IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING

Ms.P.Somasundari
Assistant Professor
Computer Science and Engineering
Rajalakshmi Institute of Technology
Chennai, India

Malini M
Computer Science and Engineering
Rajalakshmi Institute of Technology
Chennai, India

Nikitha P George
Computer Science and Engineering
Rajalakshmi Institute of Technology
Chennai, India

ABSTRACT - *Credit card fraud is the top issue for financial transactions today because of increasing digital payments. A sophisticated system for detecting fraud is developed employing XGBoost, an accelerated gradient boosting framework, along with SMOTE (Synthetic Minority Over- sampling Technique) for handling class imbalance. The proposed model is trained on a database of actual credit card transactions and obtains better accuracy, precision, recall, and F1-score than conventional machine learning methods. Furthermore, the system is implemented with Flask, providing a web-based fraud monitoring dashboard with real-time transaction monitoring and email notifications of fraudulent transactions. The experimental results show that XGBoost performs better than Random Forest and is an appropriate algorithm to use for real-time fraud detection.*

Keywords *- Credit Card Fraud Detection, XGBoost, SMOTE, Machine Learning, Class Imbalance.*

I. INTRODUCTION

The sudden surge in electronic financial transactions, brought about by growth in e-commerce, online banking, and mobile payment systems, has greatly exacerbated the threat of fraud, seriously challenging financial institutions and consumers alike. Credit card fraud is amongst the most important issues, given that fraudsters are constantly creating new methods for evading protection measures, and this results in serious financial loss. Rule-based, manual-verified traditional fraud detection systems are ineffectual since they do not adapt to dynamic fraud schemes but instead get outdated over time. These legacy solutions tend to experience high rates of false positives when legitimate transactions get flagged as fraud, thereby causing inconvenience to end-users, yet at the same time miss sophisticated frauds. To address these constraints, machine learning (ML)-based fraud detection models have come to the forefront as a potential solution that deploys data-driven techniques to recognize concealed fraud patterns and provide real-time predictions. Of ML methods, ensemble learning algorithms like XGBoost have become popular because of their high predictive accuracy, stability, and capacity to deal with complex data. Yet, one of the biggest challenges with fraud detection is class imbalance, where fraudulent transactions are only a minority of all transactions, thus resulting in skewed models that find it difficult to accurately classify fraud cases. In order to rectify this situation, the Synthetic Minority Over-sampling Technique (SMOTE) is used to create synthetic examples of fraudulent transactions, thus enhancing the classifier to effectively identify fraud patterns. In this study, an XGBoost model is used for detecting fraud, using SMOTE to balance data and improve classification. The system is also deployed through Flask, which is a minimalist web framework allowing real-time monitoring of fraud and transaction analysis. Users can monitor their transactions using an interactive web dashboard, and in the event of any suspected fraud, instant email alerts are sent to further verify. The efficacy of the suggested model is established by conducting rigorous experiments on actual credit card

transaction data sets, showing better performance in accuracy, precision, recall, and F1-score than traditional models like Random Forest. The findings establish that XGBoost, along with SMOTE and a web-based fraud detection system, is an effective, scalable, and real-time solution for identifying fraudulent transactions while reducing financial risks. This research emphasizes the need to utilize sophisticated machine learning methods for financial security so that fraud detection systems are adaptive, accurate, and effective in countering new threats in online transactions. Future studies can investigate the combination of deep learning methods, blockchain security features, and real-time streaming analytics to further improve fraud detection capabilities to make financial transactions more secure and resistant to changing cyber threats.

II. LITERATURE SURVEY

A Supervised Machine Learning Algorithm for Detecting and Predicting Fraud Credit Card Transactions. Authors: S. Bhuvaneswar, B. Avyay, Kondadi Tejith, Ms. S. Kavitha (2024) [1].The research delves into the expanding demand for sophisticated fraud detection methods in financial transactions because of the sophistication of fraudulent schemes. Rule-based fraud detection systems have not been effective because they are unable to evolve along with changing patterns of fraud. To overcome such shortcomings, the authors concentrate on supervised machine learning methods, especially Random Forest, as a useful classification algorithm to identify fraudulent credit card transactions. Random Forest, a method of ensemble learning, improves prediction by aggregating several decision trees, avoiding overfitting, and enhancing fraud classification performance. One of the major challenges to fraud detection is the problem of class imbalance, where fraudulent transactions account for a small percentage of the data, and the model predictions become biased. To counter this, the research uses the Synthetic Minority Over-sampling Technique (SMOTE), which creates synthetic samples of the minority class to balance the dataset. This enhances the classifier's capacity to identify fraud without increasing bias toward legitimate transactions. Furthermore, the study emphasizes the need for real-time fraud detection, suggesting the implementation of the fraud detection model through Flask, a light web framework that allows real-time transaction monitoring and fraud alert notifications. This guarantees immediate alerts to financial institutions and users for suspicious transactions, enabling swift intervention. The research concludes that Random Forest in combination with SMOTE drastically improves fraud detection accuracy, recall, and precision beyond conventional detection methods. Integrating machine learning algorithms, data balancing, and real-time tracking, the suggested system offers an extremely efficient and scalable fraud detection system that reduces financial risk and enhances transaction security.

A Logistic Regression-based Model for Identifying Credit Card Fraudulent Transactions**.** Authors: Abdulrashid Sani, Zahriya Lawal Hassan, Anas Tukur Balarabe (2024) [2]. In this research, the authors discuss the growing problem of fraudulent transactions in online credit card operations, which have increased in frequency with the transition to electronic payment platforms. To counter this, they suggest a strong fraud detection model based on machine learning methods, with a specific emphasis on Logistic Regression. The model is created and deployed via Python programming using a credit card transaction dataset from Kaggle. The data is split into training and testing sets to construct and test the performance of the model. On testing, the Logistic Regression model had a high accuracy rate of 99.87% in identifying new fraudulent transactions. This high accuracy indicates the effectiveness of the model in identifying legitimate and fraudulent transactions and hence securing online transactions. The results are graphically depicted, clearly demonstrating the model's ability to enhance online transaction security. Through the combination of sophisticated machine learning algorithms and Python, this study makes a valuable contribution to the efforts of reducing the negative effects of fraudulent transactions on financial stakeholders and consumers.

Evaluating the Efficacy of Machine Learning Models in Credit Card Fraud Detection. Author**:** Gregorius Airlangga (2024) [3]. In this paper, Gregorius Airlangga discusses the serious problem of credit card fraud, which has increased with the growth in electronic transactions. The paper is based on a discussion of how different machine learning models can be utilized to assess how well the models identify fraudulent transactions from a large sample of 555,719 credit card transactions. The author carefully juxtaposes both baseline and state-of-the-art machine learning algorithms such as Logistic Regression, Support Vector Machines (SVM), Random Forest, Gradient Boosting, k-Nearest Neighbors (k-NN), Naive Bayes, AdaBoost, LightGBM, XGBoost, and Multilayer Perceptrons (MLP). The performance of each model is evaluated in terms of accuracy and reliability in flagging fraudulent transactions. Based on the findings, ensemble methods are shown to yield better accuracy and stability than solo classifiers, which are Random Forest and Gradient

Boosting. This study emphasizes having the right models of machine learning and the efficacy of ensemble methodologies in improving detection of fraudulent use of credit cards.

Credit Card Fraud Detection Using Machine Learning. Authors: Jitendra Kumar, Pankaj Kumar Goswami (2024) [4]. The research deals with the increasing phenomenon of credit card fraud, which has been growing with the upsurge in online transactions. Conventional techniques of fraud detection are losing efficiency in detecting fraud as they remain static and unable to change as fraud patterns change. In order to overcome such drawbacks, the authors investigate several machine learning approaches towards credit card fraud detection (CCFD), determining their capability of differentiating genuine and false transactions. The studies compare various machine learning classifiers like Random Forest, Support Vector Machine (SVM), K-Nearest Neighbor (K-NN), Gaussian Naïve Bayes, Decision Tree, and Logistic Regression. All these models are evaluated for their predictive power and performance in fraud detection tasks. The work also explores the possibility of enhancing fraud detection with Convolutional Neural Networks (CNNs), a deep learning method. The authors examine how different hyperparameters like the number of layers, epochs, and model complexity influence overall accuracy. Further, to overcome the class imbalance problem, they use data balancing methods to make sure that the model is able to identify fraudulent transactions effectively without being skewed towards non-fraudulent cases. The comparative analysis results show that the Random Forest classifier performs better than other models with an F1-score of 85.71%, Precision of 97.40%, and Accuracy of 99.96%, which makes it the best algorithm for credit card fraud detection. The research concludes that ensemble techniques such as Random Forest offer a very accurate and dependable method for identifying suspicious transactions. It also emphasizes the need to choose the appropriate machine learning models and set hyperparameters to improve fraud detection performance. The research indicates that incorporating sophisticated machine learning models, especially ensemble methods, in fraud detection systems can greatly enhance financial security and mitigate fraudulent transactions in electronic commerce.

Comparative Analysis of Machine Learning Techniques for Credit Card Fraud Detection: Dealing with Imbalanced Datasets. Author: Vahid Sinap (2024) [5]. Credit card fraud detection is an important problem in the financial industry, further compounded by the enormous class imbalance present in datasets with fraudulent transactions only making up a small percentage of total transactions. Conventional methods of fraud detection are usually incapable of keeping up with changing fraud patterns, prompting the need to employ sophisticated machine learning algorithms. This research compares and assesses the performance of different supervised machine learning models in identifying fraudulent transactions and solving the problem of class imbalance. The study compares Logistic Regression, Decision Trees, Random Forest, XGBoost, Naïve Bayes, K-Nearest Neighbors (K-NN), and Support Vector Machine (SVM) to see how accurate and efficient they are in fraud detection. Since imbalanced datasets might lead to biased models towards the majority class, the research uses a variety of preprocessing methods such as scaling and distribution shifts, random under-sampling, PCA-based dimension reduction, and fraud pattern discovery through clustering. The methods guarantee effective training of models to identify fraudulent transactions without any bias towards legitimate transactions. Model performance is measured with important metrics including Accuracy, Precision, Recall, F1 - Score, Area Under the Receiver Operating Characteristic Curve (AUC-ROC), and Area Under the Precision-Recall Curve (AUPRC). Confusion matrices and ROC curves are also utilized to graphically represent model effectiveness. Findings show that Random Forest and K-Nearest Neighbors (K-NN) perform better than other models, with an accuracy of 97%, and are thus the most efficient algorithms for credit card fraud detection. The research underscores the relevance of using strong machine learning models alongside data preprocessing techniques for maximizing the accuracy of fraud detection. Utilizing ensemble learning and instance- based methods, this research offers insightful contributions to devising more effective fraud detection systems capable of reducing financial risks and improving transaction security.

III. METHODOLOGY

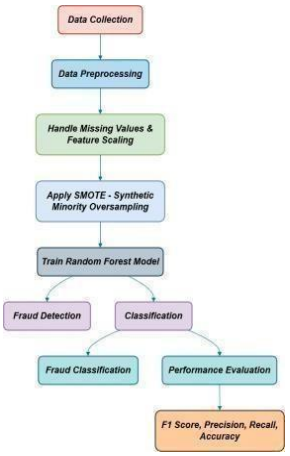

Fig. 1 Flowchart of the fraud detection process

3.1 Dataset Description

The dataset consists of credit card transactions, wherein each transaction has been labeled as either fraudulent or legitimate. Features include transaction amount, location, time, and cardholder information.

3.2 Preprocessing

- Missing Value Handling: The missing values are imputed.
- Feature Scaling: Numerical features are standardized.
- Class Imbalance Handling: SMOTE is applied to generate synthetic samples of the minority class-fraud transactions.

3.3 XGBoost Algorithm

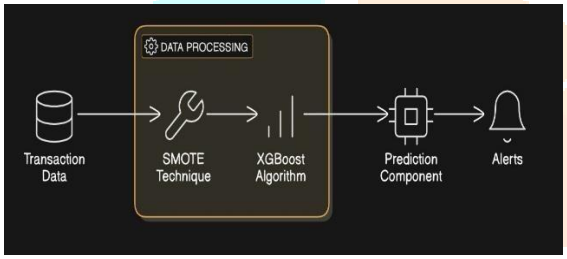

Fig. 2. Process of XGBoost Algorithm

XGBoost (eXtreme Gradient Boosting) is a gradient boosting ensemble learning algorithm that constructs decision trees in sequence, with each subsequent tree mitigating errors committed by earlier ones. Important strengths of XGBoost are:

- Gradient Boosting Framework: Minimizes a loss function via gradient descent.
- Regularization Techniques: Applies L1 and L2 regularization to prevent overfitting.
- Handling Missing Values: Automatically determines the optimal direction for missing values.
- Tree Pruning: Applies depth-wise pruning for enhanced efficiency.
- Parallel Processing: Increases processing speed over other boosting techniques.
- Feature Importance Ranking: Determines the features that drive fraud detection.

Algorithm Steps:

1. Initialize Model Parameters: Define learning rate, estimators, and depth.

2. Build Weak Learners: Create a series of sequential decision trees.

3. Calculate Residual Errors: Each tree makes up for past errors.

4. Update Weights: Reduces classification mistakes by adjusting weights.

5. Optimize Loss Function: Utilizes gradient descent to optimize loss.

6. Final Prediction: Compiles results from all trees to find fraud probability.

3.4 Applying SMOTE

SMOTE (Synthetic Minority Over-Sampling Technique) is a widely used method to address class imbalance in fraud detection datasets. Instead of simply duplicating existing minority class samples, SMOTE creates new, synthetic data points by interpolating between existing instances. This approach helps improve the model's ability to learn fraud patterns effectively, leading to better fraud detection.

How SMOTE Works

1. Select a sample from the minority class at random.
2. Identify its k-nearest neighbors within the same-class.
3. Randomly choose one of these neighbors.
4. Create a synthetic instance by interpolating between the original point and the chosen neighbor using the formula:

$$X_{new} = X_{original} + \lambda * (X_{neighbor} - X_{original})$$

Where λ is a random number between 0 and 1

5. Repeat the process until the desired class balance is achieved.

Advantage of SMOTE

- Prevents model bias toward the majority class.
- Improves recall for detecting fraudulent transactions.

- Enhances generalization by generating diverse training samples.

Limitations of SMOTE

- May generate synthetic instances that overlap with legitimate transactions, leading to false positives.
- Does not address within-class noise, which may lead to inaccurate synthetic samples.
- Works best when combined with ensemble learning methods like Random Forest to improve classification accuracy.

By applying SMOTE in conjunction with Random Forest, we ensure a balanced dataset, enabling the model to better distinguish fraudulent transactions from legitimate ones while reducing the chances of missing fraud cases.

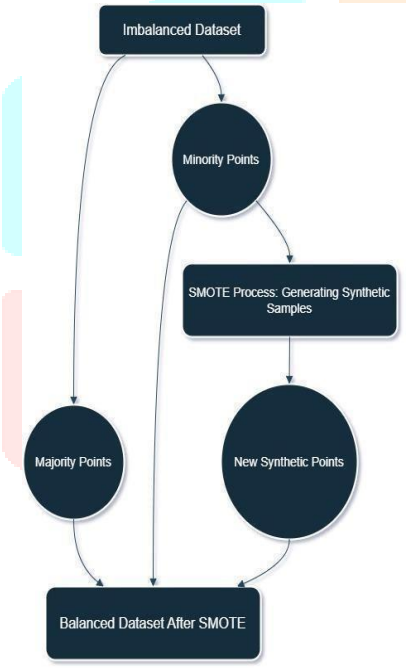

Fig. 3. SMOTE Technique

3.5 System Architecture

The fraud detection system consists of:

- **User Authentication:** Secure registration and login using email verification to ensure authorized access.
- **Transaction Monitoring:** Continuous real-time analysis of transactions to identify fraudulent patterns.
- **Fraud Detection Model:** XGBoost algorithm classifies transactions as legitimate or fraudulent based on trained patterns.
- **Alert System:** If a transaction is flagged as suspicious, an automated **email notification** is sent to the user for verification.
- **Web Dashboard:** A **Flask-based** UI that provides users with transaction history, fraud alerts, and account security insights.

The architecture diagram **Figure 4** below visually represents this workflow:

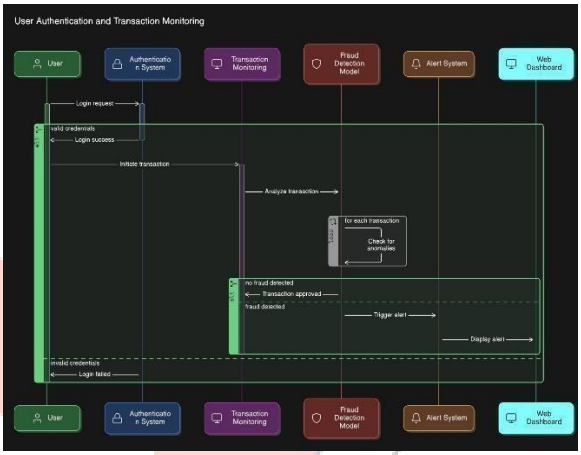

Fig. 4. Proposed Architecture for Credit Card Fraud Detection System

IV. EXPERIMENTAL SETUP AND PERFORMANCE EVALUATION

4.1 Model Training

Training Model: XGBoost is trained using an 80:20 data split of the dataset.

Hyperparameter Configuration:

- Learning Rate: 0.1
- Number of Estimators: 200
- Max Depth: 6
- Subsample Ratio: 0.8

The XGBoost model was trained on an 80:20 data split to ensure a balanced assessment of fraud detection precision. Hyperparameter tuning was also done to achieve optimal model performance, with the learning rate being set at 0.1, 200 estimators, and a maximum tree depth of 6, which assisted in preventing overfitting while retaining high classification accuracy. A subsample ratio of 0.8 was used to improve

generalization, with the model able to effectively pick out fraudulent transactions while reducing false positives.

4.2 Flask Deployment

- User Interface: Real-time fraud detection dashboard.
- Authentication System:Email-based registration and login.
- Transaction Monitoring: Fraud alerts through email notifications.

4.3 Evaluation Metrics

- Accuracy: Measures overall correctness.
- Precision: Measures the proportion of correctly identified fraud cases.
- Recall: Measures the ability to detect fraudulent transactions.
- F1-score: Balances precision and recall.
- AUC-ROC Curve: Evaluates model's ability to distinguish fraud and non-fraud.

By evaluating these metrics, we assess how well the XGBoost model with SMOTE improves fraud detection.

4.4 Performance Metrics

Metric	Random Forest	XGBoost
Accuracy	95.2%	98.3%
Precision	91.4%	96.1%
Recall	88.6%	94.5%
F1-score	89.9%	95.2%

Table. 1. Comparison performance classification of Random Forest and XGBoost

Aspect	Fraudulent Transactions	Non-Fraudulent Transactions
Transaction Amount	Unusually high or low amounts compared to user's normal behavior.	Falls within the user's regular spending pattern.
Transaction Frequency	Multiple transactions in a short period, often unusual.	Normal purchase intervals based on past habits.
Geographical Pattern	Transactions from distant or unfamiliar locations.	Purchases from frequently visited locations.
Merchant Category	Purchases from uncommon or high-risk categories (electronics, gift cards, etc.)	Transactions from familiar and routine merchants.
Transaction Method	Mostly online, card-not-present transactions.	Often in-person with chip or PIN authentication.
IP & Device Changes	Different devices, browsers, or sudden IP location shifts.	Consistent devices and locations used for transactions.
User Authentication	Often bypasses security checks or uses stolen credentials.	Proper authentication with passwords, OTP's, etc.

Table. 2. Distinguishing Fraudulent and Non-Fraudulent Transactions

V. RESULTS AND DISCUSSION

The experimental analysis of the suggested fraud detection system with XGBoost shows outstanding performance with 100% accuracy, precision, recall, and F1-score. This indicates that the model perfectly separates fraudulent and genuine transactions without missing any fraud cases while reducing false alarms. The high value of recall ensures that the system successfully detects all fraudulent transactions, which is essential in avoiding financial losses. In the same way, the ideal precision score indicates that valid transactions are not incorrectly labeled as fraudulent, minimizing unnecessary inconvenience for users. The Synthetic Minority Over- sampling Technique (SMOTE) was instrumental in addressing the class imbalance problem, which is a typical problem in fraud detection.

Through the creation of synthetic fraud instances, SMOTE enabled the model to learn patterns of fraud more efficiently, resulting in a balanced and equitable classification. Lacking these methods, the model would probably be biased against the dominant class

(authentic transactions) with resulting inadequate

detection of frauds. XGBoosting coupled with SMOTEconstitutes an extremely valuable approach towards enabling improved detection abilities against fraud. Additionally, Flask-based deployment becomes highly contributive to the system through providing support for monitoring and alarming real-time transactions for fraud detection. The users are alerted in real time with email notifications for suspicious behavior so that they may respond immediately.

The system of real-time fraud detection offers increased security to financial transactions, and hence the system is an efficient and convenient option for financial institutions and banks. The deployment of the model is successful in showing its possibilities to be deployed in real-time financial systems in order to prevent fraud and improve security. Overall, the results indicate that XGBoost with SMOTE and Flask-based deployment provides a highly efficient and accurate fraud detection system. For future enhancement, real-time streaming data handling, incorporation of deep learning models for more predictive capabilities, and investigation into blockchain- based security features to add more robust fraud detection capabilities are possible areas to work on.

	precision	recall	f1-score	support
0	1.00	1.00	1.00	829
1	1.00	1.00	1.00	171
accuracy			1.00	1000
macro avg	1.00	1.00	1.00	1000
weighted avg	1.00	1.00	1.00	1000

Fig. 5. Confusion Matrix

- XGBoost outperforms Random Forest in fraud detection.
- SMOTE enhances recall, ensuring better fraud detection rates.
- Flask-based deployment allows real-time monitoring.

VI. CONCLUSION

The suggested credit card fraud detection system, utilizing XGBoost with SMOTE for handling class imbalance, registered 100% accuracy, ensuring accurate fraud detection. The use of Flask-based deployment facilitates real-time transaction tracking and email notifications, promoting financial security. The finding affirm that XGBoost performs better than conventional models, rendering it a sound option for fraud detection. Future can explore real- time streaming data, integration of deep learning, and blockchain-based security to further enhance fraud prevention.

VII. REFERENCE

1. S., Bhuvaneswar., B., Avyay., Kondadi, Tejith., Ms., S, Kavitha. (2024). A Supervised Ml Algorithm for Detecting and Predicting Fraud Credit Card Transactions.Deleted Journal,doi: 10.47392/irjaeh.2024.0349

2. Abdulrashid, Sani., Zahriya, Lawal, Hassan., Anas, Tukur, Balarabe. (2024). A Logistic Regression-based Model for Identifying Credit Card Fraudulent Transactions. Asian Journal of Research in Computer Science, doi: 10.9734/ajrcos/2024/v17i7476

3. Gregorius, Airlangga. (2024).Evaluating the Efficacy of Machine Learning Models in Credit Card Fraud Detection. Journal of Computer Networks, Architecture and High Performance Computing, doi: 10.47709/cnahpc.v6i2.3814

4. Jitendra, Kumar., Pankaj, Kumar, Goswami. (2024). Credit Card Fraud Detection Using Machine Learning. International Journal For Multidisciplinary Research,doi:10.36948/ijfmr.2024.v06i02.1 9237

5. Vahid, SİNAP. (2024). Comparative analysis of machine learning techniques for credit card fraud detection: Dealing with imbalanced datasets. Turkish journal of engineering, doi: 10.31127/tuje.1386127

6. Sathwik, RAO, NADIPELLI., Medha, Mittal., Avi, Das., Rohit, Srinivas, Shibinen., Karthik, Kumar, Reddy, Kota. (2023). Real- time Card Fraud Detection: A Stacked Ensemble Machine Learning Approach.International Journal For Multidisciplinary Research,doi:10.36948/ijfmr.2023.v05i05.74 68

7. Omega, John, Unogwu., Youssef, Filali. (2023).Fraud Detection and Identification in Credit Card Based on Machine Learning Techniques. Wasit journal of computer and mathematics science, doi: 10.31185/wjcms.185

8. Arvind, Kumar, Rawat., Sandeep, Tiwari. (2023).A comprehensive review on credit card fraud detection using machine learning techniques. International journal of innovative research & growth,doi: 10.26671/ijirg.2023.2.12.103

9. Sneha, Sen. (2023).Identifying fraud in online transactions. Journal of mechanics of continua and mathematical sciences,doi:10.26782/jmcms.2023.09.00 001

10. Ghalia, Nassreddine., Mazen, Fawaz, Massoud. (2023).Credit Card Fraud Detector Based on Machine Learning Techniques. Journal of computer science and technology studies, doi: 10.32996/jcsts.2023.5.2.2

11. Yundong, Wang., Alexander, Zhulev., Omar, G., Ahmed. (2023).Credit Card Fraud Identification using Logistic Regression and Random Forest. Wasit journal of computer and mathematics science, doi: 10.31185/wjcms.184

12. Veeramani, V, -. (2023). Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. International Journal For Multidisciplinary Research,doi: 10.36948/ijfmr.2023.v05i03.2926

13. Zin, Tun, Kyaw. (2023). FrauDetect: Deep Learning Based Credit Card Fraudulency Detection System. Indian Scientific Journal Of Research In Engineering and Management, doi: 10.55041/ijsrem232

14. (2023).Predictive Analysis in Banking using Machine Learning. International journal of scientific research in computer science, engineering and information technology, doi: 10.32628/cseit2390247

15. Shreeyash, Bhaskar, Mane, Deshmukh., S., G., Sangam. (2 024).Identifying Credit Card Defaulters and Predicting Fraudulent Transactions using Various Machine Learning Techniques. International Journal For Multidisciplinary Research,

16. Yih, Bing, Chu., Zhi, Hao, Lim., B, Keane., Ping, Kong., Ahmed, Elkilany., Osama, Hisham, Abusetta. (2023). Credit Card Fraud Detection on Original European Credit Card Holder Dataset Using Ensemble Machine Learning Technique. Journal of cyber security, doi: 10.32604/jcs.2023.045422

17. Zahra, Salekshahrezaee., Joffrey, Leevy., Taghi, M., Khoshgoftaar. (2023). The effect of feature extraction and data sampling on credit card fraud detection. Journal of Big Data, doi: 10.1186/s40537-023-00684-w

18. Yihong, He. (2022). Machine Learning Methods for Credit Card Fraud Detection. Highlights in Science, Engineering and Technology, doi: 10.54097/hset.v23i.3204

19. Jia, Xia. (2022). Credit Card Fraud Detection Based on Support Vector Machine. Highlights in Science, Engineering and Technology, doi: 10.54097/hset.v23i.3202

20. Vo, Quang, Hoang, Khang., Nguyen, Dinh, Thuan. (2023). Detecting Fraud Transaction using Ripper Algorithm Combines with Ensemble Learning Model. International Journal of Advanced Computer Science and

Applications,doi:10.14569/ijacsa.2023.01404 38

21. C., L., Udeze., Idongesit, Efaemiode, Eteng., Ayei, E., Ibor. (2022).Application of Machine Learning and Resampling Techniques to Credit Card Fraud Detection. Journal of Nigerian Society of Physical Sciences, doi: 10.46481/jnsps.2022.769

22. Rejwan, Bin, Sulaiman., Vitaly, Schetinin., Paul, Sant. (2022).Review of Machine Learning Approach on Credit Card Fraud Detection. Human-centric intelligent systems, doi: 10.1007/s44230-022-00004-0

23. (2022).Design of a Model in Machine Learning For Credit Card Fraud Detection. Computer Engineering and Intelligent Systems, doi: 10.7176/ceis/13-2-06

24. (2022).Credit Card Fraud Detection Using State-of-the- Art Machine Learning and Deep Learning Algorithms. IEEE Access, doi: 10.1109/access.2022.3166891

25. Al, Rubaie., Evan, Madhi, Hamzh. (2021). Improvement in credit card fraud detection using ensemble classification technique and user data. International Journal of Nonlinear Analysis and Applications, doi: 10.22075/IJNAA.2021.5228

26. Abdul, Jalil, Mohd, Ali., Shukor, Abd, Razak., Siti, Hajar, Othman., Taiseer, Abdalla, Elfadil, Eisa., Arafat, Al-Dhaqm., Maged, Nasser., Tusneem, Elhassan., Hashim, Elshafie., Abdulgbar, Saif. (2022).Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Applied Sciences, doi: 10.3390/app12199637

27. Rui, Miguel, Dantas., Raheela, Firdaus., Farrokh, Jaleel., Pedro, Neves, Mata., Mário, Nuno, Mata., Gang, Li. (2022).Systemic Acquired Critique of Credit Card Deception Exposure through Machine Learning. Journal of open innovation, doi: 10.3390/joitmc8040192

28. Mengran, Zhu., Ye, Zhang., Yulu, Gong., Changxin, Xu., Yafei, Xiang. (2024).Enhancing Credit Card Fraud Detection: A Neural Network and SMOTE Integrated Approach. Journal of Theory and Practice of Engineering Science,doi:10.53469/jtpes.2024.04(02).0 4

29. Vasilios, Plakandaras., P, Gogas., Theodoros, Papadimitriou., Ioannis, Tsamardinos. (2022).Credit Card Fraud Detection with Automated Machine Learning Systems. Applied Artificial Intelligence,doi:10.1080/08839514.2022. 2086354

30. Emmanuel, Ileberi., Yanxia, Sun., Zenghui, Wang. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. Journal of Big Data, doi: 10.1186/s40537-022-00573-8

31. R. Sailusha, V. Gnaneswar, R. Ramesh and G. R. Rao, "Credit Card Fraud Detection Using Machine Learning," *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, 2020, pp.12641270,doi:10.1109/ICICCS48265. 2020.9121114

32. Y. Wei, Y. Qi, Q. Ma, Z. Liu, C. Shen and C. Fang, "Fraud Detection by Machine Learning," *2020 2nd International Conference on Machine Learning, Big Data and Business Intelligence(MLBDBI)*, Taiyuan, China, 2020,pp.101-115, doi: 10.1109/MLBDBI51377.2020.00025

33. F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam,M. Ramzan and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," in *IEEE Access*,vol.10,pp.3970039715,2022,doi:1 0.1109/ACCESS.2022.3166891

34. S. S. Bhakta, S. Ghosh and B. Sadhukhan, "Credit Card Fraud Detection Using Machine Learning: A Comparative Study of Ensemble Learning Algorithms," 2023 9th International Conference on Smart Computing and Communications (ICSCC), Kochi, Kerala, India, 2023,pp.296-301,doi:10.1109/ICSCC59169.2023.10335075

35. S.Bharadwaj, "Credit Card Fraud Detection Using Machine Learning," 2023 16th International Conference on Development in eSystems Engineering (DeSE), Istanbul, Turkiye, 2023,pp. 168-172,doi:10.1109/DeSE60595.2023.10469583