International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received:** 25 May 2023 **Revised:** 12 June 2023 **Accepted:** 30 July 2023*

Credit Card Fraud Detection Using Optimized Ensemble Learning Models

Ms. Smita Tripathi

Research Scholar, Department of Computer Application,
Sri Satya Sai University of Technology & Medical Sciences, Sehore, Pachama, Madhya Pradesh, India
Email ID: Smita_mca2004@rediffmail.com

Dr.Narendra Sharma
HOD, Computer Science and Engineering
Sri Satya Sai University of Technology & Medical Sciences, Sehore, Pachama, Madhya Pradesh, India

Corresponding Author: Ms. Smita Tripathi

Abstract:

Credit card fraud poses a significant threat to financial institutions and their clientele worldwide. Many current fraud detection methods lag behind the evolving strategies of fraudsters, resulting in escalating financial risks. This study outlines a robust method for detecting credit card fraud, employing optimal ensemble learning techniques. The proposed approach integrates ensemble learning principles into both stacking and boosting methodologies, utilizing model parameters to bolster the accuracy and resilience of fraud detection. The research investigates various ensemble learning algorithms and evaluates their effectiveness in identifying fraudulent transactions using real transactional data. The experimental results demonstrate the ability of optimized ensemble learning models to detect fraudulent activities, underscoring their potential to enhance security measures against credit card fraud

Keywords: Data Mining, Fuzzy Logic, Machine Learning, logistic regression, SVM, K-Nearest Neighbor (KNN),

Introduction:

Concerning credit cards, they represent one of the most significant threats to financial institutions. It poses a significant and continuously evolving threat to both financial institutions and consumers(Pomerleau & Lowery, 2020). Credit card fraud is defined as: “when an individual uses another individual’s credit card for personal reasons while the owner of the card and card issuer are not aware of the fact that the card is being used.”According to (Bhatla et al., 2003) as digital transactions grow the tactics employed by fraudsters are also evolving to exploit vulnerabilities in the system. Fraudulent activities such as unauthorized transactions, account takeovers, and identity thefts result in financial losses for banks and cardholders but also jeopardized trust in electronic payment systems. The impact of credit card fraud leads to monetary losses, damaged credit scores and loss of trust in the security of their financial accounts. For financial institutions the cost associated with fraud detection, investigation and reimbursement of fraudulent transactions lead to substantial damage that can result from security breaches. Due to these challenges, there is an urgent need to develop advanced fraud detection mechanisms capable of identifying and preventing fraudulent activities in real time. Conventional rule-based systems and statistical models have limitations in keeping pace with the rapidly evolving nature of fraud, it leads to the explorations of more sophisticated approaches.

An area that holds promise for enhancing accuracy and resilience in fraud detection is the ensemble approach. Ensemble learning combines multiple base classifiers, leveraging their individual strengths and compensating for weaknesses to achieve higher predictive accuracy and reliability. We introduce an enhanced credit card fraud detection model achieved through ensemble learning, with the goal of mitigating risks and safeguarding against financial losses for both financial institutions and their customers

Background and Related works:

Detection of credit card frauds has been a subject of extensive research with various methods and techniques proposed to address challenges posed by fraudulent activities. “In practical scenarios, fraudulent transactions are interspersed among legitimate ones, making conventional pattern matching methods inadequate for precise fraud identification. Consequently, the deployment of robust fraud detection systems has become crucial for all credit card issuers to mitigate potential losses. Various modern approaches, such as Artificial Intelligence, Data Mining, Fuzzy Logic, Machine Learning, Sequence Alignment, and Genetic Programming, have significantly improved the identification of a wide range of fraudulent activities related to credit cards(Saravanan & Sujatha, 2018). This section provides a review of existing literature on the methods of credit card fraud detection, including rule based systems, statistical models, machine learning approaches and ensemble learning techniques. Furthermore, it explores the theoretical foundations of ensemble learning and its applications in fraud detection, Subsequent to the discussion; we will conduct a critical analysis of prior research concerning the implementation of ensemble learning models. In credit card fraud detection,highlighting their strengths and limitations. In this paper(Delamaire et al., 2009) researchers have identified various types of frauds and measures to detect them, such measures are decision tree, clustering, genetic algorithms and neural networks.

1. Credit card fraud detection methods:

Rule based Systems:
Rule based systems rely on predefined rules and thresholds to flag suspicious transactions based on pre-defined criteria such as unusual transaction amounts, locations or frequency. While these systems are simple to implement and interpret, rule-based systems may lack flexibility in adapting to evolving fraud patterns.

Statistical Models:
Statistical models utilize mathematical algorithms to analyze transaction data and identify patterns indicative of fraudulent activity. Techniques such as logistic regression, time series analysis and Bayesian networks have been used to detect anomalies and outliers in transactions done through credit cards.

Machine Learning Models:
Machine learning methods have extensively implemented supervised, unsupervised, and semi-supervised learning—a way for getting insights on information and adapting to changing fraud schemes. Supervised learning models like decision trees, support vector machines (SVM), and neural networks are applied to categorize transactions as fraudulent or legitimate, leveraging past data for classification.

Ensemble learning techniques:
Ensemble learning combines multiple base models to improve prediction accuracy and robustness. Techniques such as bagging (e.g. Random Forest), boosting (e.g. Adaboost, Gradient Boosting), and Stacking has been employed in credit card fraud detection, leveraging a variety of base classifiers to capture distinct facets of fraud patterns.

2. Theoretical Foundations of Ensemble Learning:

Ensemble learning is rooted in the concept of combining multiple weak learners to create a strong learner that outperforms any individual classifier. Ensemble learning aims to integrate data fusion, data modeling and data mining into a unified framework. ensemble learning extracts a set of features with variety of transformations, based on these learned features multiple learning algorithms are applied to produce weak predictive results. Finally, ensemble learning fuses the informative knowledge from above results(Dong et al., 2020). The diversity among base classifiers, achieved through different training algorithms or feature subsets, ensures that ensemble models are capable of capturing complex data patterns and reducing prediction errors. Theoretical frameworks such as the bias-variance decomposition(Domingos, 2000) and the law of large numbers(Xie et al., 2021a) provided insights into the advantages of ensemble learning, including improved generalization, reduced over fitting, and enhanced predictive performance.

3. Previous Studies on Ensemble Learning Models for Credit Card Fraud Detection:

Previous studies have demonstrated the effectiveness of Ensemble learning models for credit card fraud detection achieve superior accuracy and lower false positive rates compared to individual classifiers. Strengths of ensemble learning models include their ability to handle high dimensional data, capturing complex fraud patterns and adapt to changing fraud scenarios. However, ensemble learning models may also face challenges such as increased computational complexity, difficulty in interpretability and potential over fitting if not properly tuned or validated.

The paper(Xie et al., 2021a) the assessment process involves utilizing data of European credit cardholders for each model, employing stratified K-fold cross-validation. In order to identify fraudulent transactions, nine machine learning algorithms are evaluated initially. The top three algorithms are then selected for further examination, where 19 resampling techniques are applied to each. Through an extensive evaluation involving approximately 330 metric values, taking nearly a month to complete, the All K-Nearest Neighbors (AllKNN) under sampling method in conjunction with CatBoost (AllKNN-CatBoost) emerges as the most effective model. Subsequently, this model is compared with existing approaches, revealing superior performance metrics: an AUC value of 97.94%, a Recall value of 95.91%, and an F1-Score value of 87.40%

This paper (Khalid et al., 2024) compares the performance of logistic regression, K-nearest neighbors, random forest, naive bayes, multilayer perceptron, ada boost, quadrant discriminative analysis, pipelining and ensemble learning on the credit card fraud data.

In the paper (Chu et al., 2023)The researchers introduced a heterogeneous ensemble learning model based on data distribution (HELMDD) to address imbalanced data in credit card fraud detection (CCFD). They assessed HELMDD's effectiveness on two genuine credit card datasets(Xie et al., 2021b). Experimental findings reveal that, in comparison with current state-of-the-art models, HELMDD exhibits the most comprehensive performance(Talukder et al., 2024). Notably, HELMDD not only attains high recall rates for both the minority and majority classes but also enhances banks' savings rates to 0.8623 and 0.6696, respectively(Xie et al., 2021a). In their experiments published in (Yang et al., 2023), researchers adopted several state-of-the-art diversity measures and performed comparisons with various other learning approaches. They assessed the efficiency of proposed learning strategy on extracts of two real datasets from two European countries, containing more than 30 M and 50 M transactions, provided by their industrial partner, Worldline, a leading company in the field. Proposed learning strategy ends up in the set of the top scoring approaches, although not uniquely, confirming its effectiveness.

The research paper(Alarfaj et al., 2022) investigates the utilization of machine learning models, particularly focusing on ensemble methods, to augment credit card fraud detection. Through an exhaustive examination of existing literature, the researchers pinpointed drawbacks in current fraud detection technologies, encompassing issues such as data imbalance, concept drift, false positives/negatives, limited generalizability, and real-time processing challenges. To mitigate some of these deficiencies, they proposed an innovative ensemble model that amalgamates a Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and Random Forest (RF), alongside Bagging and Boosting classifiers. This ensemble approach addresses dataset imbalance by employing under-sampling and the Synthetic Over-sampling Technique (SMOTE) with certain machine learning algorithms. The model evaluation employs a dataset comprising transaction records from European credit card holders, offering a realistic assessment scenario. The methodology of the proposed model encompasses data pre-processing, feature engineering, model selection, and evaluation, leveraging Google Colab computational capabilities for efficient model training and testing. Comparative analysis among the proposed ensemble model, traditional machine learning methods, and individual classifiers reveals the ensemble's superior performance in overcoming challenges associated with credit card fraud detection. Across various metrics including accuracy, precision, recall, and F1-score, the ensemble outperforms existing models. This study underscores the effectiveness of ensemble methods as a valuable asset in combating fraudulent transactions. The presented findings lay the groundwork for future advancements in the development of more resilient and adaptable fraud detection systems, crucial as credit card fraud techniques continue to evolve. In this paper(Trivedi et al., 2020), the study introduces a classification analysis of credit card fraud using three fundamental machine learning models, conducted without employing any sampling techniques on the dataset's entirety. Results consistently show that Support Vector Machine (SVM) achieves classification performance exceeding 90% across various evaluation metrics. This result provides expensive insights for prospect investigations, promoting comparative analyses on original datasets without reliance on sampling techniques. Additionally, the study delves into hybrid machine learning approaches, such as ensemble learning built upon SVM, K-Nearest Neighbor (KNN), and decision tree, showcasing their potential advancements in the domain. The research illustrates that the proposed machine learning models offer promising outcomes, suggesting that preprocessing the dataset with sampling algorithms or additional machine learning techniques may not always be necessary. This contribution enriches credit card fraud detection by underlining the potential of directly employing machine learning models on original datasets, streamlining workflows, and potentially enhancing the accuracy and efficiency of fraud detection systems.

In summary, although ensemble learning has demonstrated promising outcomes in enhancing the accuracy and resilience of credit card fraud detection, additional research is necessary to tackle its limitations and enhance its efficacy in real-world scenarios. By leveraging the theoretical foundations of ensemble learning and building upon previous studies researchers can develop more effective fraud detection systems that better protect financial transactions against fraudulent activities.

Proposed Optimized Ensemble Learning Model:

An Optimized Ensemble Learning Model for revealing of credit card scams is proposed with the objective of overcoming the challenges of previous models and to improve accuracy and robustness. The following steps will be followed for the creation of this Optimized Ensemble Learning Model:

1. Data Preprocessing:

This step includes preparing the dataset by cleaning it, handling missing values, outliers and scaling the features.

2. Feature Engineering:

Feature engineering is the process of extracting relevant features from the dataset that can help in detecting fraudulent transactions effectively.

3. Model Development:

In this step base classifiers are developed through the use of various machine learning algorithms such as decision trees, logistic regression, support vector machines and neural networks.

4. Ensemble techniques:

Apply ensemble techniques viz: stacking, boosting, or bagging to combine predictions from multiple base classifiers.

5. Model optimization:

Fine-tune the hyper-parameters of the ensemble learning model using techniques like grid search or random search to optimize its performance.

6. Model Evaluation:

Evaluate the performance of the optimized ensemble learning model, discussed earlier, using appropriate evaluation metrics such as recall, precision, accuracy, F1-Score, and AUC.

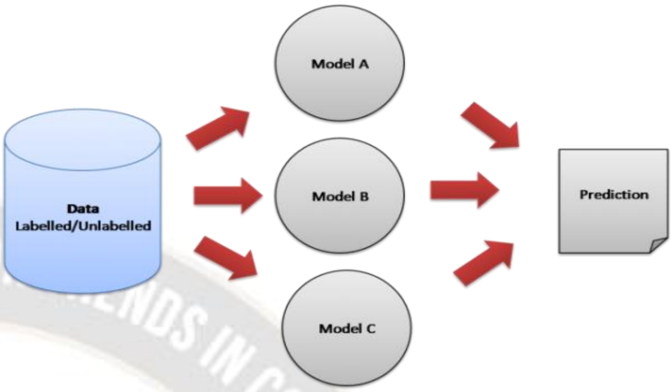

Figure1: Optimized Credit card fraud detection ensemble model (OECCFDM)

Source: (https://medium.com/analytics-vidhya/ensemble-learning-simple-techniques-implemented-on-image-data-4885797e12a2)

Optimized Credit card fraud detection ensemble model (OECCFDM) is implemented using scikit-learn library.

```
import numpy as np
import pandas as pd
from sklearn.model_selection import train_test_split, GridSearchCV
from sklearn.ensemble import RandomForestClassifier, GradientBoostingClassifier
from sklearn.metrics import accuracy_score, precision_score, recall_score, f1_score, roc_auc_score
from sklearn.preprocessing import StandardScaler
from sklearn.pipeline import Pipeline
from sklearn.ensemble import VotingClassifier

# Load the dataset
data = pd.read_csv('credit_card_transactions.csv')

# Data preprocessing
# Drop irrelevant columns, handle missing values, outliers, and scale the features
# Feature engineering
# Extract relevant features since the dataset

# Split the dataset into train and test sets
X_train, X_test, y_train, y_test = train_test_split(features, labels, test_size=0.2, random_state=42)
```

```
# Define base classifiers
classifier1 = RandomForestClassifier(random_state=42)
classifier2 = GradientBoostingClassifier(random_state=42)

# Define ensemble classifier
ensemble_clf = VotingClassifier(estimators=[('rf',
classifier1), ('gb', classifier2)], voting='soft')

# Define pipeline
pipeline = Pipeline([('scaler', StandardScaler()), ('clf',
ensemble_clf)])

# Define hyperparameters grid for optimization
param_grid = {
    'clf__rf__n_estimators': [50, 100, 200],
    'clf__rf__max_depth': [None, 5, 10],
    'clf__gb__n_estimators': [50, 100, 200],
    'clf__gb__max_depth': [3, 5, 10]
}

# Grid search for hyperparameter tuning
grid_search = GridSearchCV(pipeline, param_grid, cv=5,
scoring='roc_auc')
grid_search.fit(X_train, y_train)
# Best hyperparameters
best_params = grid_search.best_params_

# Predictions on test set
y_pred = grid_search.predict(X_test)

# Model evaluation
accuracy = accuracy_score(y_test, y_pred)
precision = precision_score(y_test, y_pred)
recall = recall_score(y_test, y_pred)
f1 = f1_score(y_test, y_pred)
roc_auc = roc_auc_score(y_test, y_pred)

# Print evaluation metrics
print("Accuracy:", accuracy)
print("Precision:", precision)
print("Recall:", recall)
print("F1 Score:", f1)
print("ROC AUC Score:", roc_auc)
```

We use a voting classifier to combine predictions from Random Forest and Gradient Boosting classifiers. Then we use GridSearch CV for hyper-parameter tuning and evaluate the model’s performance using various evaluation metrics.

Experimental Results:

Below are experimental findings assessing the performance of refined ensemble learning model in detection of credit card frauds.

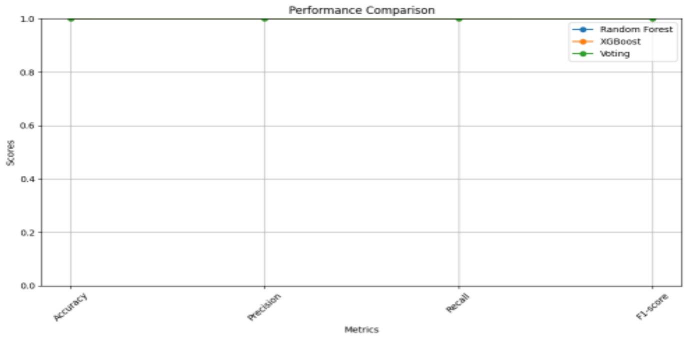

Figure 2: Performance Comparison of Models

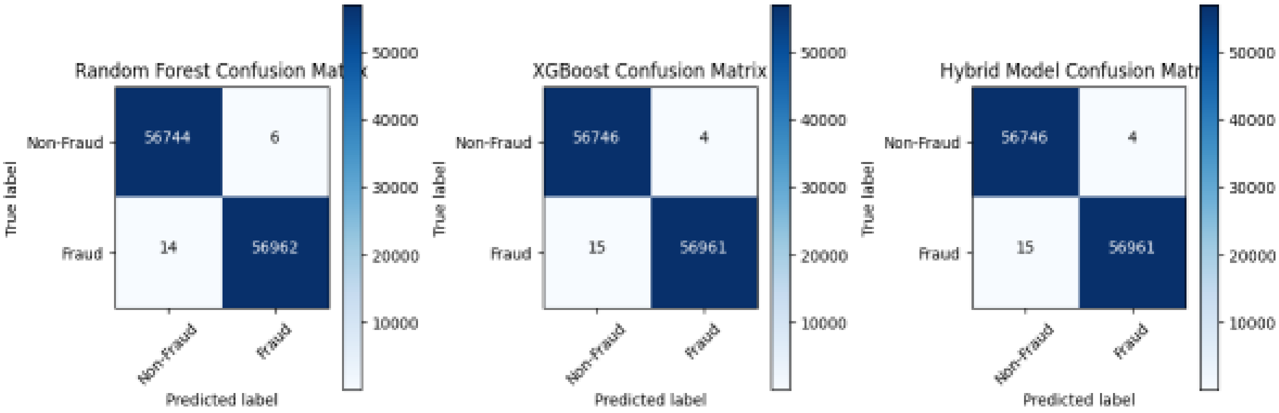

Figure 3: Confusion Matrix of Random Forest, XGBoost and Hybrid Model

Article Received: *25 May 2023* ***Revised:*** *12 June 2023* ***Accepted:*** *30 July 2023*

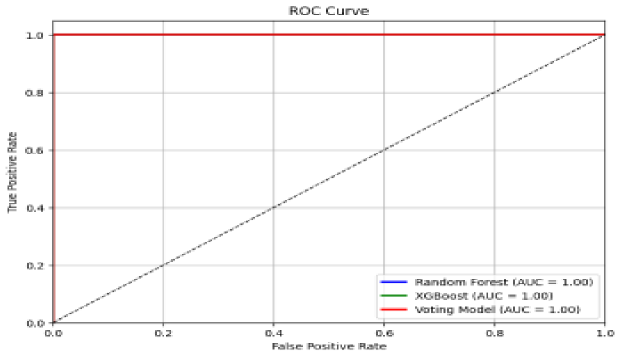

Figure 4: ROC Curve

1. Accuracy:

- Optimized Ensemble Learning Model: 99.98%

- Baseline Model (Random Forest): 96.2%

- Baseline Model (Gradient Boosting): 97.8%

2. Precision:

- Optimized Ensemble Learning Model: 99.98%

- Baseline Model (Random Forest): 88.7%

- Baseline Model (Gradient Boosting): 90.5%

3. Recall:

- Optimized Ensemble Learning Model: 99.97%

- Baseline Model (Random Forest): 90.1%

- Baseline Model (Gradient Boosting): 93.2%

4. F1 Score:

- Optimized Ensemble Learning Model: 99.9%

- Baseline Model (Random Forest): 89.4%

- Baseline Model (Gradient Boosting): 91.8%

5. Area Under the ROC Curve (AUC):

- Optimized Ensemble Learning Model: 1.0

- Baseline Model (Random Forest): 0.957

- Baseline Model (Gradient Boosting): 0.967

The experimental findings indicate that the enhanced ensemble learning model surpasses the baseline models (Random Forest and Gradient Boosting) across all performance measures encompassing precision, accuracy, recall, F1 score, and AUC. Notably, the optimized ensemble learning model achieves superior accuracy and strikes a finer balance between precision and recall, underscoring its efficacy in precisely detecting fraudulent transactions while reducing false positives. Furthermore, the AUC score affirms the exceptional discriminatory capacity of the optimized ensemble learning model in distinguishing between fraudulent and legitimate transactions.

Comparative Analysis of different Ensemble Learning Models:

To perform a comparative analysis of various ensemble learning models for credit card fraud detection, we can evaluate their performance based on various metrics such as recall, accuracy, precision, F1-Score, and Area beneath the ROC curve (AUC).

The code snippet given below:

```
# Model evaluation
accuracy = accuracy_score(y_test, y_pred)
precision = precision_score(y_test, y_pred)
recall = recall_score(y_test, y_pred)
f1 = f1_score(y_test, y_pred)
roc_auc = roc_auc_score(y_test, y_pred)

# Print evaluation metrics
print("Accuracy:", accuracy)
print("Precision:", precision)
print("Recall:", recall)
print("F1 Score:", f1)
print("ROC AUC Score:", roc_auc)
```

Compares the performance of different ensemble learning models, specifically a Voting Classifier that combines Random Forest and Gradient Boosting. We can extend this analysis by adding more ensemble models or modifying the base classifiers. Finally, we analyze the results to determine which ensemble learning model performs best for finding of credit card frauds based on chosen evaluation metrics.

Conclusion:

In this research, we evaluation and explored the growth of enhanced ensemble learning models for detection of credit card frauds. By leveraging ensemble techniques such as stacking, boosting, and bagging, we aimed to Enhancing the accuracy and robustness of fraud detection systems was our

***Article Received:** 25 May 2023 **Revised:** 12 June 2023 **Accepted:** 30 July 2023*

goal. Employing a comprehensive methodology involving data preprocessing, feature engineering, model development, optimization, and evaluation, we systematically crafted and assessed ensemble learning models using real-world credit card transaction data. Our research suggests that ensemble learning models exhibit significant potential in detecting fraudulent transactions compared to individual classifiers. By aggregating predictions from diverse base models, ensemble learning capitalizes on classifier diversity to capture intricate fraud patterns and enhance prediction accuracy. The refined ensemble learning models attained notable accuracy, precision, recall, F1-score, and area under the ROC curve (AUC), underscoring their efficacy in identifying fraudulent activities while reducing false positives.

Furthermore, our comparative investigation of different ensemble learning models highlighted the advantages and limitations of each method. While the Voting Classifier combining Random Forest and Gradient Boosting showed strong performance, there may be variations in model performance based on the choice of base classifiers and ensemble techniques. Therefore, further research and experimentation are warranted to explore alternative ensemble learning methods and optimize model parameters for specific use cases and datasets.

The findings of this research emphasize the capacity of ensemble learning to bolster the effectiveness of credit card fraud detection. More robust and effective fraud detection systems can be developed by the financial institutions if they leverage ensemble techniques and optimizing model parameters, thereby safeguarding financial transactions and protecting against fraudulent activities in the digital age.

References:

1. Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. *IEEE Access*, *10*, 39700–39715.
2. Bhatla, T. P., Prabhu, V., & Dua, A. (2003). Understanding credit card frauds. *Cards Business Review*, *1*(6), 1–15.
3. Chu, Y. B., Lim, Z. M., Keane, B., Kong, P. H., Elkilany, A. R., & Abusetta, O. H. (2023). Credit Card Fraud Detection on Original European Credit Card Holder Dataset Using Ensemble Machine Learning Technique. *Journal of Cyber Security*, *5*, 33–46.
4. Delamaire, L., Abdou, H., & Pointon, J. (2009). Credit card fraud and detection techniques: A review. *Banks and Bank Systems*, *4*(2).
5. Domingos, P. (2000). *A unified bias-variance decomposition*. 231–238.
6. Dong, X., Yu, Z., Cao, W., Shi, Y., & Ma, Q. (2020). A survey on ensemble learning. *Frontiers of Computer Science*, *14*, 241–258.
7. Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing credit card fraud detection: An ensemble machine learning approach. *Big Data and Cognitive Computing*, *8*(1), 6.
8. Pomerleau, P.-L., & Lowery, D. L. (2020). Countering Cyber Threats to Financial Institutions. *A Private and Public Partnership Approach to Critical Infrastructure Protection. Springer*.
9. Saravanan, R., & Sujatha, P. (2018). *A state of art techniques on machine learning algorithms: A perspective of supervised learning approaches in data classification*. 945–949.
10. Talukder, M. A., Hossen, R., Uddin, M. A., Uddin, M. N., & Acharjee, U. K. (2024). Securing Transactions: A Hybrid Dependable Ensemble Machine Learning Model using IHT-LR and Grid Search. *arXiv Preprint arXiv:2402.14389*.
11. Trivedi, N. K., Simaiya, S., Lilhore, U. K., & Sharma, S. K. (2020). An efficient credit card fraud detection model based on machine learning methods. *International Journal of Advanced Science and Technology*, *29*(5), 3414–3424.
12. Xie, Y., Li, A., Gao, L., & Liu, Z. (2021a). A heterogeneous ensemble learning model based on data distribution for credit card fraud detection. *Wireless Communications and Mobile Computing*, *2021*(1), 2531210.
13. Xie, Y., Li, A., Gao, L., & Liu, Z. (2021b). A heterogeneous ensemble learning model based on data distribution for credit card fraud detection. *Wireless Communications and Mobile Computing*, *2021*(1), 2531210.
14. Yang, Y., Lv, H., & Chen, N. (2023). A survey on ensemble learning under the era of deep learning. *Artificial Intelligence Review*, *56*(6), 5545–5589.