banking and customer satisfaction. Network infrastructure and transaction systems are constantly monitored and verified by cybercrime experts. (Sarkosh, 2023) In 2015, Ganesh et al presented a new proposed method based on support vector machine combined with the nearest neighbor technique to detect fraud in credit cards and car insurance. The results of their research show that the proposed method is more accurate than methods such as decision tree, logical regression, probabilistic artificial neural network and multilayer artificial neural network. Pooja Tiwari et al presented methodologies of Hidden Markov Model, Decision Trees, Logistic Regression, Support Vector Machines, Genetic Algorithm, Neural Networks, Random Forests, Bayesian Network for credit card fraud detection. A comprehensive analysis of various techniques has shown the good performance of the support vector machine algorithm compared to other algorithms. Sudha et al. propose support vector machine and random forest algorithms for credit card fraud detection. Users' operational features were extracted and then random forest classifier and support vector machine were used to classify the features into healthy and suspicious. System performance based on accuracy, precision, recall and F-1 score criteria showed that both classifiers provided high recognition rates with good accuracy. Gyamfi et al used supervised learning methods of support vector machines to build models that represent normal and abnormal customer behavior and then used it to evaluate the validity of new transactions. Results obtained from credit card transaction databases show that these techniques are effective in combating bank fraud in big data. Experimental results from this study show that support vector machine has better prediction performance than back propagation networks. Chen et al. used support vector machine algorithm and artificial neural networks to investigate the time-varying cheating problem. The results show that support vector machines and artificial neural networks are comparable in training, but neural networks show higher accuracy. However, neural networks overfit the training data and therefore do not perform well in data prediction, especially for small databases. Based on real credit card business transaction data, Li et al. first finds the optimal kernel function suitable for the dataset. In the second step, he proposes the optimization method of support vector machine parameters with cuckoo search algorithm, genetic algorithm and particle swarm optimization algorithm. Particle swarm optimization algorithm, linear kernel function was recognized as the best kernel function with an accuracy rate of 91.56%. In addition, the radial basis function was used to optimize the kernel function, which can increase the accuracy from 42.86% to the highest accuracy rate of 98.05%. In 2013, Sahin et al presented a new method to detect bank fraud in credit cards using a cost-sensitive decision tree technique. By understanding the necessity of anti-bank fraud systems and the knowledge of the development of fraud methods with the advancement of technology, they presented their proposed method. In their study and research, they presented an approach based on decision tree by reducing the cost of classifying abnormal transactions from normal ones. In this method, each end node of the tree is expanded when it provides the lowest classification cost for fraud detection. The results of the implementation of their method show that at least it is more accurate in identifying bank fraud than methods such as decision tree, support vector machine and artificial neural network. On the other hand, their research results show that the financial losses caused by Fake transactions can be significantly reduced by implementing this method in banking systems. In 2014, Gary et al discussed the role of data mining algorithms in fraud detection in the banking system in a review study. In their study, they showed that data mining methods can extract useful knowledge and hidden patterns to detect fraud, and they can be used as reliable methods in detecting fraud. Winkler et al. have presented a new representation that includes both index selection and parameter optimization of a specific classification algorithm such as a support vector machine. The length is equal to the total number of indicators and parameters. Today, fraud and violation, which is as old as the life of humanity, is considered a lucrative business in the world, and it is increasing day by day. The results of the evaluation and studies show that the patterns in fraud are complex and to detect these patterns, appropriate tools and methods of knowledge discovery such as data mining and machine learning are needed. The results of the review of articles show that techniques such as support vector machine have a more accurate ability to detect fraud than other supervised learning methods. By reviewing the field of

fraud detection, it can be concluded that fraud detection is one of the most important issues in the world, which still needs more discussion and investigation. However, in this research, an attempt is made to simulate the real environment to some extent and detect fraudulent transactions.

3. Conceptual model

In this figure, the conceptual model of the implemented method was shown.

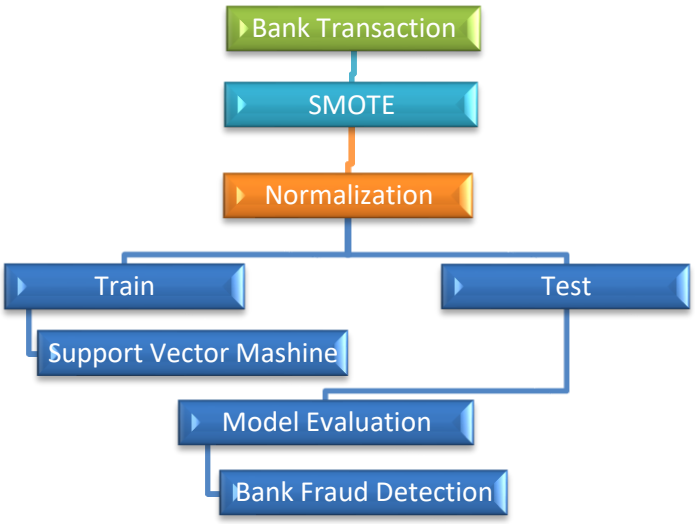


Figure 1. the conceptual model of the implemented method

4. Dataset

The bank transaction data set was downloaded from the Kaggle site, which includes credit card transactions made by European cardholders for 2 days in September 2013. This data set contains 284,807 transactions, in which 17% of transactions are IT is fake. All its features are numerical. The last column class shows the type of transaction whether it is healthy or fraudulent, a value of one is a fraudulent transaction and a value of zero is a healthy transaction. This total data includes features extracted from the original data and due to security issues, the original information of the users is not known. Features v1 through v28 are not named for security reasons. We called this dataset by Pandas. Available from this dataset .The bank transaction dataset is downloaded from and read by Pandas. This total data includes features extracted from the original data and due to security issues, the original information of the users is not known.

4.1. Data set preprocessing

This stage of the data mining process is one of the most important stages, because all data mining projects and modeling results are closely related to data and their quality. In this step, all possible problems and defects are found in the data set and appropriate solutions are suggested to solve these problems. Finally, the refined data is removed from this part and goes to the modeling stage. To prepare the data, it is necessary to remove it from its original form and transform it into a suitable form for the algorithm. Also, the available data usually have various frills that may cause the algorithm to make an error. In the first step, the transaction without value or duplicates were deleted. The dataset is visualized with Matplotlib tools for better understanding. The first chart is a Count Plot chart. Purple color indicates normal transactions and yellow color indicates abnormal transactions. This dataset is highly unbalanced.

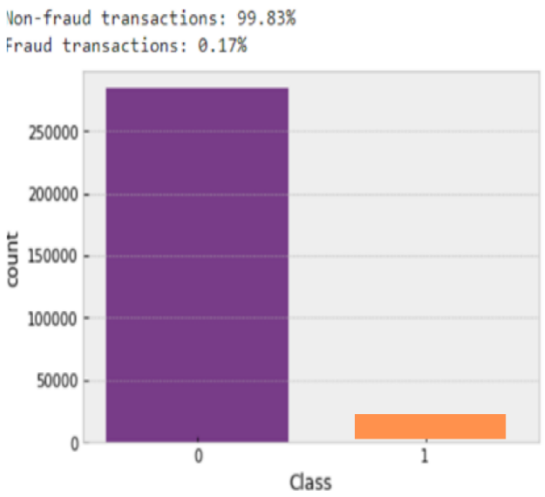


Figure 2. An image of the dataset before pre-processing

Figure 2 depicts a bar graph of the distribution of healthy and fraudulent transactions in a data set. The horizontal axis (Class): contains class 0, which represents non-fraudulent transactions, and class 1, which represents fraudulent transactions. The vertical axis (Count): displays the number of transactions in each category. The purple column represents healthy transactions with a value of 99.83%. These transactions make up the majority of the entire data set. The orange column represents fraudulent transactions with a value of 0.17%. This distribution indicates a significant imbalance in the data set, where non-fraudulent transactions significantly outnumber fraudulent transactions. This imbalance creates a challenge in fraud detection, as machine learning models may tend to focus more on the majority class (non-fraudulent transactions) and reduce accuracy in identifying fraudulent transactions.

5. Data normalization with SMOTE method

The efficiency of machine learning algorithms is usually evaluated using prediction accuracy. However, this is not appropriate when the data is unbalanced. Using an appropriate sampling method can ensure the success of learning algorithms in generalizing the training done to the testing stage. One of the methods that can help us solve the problem of uneven distribution of samples in classes is artificial minority oversampling technique. In resampling techniques, the data is reused, but in this method, new synthetic data samples are generated in the neighborhood of the samples in the classes. The artificial minority oversampling technique for the minority class generates new samples in the neighborhood of the existing samples in this class. The new synthetic samples are placed on a line and connected to the samples of the minority class that are adjacent to them. Properties of instances in adjacent classes are not changed. Because of this, this technique can produce samples that belong to the same original distribution. Unlike the resampling method, in this method, the new dataset will have a higher standard deviation and a suitable classifier can easily find a better separating hyperplane. The Synthetic Minority Oversampling Technique is in the unbalanced-learn software package. This algorithm generates new examples for the minority class in the neighborhood of the existing examples in this class. This method can produce samples that belong to the same original distribution.

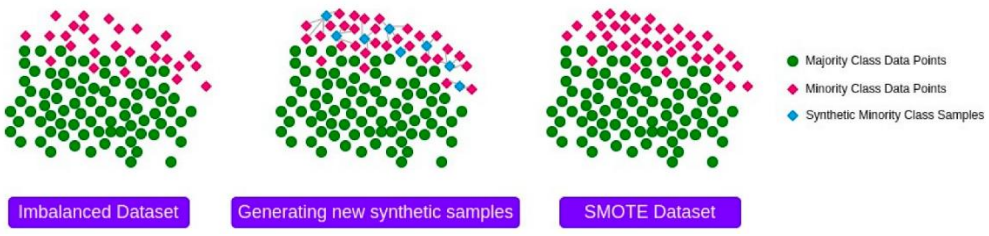


Figure 3. Artificial minority oversampling technique

Figure 3 shows three scatter plots, each representing a process for handling imbalanced data in a dataset:

1. "Imbalanced Dataset" plot: This plot shows an imbalanced distribution of data with a large number of majority class data points (green circles) and a small number of minority class data points (pink diamonds).

2. "Generating new synthetic sample" plot: In addition to the original data (green circles and pink diamonds), new synthetic minority samples (blue diamonds) have been generated.

3. "SMOTE Dataset" plot: This plot shows a balance between the two classes, with a better distribution of minority points (pink and blue diamonds) and the majority class.

The SMOTE process is a technique for generating synthetic data to balance the minority class. This technique is used in machine learning to improve the performance of models.

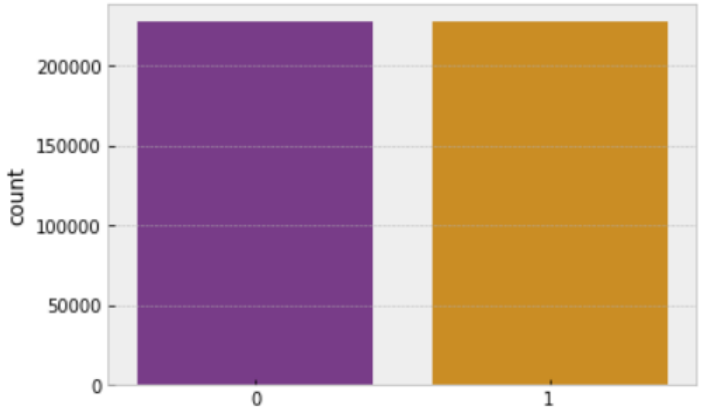


Figure 4. Data image after balancing

The dataset is divided into two parts, training data, and test data, for fair evaluation. This division is separated by similar distribution in terms of classes. Performance evaluation criteria calculated in this research, Mean Squared Error test MSE is the measure of Accuracy, Recall, Specificity, Precision, and F-measure.

6. Proposed Solution

There are different types of machine learning algorithm evaluation criteria. It is possible that the model gives satisfactory results when evaluated using the accuracy criterion, but when evaluated against other criteria such as accuracy or other criteria, it obtains poor results. Most of the time, classification accuracy is used to measure the performance of the model, but it is not enough to make a real judgment about the model. Models are as useful as the quality of their predictions, and our goal is not to create models, but to create high quality models. We used this test to see how well the models are able to predict data that they have never seen before. The mean square error is used to predict the model error when faced with new data. We used Numpy and Scikit-Learn library for implementation.

$$MSE = \frac{1}{n}\sum_{i=1}^{n} \left(Y_i - \hat{Y}_i\right)^2 \quad (1)$$

The above formula is the mean square formula which is used to measure prediction errors. In this formula, Y_i represents the actual dependent value (original value) for sample i, and Y_i represents the predicted value for dependent value of sample i. Also, n is the total number of samples. Using this formula, the mean squared error between the actual and predicted value is calculated for each sample. Then we add the squared errors and divide by the total number of samples to get the mean squared error. The mean squared error is a common measure in evaluating the quality of models, so that a lower value of MSE indicates a better match between the predictions and the actual values. To improve the performance of the model, we can minimize the MSE and increase the accuracy of the predictions by changing the parameters and techniques. The smaller this error is, the more efficient the model is.

Accuracy: Things that are correctly predicted.

$$Accuracy = \frac{TP + TN}{TP+TN+FP+FN} \quad (2)$$

Recall: Maximum accuracy in detecting the positive class for classification evaluation.

$$\text{Recall}=\frac{TP}{TP+FN} \quad (3)$$

Specificity: Negative cases that are correctly diagnosed.

$$\text{Specificity}=\frac{TN}{TN+FP} \quad (4)$$

Precision: When the model predicts the result positively, how true is this result.

$$\text{Precision}=\frac{TP}{TP+FP} \quad (5)$$

F-measure: Harmonic mean accuracy and recall evaluating model accuracy.

$$F1=2.\frac{\text{Precision}\cdot\text{Recall}}{\text{Precision}+\text{Recall}} \quad (6)$$

In machine learning, hyperparameters refer to parameters that cannot be learned from data and must be provided before training. The performance of machine learning models is highly dependent on finding the optimal set of hyperparameters. Hyperparameter optimization is finding the best combination of algorithm parameters in such a way that the efficiency of the model is improved. This algorithm is search in nature. For each combination of parameters of the algorithm, which is specified in the mesh network, it builds and evaluates the model in a methodical way. The tuning parameter C and the gamma kernel coefficient are two important hyperparameters in SVC:

• The tuning parameter C determines the tuning strength.

• The gamma kernel coefficient controls the width of the kernel. By default, SVC uses a radial basis function (RBF) kernel (also known as a Gaussian kernel).

We used the Scikit-learn library to implement Grid Search. Hyperparameters of SVM algorithm are optimized with Grid Search on c, gamma and kernel to find the best model. A Support Vector Machine (SVM) is a discriminative classifier formally defined by a separating hyperplane (Rabbani et al., 2020). The SVM algorithm is one of the relatively new methods that has shown good performance compared to the older classification methods in recent years. The working basis of SVM classifier is the linear classification of data, and in the linear division of data, we try to choose a line that has a higher margin of confidence. Grid Search algorithm belongs to the family of brute force methods. In other words, in this method, all the backtests are executed and then they are ranked.

7. Data Analysis

In this research, detection, identification and classification of healthy and fraudulent transactions were done using the combined method of support vector machine with grid search technique and the results obtained from the algorithm were compared based on different criteria. The outputs and results indicate the high speed and accuracy of the support vector machine algorithm. The results showed that the optimization of the support vector machine algorithm in many criteria, the most important of which are precision and accuracy, has a good performance in detecting fraudulent transactions. Figure 2 shows the value obtained for the accuracy criterion of the vector machine algorithm after optimization with grid search technique. This measure shows the accuracy of detecting the desired transactions compared to the total number of cases suggested by the algorithm for a label. As it is clear in the figure, this value for the support vector machine algorithm combination is equal to 94% with a mean square error of 22%.

Table1. Output of support vector machine algorithm optimized with grid search technique

accuracy	Mean Squared error	F1-score	recall	precision
0.94	0.22	0.95	0.93	0.97

8. Conclusion

Our study shows the effectiveness of using the support vector machine algorithm along with the meta-parameter optimization technique to detect fraud in electronic banking systems. Unlike conventional methods, the use of network search to fine-tune parameters automatically focuses on dynamic optimization of hyperparameters while saving processing time. The integration of these techniques not only ensures high accuracy and F1 scores, but also emphasizes the critical role of comprehensive datasets in enhancing model performance. These findings have significant implications for real-world applications, particularly in the financial sector, where fraud detection is a priority. In the face of increasing financial threats, this research provides a valuable contribution to the development of robust fraud detection methods. With seamless integration in electronic banking systems, the proposed model is a reliable solution to identify and prevent fraudulent transactions, thus protecting the integrity of banking services and reducing significant financial risks. As the exploration of alternative meta-heuristic algorithms such as evolutionary algorithms progresses, there is promise to further increase the optimization of fraud detection parameters and foster the development of even more sophisticated and accurate fraud detection systems.

References

Benchaji, I., Douzi, S., & El Ouahidi, B. (2019). Using genetic algorithm to improve classification of imbalanced datasets for credit card fraud detection. In Smart Data and Computational Intelligence: Proceedings of the International Conference on Advanced Information Technology, Services and Systems (AIT2S-18) Held on October 17–18, 2018 in Mohammedia 3 (pp. 220-229). Springer International Publishing.

Burkov, A. (2019). The hundred-page machine learning book (Vol. 1, p. 32). Quebec City, QC, Canada: Andriy Burkov.

Chen, R. C., Luo, S. T., Liang, X., & Lee, V. C. (2005, October). Personalized approach based on SVM and ANN for detecting credit card fraud. In 2005 international conference on neural networks and brain (Vol. 2, pp. 810-815). IEEE.

Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. Security and Communication Networks, 2018.

Gyamfi, N. K., & Abdulai, J. D. (2018, November). Bank fraud detection using support vector machine. In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 37-41). IEEE.

Li, C., Ding, N., Zhai, Y., & Dong, H. (2021). Comparative study on credit card fraud detection based on different support vector machines. Intelligent Data Analysis, 25(1), 105-119.

Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. Journal of Big Data, 9(1), 1-17.

Mienye, I. D., & Sun, Y. (2023). A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection. IEEE Access, 11, 30628-30638.

Ni, L., Li, J., Xu, H., Wang, X., & Zhang, J. (2023). Fraud feature boosting mechanism and spiral oversampling balancing technique for credit card fraud detection. IEEE Transactions on Computational Social Systems.

Ojugo, A. A., & Nwankwo, O. (2021). Spectral-cluster solution for credit-card fraud detection using a genetic algorithm trained modular deep learning neural network. JINAV: Journal of Information and Visualization, 2(1), 15-24.

Patel, R. D., & Singh, D. K. (2013). Credit card fraud detection & prevention of fraud using genetic algorithm. International Journal of Soft Computing and Engineering, 2(6), 292-294.

Pouramirarsalani, A., Khalilian, M., & Nikravanshalmani, A. (2017). Fraud detection in E-banking by using the hybrid feature selection and evolutionary algorithms. International Journal of Computer Science and Network Security, 17(8), 271-279.

Rabbani, M., Abazari, A., & Farrokhi-Asl, H. (2020). An economic analysis for integrated bi-objective biofuel supply chain design using support vector machine. Journal of Industrial Engineering and Management Studies, 7(2), 77-97.

Sadgali, I., Sael, N., & Benabbou, F. (2018). Detection of credit card fraud: State of art. Int. J. Comput. Sci. Netw. Secur, 18(11), 76-83.

Sahin, Y., Bulkan, S., & Duman, E. (2013). A cost-sensitive decision tree approach for fraud detection. Expert Systems with Applications, 40(15), 5916-5923.

Seera, M., Lim, C. P., Kumar, A., Dhamotharan, L., & Tan, K. H. (2021). An intelligent payment card fraud detection system. Annals of operations research, 1-23.

Srokosz, M., Bobyk, A., Ksiezopolski, B., & Wydra, M. (2023). Machine-Learning-Based Scoring System for Antifraud CISIRTs in Banking Environment. Electronics, 12(1), 251.

Sudha, C., & Akila, D. (2021, January). Credit card fraud detection system based on operational & transaction features using svm and random forest classifiers. In 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 133-138). IEEE.

Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J., & Singh, A. K. (2021). Credit card fraud detection using machine learning: a study. arXiv preprint arXiv:2108.10005.

Voican, O. (2021). Credit Card Fraud Detection using Deep Learning Techniques. Informatica Economica, 25(1).

Wu, J., Chen, X. Y., Zhang, H., Xiong, L. D., Lei, H., & Deng, S. H. (2019). Hyperparameter optimization for machine learning models based on Bayesian optimization. Journal of Electronic Science and Technology, 17(1), 26-40.

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. Computers & security, 57, 47-66.