AL-AASAR Journal
Quarterly *Research Journal*
www.al-aasar.com

Vol. 2, No. 3 (2025)
Online ISSN: 3006-693X

Print ISSN:3006-6921

DETECTION OF CREDIT CARD FRAUD USING MACHINE LEARNING MODELS

Hamza Iqbal[1], Abu Bakar Iqbal[2], Saleem Mustafa[3]
[1,2,3] Faculty of Computer Science and Information Technology, Superior University, Lahore 540000, Pakistan

Abstract:
Nowadays, credit card fraud has increased because of all the traditional payment modes being converted into online payment modes. Individuals and financial organizations face heavy losses every year due to fraud. The customer is very scared because of the scam. Frauds and heavy losses destroy the business of financial institutions; hence, researchers give an overview of who detects fraudulent activities. The second researcher used machine learning algorithms for scam detection. This research focuses on machine-learning algorithms that detect scams and scammers. It reveals that a machine learning approach can predict whether the transaction is a scam. In this research, the machine learning algorithms were applied using the European dataset gathered from Kaggle. The imbalance is because there are many genuine and very few fraudulent transactions. These algorithms are also used to identify genuine and fraudulent transactions. All models have the same accuracy of 99%. However, compared to the other models, a random forest has better recall, precision, and an F1 score in its evaluation metrics. Therefore, a random forest comparatively shows better results than logistic regression and a decision tree.

Keywords: *Credit Card, Detecting fraud, Machine Learning, Transactions, Banking System.*

1. Introduction:

Digital transactions have increased in the modern world due to the rise of internet commerce, mobile banking, and payment systems. E-commerce trading of goods and services via the electronic Internet or other computer networks, and transferring payment and data [1]. Generally, cards are assigned to customers and cardholders as an advance in purchasing goods and services within a limit or withdrawing cash [2]. It gives the cardholder the time advantage to repay, making it its primary purpose. Banking and other financial institutions continuously issue credit cards to their credit-worthy customers to expand their business [3].

They have several benefits [4]. However, credit card holders face problems like cards left, cards misplaced, and online transactions performed without the card and the cardholder's knowledge [5]. The fraudsters make unethical transactions [6] and sometimes other illegal transactions without the knowledge of cardholders. This leads to heavy financial losses for the cardholder. The customer's information can be stolen without knowledge if a cardholder gives their card to a merchant to complete their purchase [7]. The credit card transaction process involves cardholders and merchants, acquiring banks' credit card networks, and issuing banks. The security system[8] protects sensitive credit card information during transactions. Figure 1 displays the range of credit card scams .

AL-AASAR Journal
Quarterly *Research Journal*
www.al-aasar.com
Vol. 2, No. 3 (2025)
Online ISSN: 3006-693X
Print ISSN:3006-6921

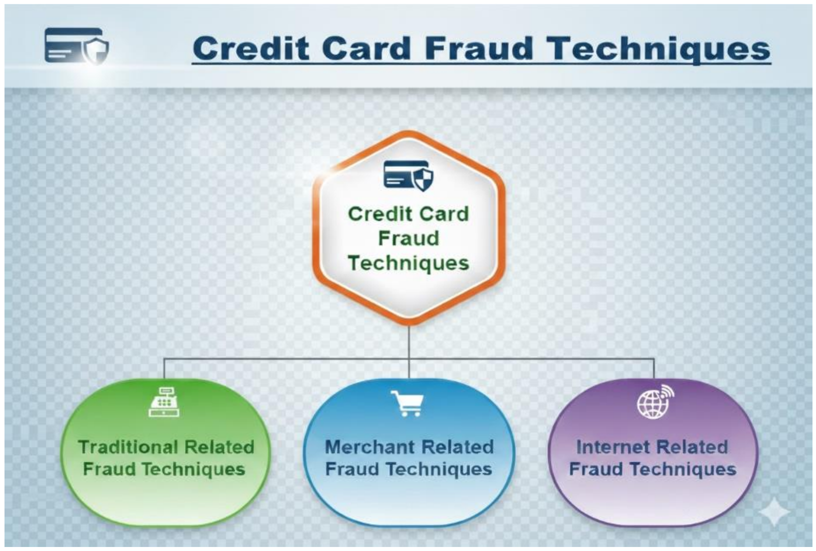

Figure 1. Credit card fraud techniques

Figure 1 shows that fraudsters use these techniques to commit illegal activity or credit card fraud when customers perform transactions. Credit card fraud is alarming worldwide because every country faces this problem. Figure 2 shows a statistical report of countries that face credit card fraud.

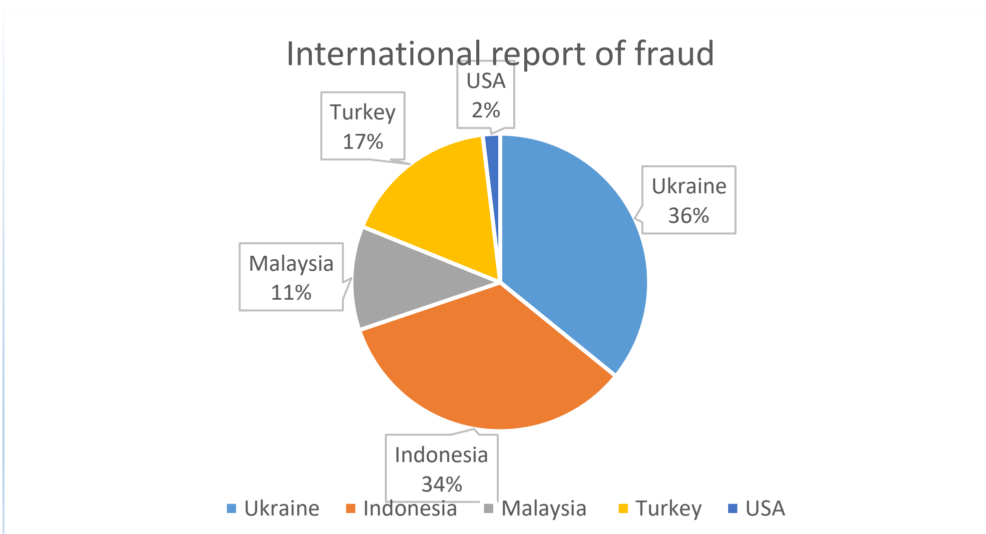

Figure 2. International report of fraud

Figure 2 displays that traditional fraud detection techniques, such as rule-based systems [9] and manual monitoring, cannot support high-scale fraud schemes. Institutions and payment service providers have started to use advanced technologies [10] to upgrade their fraud detection, such as machine learning (ML)[11]. Machine learning is a fantastic invention of the current century that can work with large datasets, which people cannot instantly access and replace traditional methods. The financial institutes focused on new methodologies [12] to handle the techniques of credit

AL-AASAR Journal
Quarterly *Research Journal*
www.al-aasar.com

Vol. 2, No. 3 (2025)
Online ISSN: 3006-693X
Print ISSN:3006-6921

cards. It has great potential for detecting credit card fraud. Machine learning is learnable [13]. It learns from previous data and consumer transactions, which allows for implementing machine learning algorithms on the dataset to detect fraud. This will be very beneficial in detecting credit card fraud [14]. Credit card fraud detection is based on an analysis of a card's spending behavior by the customer [15]. One needs to be aware of the technologies [16] involved in detecting credit card fraud and identifying different types of fraud. Machine learning techniques are dependent on the availability of large datasets and high-quality data sets. In detecting credit card fraud, machine learning algorithms are giving better results. The various techniques in use for credit card fraud detection [17]. Supervised learning methods and unsupervised learning methods used in fraud detection. The algorithms in supervised learning try to learn with the labeled data, but the data should be pre-defined and pre-labeled [18]. In the unsupervised learning method, the data is not predefined, and neither is it pre-labeled. It is usually represented in a clustered format. The algorithms try to learn by themselves and understand the data. These techniques can detect fraudulent transactions from labeled data . However, the major problem faced by the researchers is the large, unbalanced data set [19]. Machine learning gives better results on the majority data, not minority data [20]. The imbalanced data set has few entries of fraud. The data analysts understand the data set and build a model to detect credit card fraud [21]. Machine learning techniques solve the imbalance data set problem. The machine learning approaches provided the best solution and implementation for the financial institute's credit card fraud detection structure. It is beneficial in perceiving and averting credit card fraud [22]. The steps of fraud detection are presented in Figure 3.

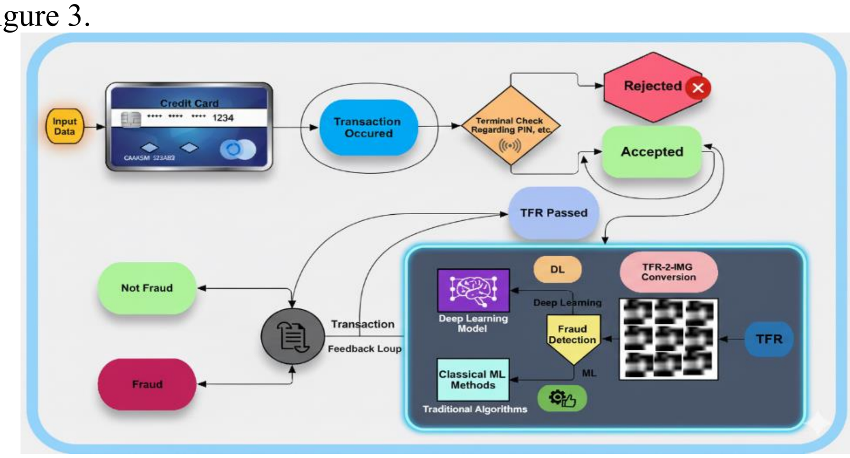

Figure 3. Flowchart for Proposed Framework

Figure 3 shows all the steps for transactions performed by the customer. The figure shows the basic steps of credit card fraud detection. Firstly, a customer presents the card for a transaction, and the terminal checks the credit card's validity. The intelligent fraud detection system is performed on the customer transaction record. However, the public dataset is highly imbalanced. The different techniques used in discourse the session discrepancy. This balance data set is utilised to detect credit card fraud. The machine learning approaches apply to the balanced dataset for better results.

2. Related Work:
It's a critical area that attracts attention in both the practical and research industries [23]. Financial institutions issue credit cards to their customers. But now, credit card fraud has increased due to online transactions. Due to fraudulent activities, individuals and financial institutions face heavy losses. The fraudsters introduce new strategies for making frauds. So, it is an area of interest for researchers and motivating researchers to discover a solution to credit card fraud [24]. The researchers use different methods to detect credit card fraud. The researchers use different techniques to handle large and imbalanced data sets[25]. The authors applied three main techniques: machine learning computations, algorithms with supervision, and unsupervised training techniques to identify fraudulent transactions. Many machine-learning methods are already used for credit card fraud detection. Thus, the foundations for performance are accuracy, sensitivity, specificity, and precision[26]. The SVM classifier has an accuracy of 97.5%, Random Forest 98.6%, Decision Trees 95.5% and Logistic Regression 97.7%. The findings indicate that random forest performs better than the other algorithms concerning fraud detection in credit. Moreover, they concluded that the decision tree methods do not work any better in identifying the scam. There is a problem related to insufficient data [27]. The accuracy of LR was 99%, SVM was 99%, RF was 99%, and ANN was 99%. The recall of LR was 83%, for SVM was 89.5%, for RF was 55.3%, and for ANN was 65%. The precision value of LR was 59%, SVM was 74.7%, RF was 77%, and ANN was 78%. The F1 score value of LR was 69%, for SVM was 81.5 %, for RF was 64.3%, and for ANN was 71.4%. Typically, the results make the SVM algorithm the best in fraud detection as it gives quality results [28]. The accuracy achieved by Random Forest was 95.5%; by Decision Trees, it was 94.3%; and by Logistic Regression, it was 90.05%. Hence, the most accurate result was derived using random forest, with a high accuracy of 95.5% [29]. These results are obtained by AUC, F1 score, accuracy, and precision. The accuracy rate of the decision tree was 99.9%. Logistic Regression models achieved an accuracy of 99.8%, and the SVM model achieved a model accuracy of 99.7%. Due to better performance, the decision tree model could classify fraud in the unbalanced dataset [30]. The methodologies produce 99.7% of RF and 94.4% week results of SVM. The random forest is the most accurate and productive method among these machine-learning techniques. However, the KNN had the lowest accuracy rating among all the models [31]. Their machine-learning methods had an accuracy of 99.95% [32]. Iqra et al. [33] used the SMOTE approach to address data imbalance. Different machine learning techniques exist that are used in fraud detection applications. For random forest, impression recall scored 84% in the results. Varmedja et al. [34] worked on the models NB, logistic regression, and RF. The performance was compared using four assessment models, comparing the confusion matrix. The research also examined why random forests performed better than others in accuracy. Muhammad et al. [35], show a comparison, and the LR is preferable to others. Jia et al. [36] The AUC for the SVM model was 0.90. Tesfahun et al. [37], in the work, the researchers used a model of CNN-SVM to identify credit card fraud. Their findings were that the accuracy of CNN-SVM was 91.80%.

Table 1. Summary of recent Studies for Credit card fraud detection

Ref.	Authors	Dataset	Method	Results
25	Navanushu et al.	European Dataset	SVM, DT, RF, LR	RF, accuracy 98%
26	Omar et al.	European Dataset	ANN, SVM, LR, DT	Accuracy 99%
27	Lakshmi et al.	European Dataset	LR, RF, DT	Accuracy 95.5%
28	Minjun et al.	European Dataset	SVM, DT, RF	DT accuracy 99.9%
29	Hazeel et al.	European Dataset	NB, KNN, RF, LR	RF accuracy 99.7%
30	Omega et al.	European Dataset	NB, RF	Accuracy 99.7%
31	Iqra et al.	Dataset source from Kaggle	SVM, ANN, RF, LR	Recall score 84%
32	Varmedja et al.	Credit card fraud detection dataset	NB, RF, LR	LR achieved the best results

The increasing sophistication of financial fraud necessitates advanced detection methodologies[38], moving beyond traditional rule-based systems. Recent literature highlights the application of advanced machine learning and AI paradigms for enhanced security[39]. For instance, Hassan et al[40] explore the foundational and functional aspects of AI and machine learning, emphasizing their role in advancing computer science and reducing data dependency through self-supervised learning. This is particularly relevant for handling vast, imbalanced datasets that are standard in fraud detection. Furthermore, the need for transparent and scalable solutions is addressed by Khan (2024)[41], who focuses on explainable AI (XAI) for intrusion detection systems (IDS). This is a crucial aspect, as understanding the “why" behind a model's prediction is essential for financial institutions to comply with regulations and build trust. Building on this, Akter (2024)[42] introduces the concept of quantum-inspired machine learning for zero-trust cybersecurity, and Ferdous (2024)[43] explores energy-aware AI approaches for next-generation IDSs. These studies collectively underscore the paradigm shift towards more intelligent, transparent, and resource-efficient security frameworks, which directly informs the approach taken in this research to apply machine learning algorithms like Random Forest for robust credit card fraud detection.

3. Contribution:

In this research, we are contributing to detecting credit card fraud. We used a machine learning approach to enhance the ability to detect fraud. The study shows that the models monitor real-time transactions and identify fraudulent transactions. The results of the model are highly reliable and accurate. The models must detect the fraudulent transaction quickly and take corrective action.

AL-AASAR Journal
Quarterly *Research Journal*
www.al-aasar.com

Vol. 2, No. 3 (2025)
Online ISSN: 3006-693X
Print ISSN:3006-6921

4. Methodology:

This is the part where experiments on the dataset are carried out. The dataset undergoes several machine learning algorithms for better results. Algorithms of machine learning are called as. Experimenting: A measure is included in the confusion matrix to quantify its evaluation, such as a performance comparison of the algorithms. The different processes involved in the studies of classifier processing are based on data gathering, pre-processing, analysis, training, and testing of algorithms. During this first phase of data collection, the dataset's quality should be up to the standards and knowledge base available, and it also needs to be readily available. The next step in this process is preparing the data, which is when the information transforms into format, fit, and usable information. The feature selection and reduction for that analysis stage have already been done thanks to PCA. Training is the first phase in the machine learning process. The trained algorithms identify the patterns and give their predictions. The dataset must be divided into 80% training and 20% testing data. In the next phase, the performance of the model will be assessed. The testing data set will form the basis of the assessment. Also, the training and testing datasets should not be identical; otherwise, the results would not be valid. Figure 4 illustrates subsequent processing stages.

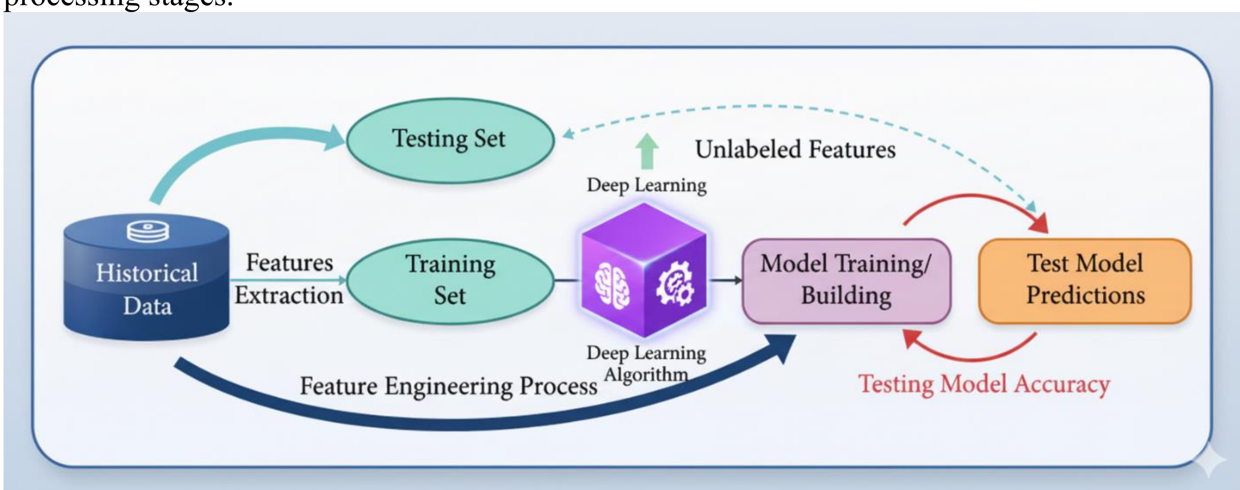

Figure 4**:** Machine learning workflow

4.1 Dataset:

This experiment was completed on an open dataset. The dataset was from a machine learning group in ULB. The source of the dataset is Kaggle. There are 284,807 credit card transaction records in this dataset of European cardholders in September 2013. The total time needed to perform all the datasets is two days. Only 492 of the total transactions are fraud cases, a very minute percentage. Among all of the transactions in this dataset, only 0.172% represent fraudulent cases. The number of features is thirty. As mentioned, columns V1–V28 include all the relevant information, but PCA is applied to transform them into numerical values. Personal information has been kept private for apparent reasons of privacy. PCA Amount and Time may only be used to alter two features. The last element, "Class," indicates if the transaction is fraudulent, another crucial detail. The fraudulent transaction is denoted by a 1, whereas the non-fraudulent transaction is denoted by a 0. The distribution of fraudulent and non-fraudulent transactions in classes 0 and 1 is shown in Figure 5.

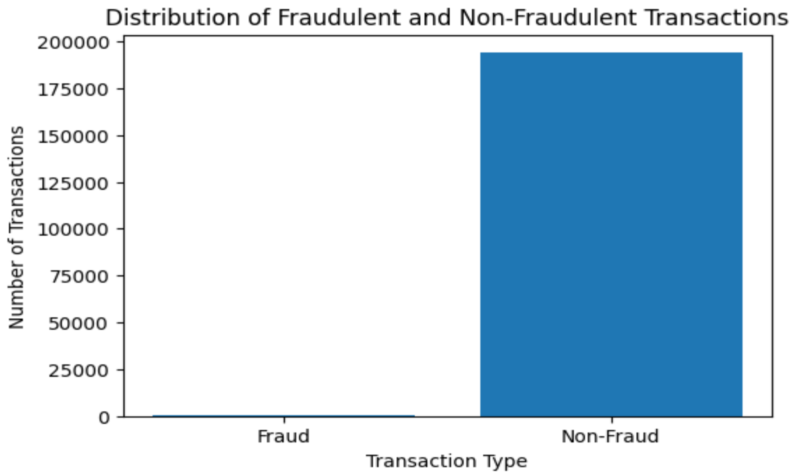

Figure 5: Show Distribution of Fraud and non-fraud transaction

Table 2 shows the statistical analysis of the dataset. It contains all the essential information, such as total transactions, fraudulent transactions, dataset features, the number of columns, and the days of transactions.

Table 2: Statistical information of dataset

Items	Value
Total transactions	284,807
Fraudulent transactions	492
Percentage fraudulent transaction	0.172%
Features	30
Number of columns	28
Days of transactions	2

Table 3 shows the dataset's features, such as cardholder ID, transaction ID, transaction time, amount, and transaction status, whether fraudulent or non-fraudulent.

Table 3: Features of Dataset

Features	Description
Cardholder ID	ID must be unique
Transaction ID	ID must be unique
Time	Duration of Transaction
Amount	A specific amount of spending
Status	Genuine or Fraudulent

AL-AASAR Journal
Quarterly *Research Journal*
www.al-aasar.com

Vol. 2, No. 3 (2025)
Online ISSN: 3006-693X
Print ISSN:3006-6921

4.2 Decision Tree:

Decision trees provide an efficient approach to machine learning, allowing classification and, therefore, credit card fraud detection. It is also the most popular machine-learning model. The decision tree built a tree-like structure for prediction. It helps by sorting different types of information about the transaction to decide whether it's fraudulent. The transaction attributes used for fraud prediction are transaction amount, time, location, and merchant category. The decision tree is trained from the transaction attributes and historical data. After learning this, the model can check whether the new transaction is original or fraudulent. Equation 1 of the decision tree is the following:

$$\boldsymbol{Entropy} = -\sum_{j=1}^{c} P(i)\, log_2 P(i) \qquad (1)$$

4.3 Random Forest:

Random Forest is one of the excellent machine-learning approaches to credit card fraud detection. Indeed, it's an extensively used statistical technique that can cope efficiently with large datasets, complex patterns, and fraud detection. It predicts by building many decision trees. These decision trees are trained from only a random subset of characteristics and data. All the decision trees give predictions according to their training and on behalf of the feature, such as whether each transaction is fraudulent. It provides a prediction on the base multiple decision trees. Equation 2 following:

$$\boldsymbol{Prediction}\ (\boldsymbol{Fraud\ or\ Not\ Fraud}) = mode\big(T1(y), T2(y), \dots, Tm(y)\big) \qquad (2)$$

4.4 Logistic Regression:

Logistic regression is the statistical method that is the best identifier of credit card scams. It used binary classification tasks for predictions. Logistic regression estimates the probability of fraudulent transactions based on dataset features. It is used to improve system performance. Logistic regression is used to input into one or two categories. The regression algorithms give output into 0 and then 1. The logistic regression model is trained from related features of the training dataset. The trained model predicts the possibility of fraud in new transactions. Equation 3 of logistic regression are following as:

$$\boldsymbol{Probability\ of\ Fraud}\ \big(\boldsymbol{P}(\boldsymbol{Fraud})\big) = \frac{1}{1 + \mathrm{e} - (\beta 0 + \beta 1 \mathrm{y}1 + \beta 2 \mathrm{y}2 + \cdots + \beta \mathrm{nyn})} \qquad (3)$$

5. Experimental Results:

We performed experiments on three suitable algorithms for fraudulent transaction detection. We present our results on the confusion matrix by heat map and analyze and compare our results on evaluation metrics.

5.1 Key Performance Metrics:

The models' performance is evaluated using the following metrics: True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN).

- Accuracy: It's measured when TP and TN are divided by all forecasts.

  Accuracy=TP + TN /TN + FP + FN + TP
- Precision: It's measured when an optimistic prediction is divided by the overall digit of affirmative forecasts.

  Precision=TP/ TP + FP
- Recall: The ratio of accurate optimistic predictions to the true positive and false negative.

  Recall=TP/ TP + FN
- F1 Score: The harmonic means providing a single metric that balances both.

  F1 Score=2×Precision×Recall/ Precision + Recall

Both the confusion matrix and the evaluation metrics express the outcome of the machine learning models. Figure 6 presents the heat map confusion matrix of the random forest model, Figure 7 presents the confusion matrix for the logistical regressed model, and Figure 8 presents the decision tree strategy confusion matrix.

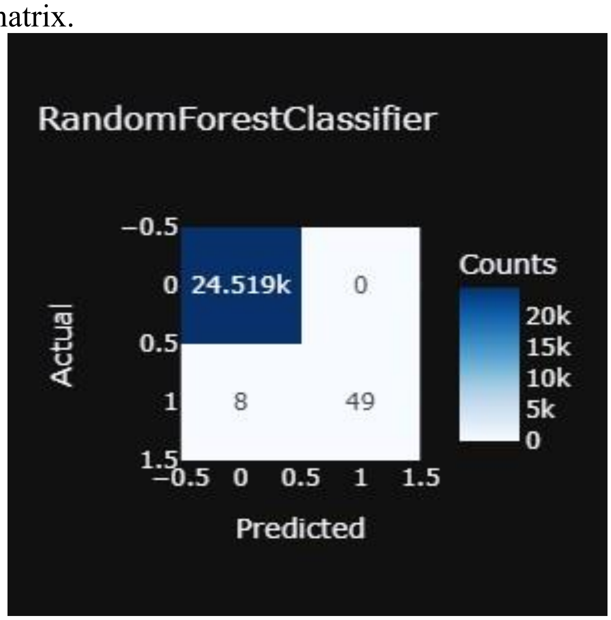

Figure 6: The confusion matrix of Random Forest

AL-AASAR Journal
Quarterly *Research Journal*
www.al-aasar.com

Vol. 2, No. 3 (2025)
Online ISSN: 3006-693X
Print ISSN:3006-6921

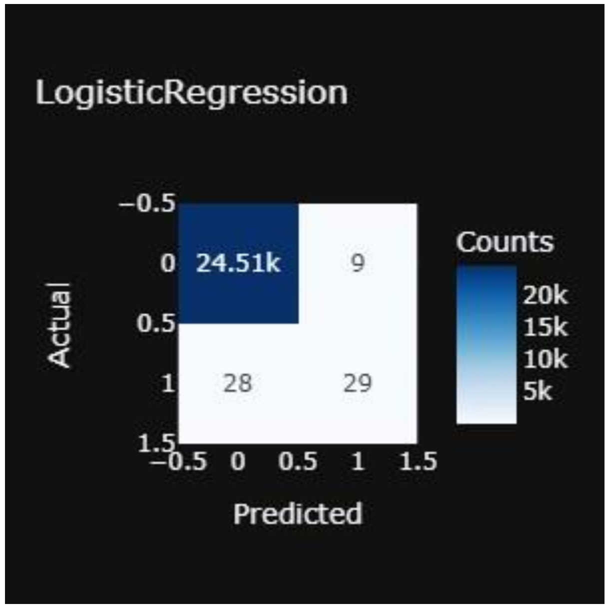

Figure 7: The confusion matrix of Logistic Regression

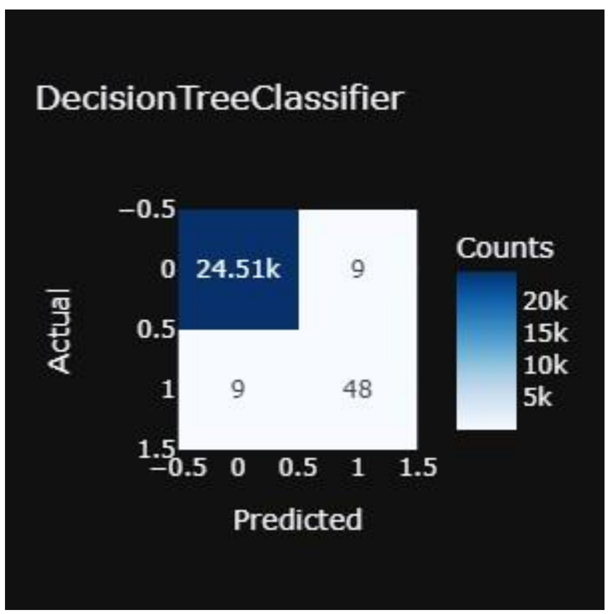

Figure 8: Forecasting decision tree classifier

Table 4 shows that the comparing of the results is evaluated using the following metrics:

Table 4. The Performance of Applied Machine Learning Models.

Models	Precision	Recall	F1-Score	Accuracy
Random Forest	0.98	0.93	0.96	0.99

AL-AASAR Journal
Quarterly *Research Journal*
www.al-aasar.com

Vol. 2, No. 3 (2025)
Online ISSN: 3006-693X
Print ISSN:3006-6921

Logistic Regression	0.88	0.75	0.80	0.99
Decision Tree	0.94	0.92	0.90	0.99

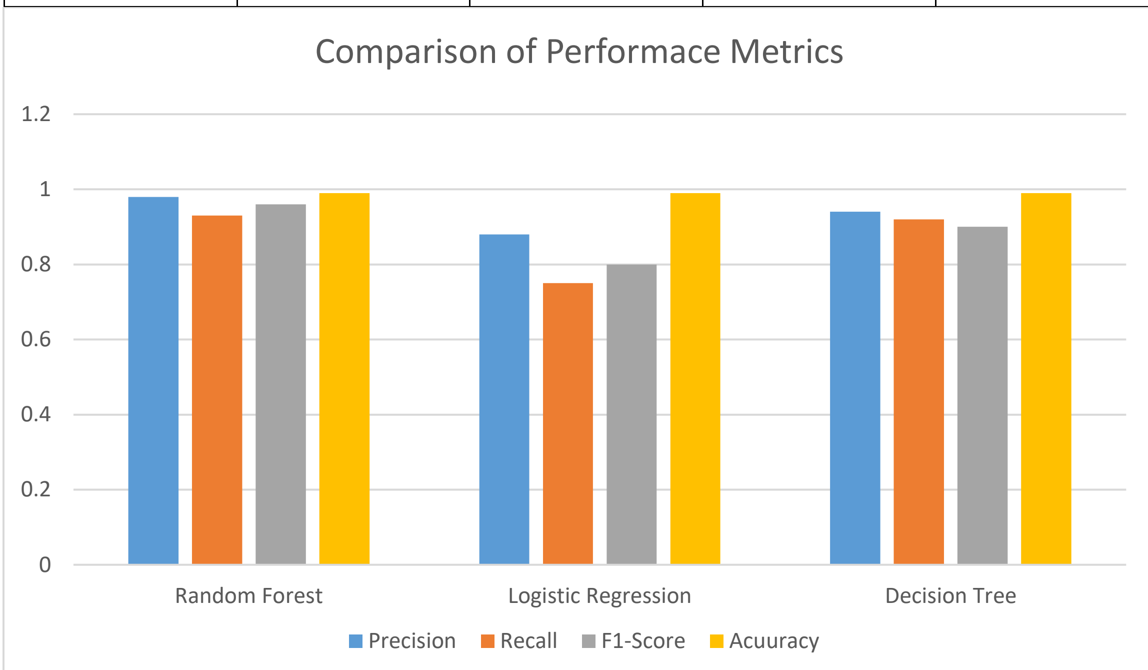

Figure: 9 Comparison of Performance Metrics

Figure 9 shows the results of machine learning models. The accuracy of all the models is 0.99 percent. Because the majority of data sets are non-fraudulent transactions, only 492 fraudulent Transactions are present, and the accuracy is very high. The decision tree performs better than the logistic regression, and the random forest accuracy is better than other evaluation metrics. Figure 10 shows the contrast of the accuracy for all machine learning models.

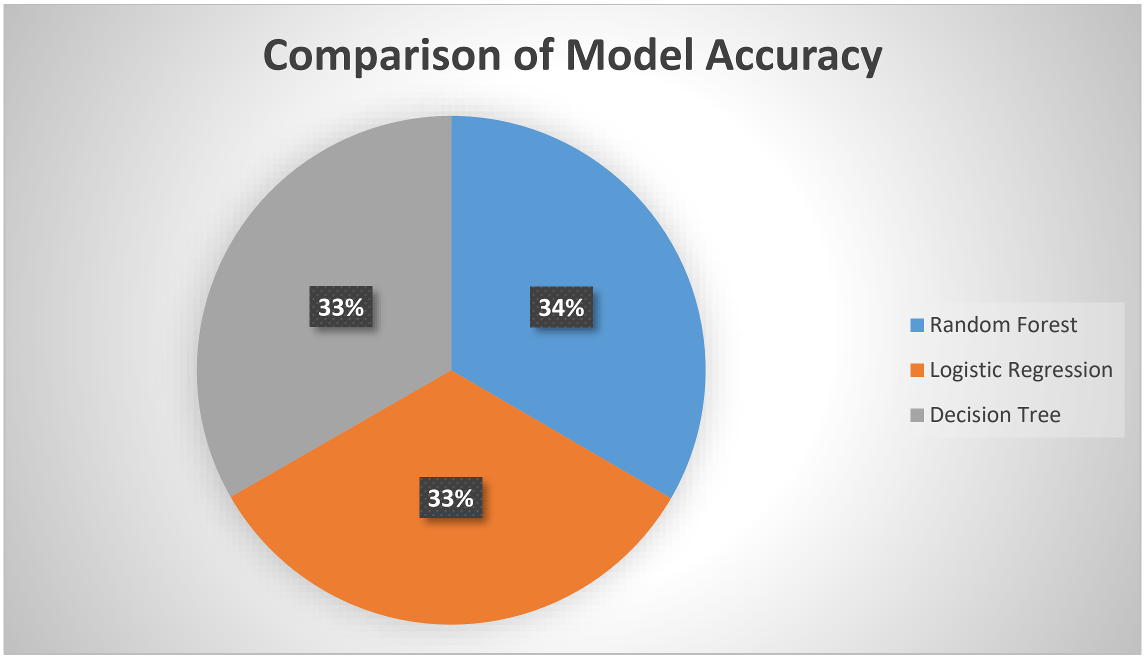

Figure: 10. Comparison of accuracy

6. Conclusion:

Credit card fraud is one of the major problems prevailing in today's computerized world, both for the consumer and financial organizations. It's posed a severe threat to financial organizations' transactions. Therefore, the economic organization invested a lot of money in developing new techniques to prevent scams. Since these methods brought better results, previous research was based on these techniques. This paper compares machine learning algorithms for detecting fraud. This study used decision trees, logistic regression, and random forests. All of the models have an accuracy rate of 99%. Studies have proven that Random Forest is the best machine-learning for detecting scams. In future studies, resampling techniques like SMOTE will improve the output of the machine learning model. Deep learning models will also be used to enhance the efficacy of fraud detection methods.

References

1. Zainab, Hira, Ali Raza A. Khan, Muhammad Ismaeel Khan, and Aftab Arif. "Ethical Considerations and Data Privacy Challenges in AI-Powered Healthcare Solutions for Cancer and Cardiovascular Diseases." Global Trends in Science and Technology 1, no. 1 (2025): 63-74.
2. Bhatla, Tej Paul, Vikram Prabhu, and Amit Dua. "Understanding credit card frauds." *Cards business review* 1.6 (2003): 1-15.
3. Siddiqi, Naeem. *Credit risk scorecards: developing and implementing intelligent credit scoring*. Vol. 3. John Wiley & Sons, 2012.
4. Surekha, M., U. Umesh, and D. Paul Dhinakaran. "A study on utilisation and convenience of credit card." *Journal of Positive School Psychology* (2022): 5635-5645.

5. Aziz, Rimsha, Aneela Mehmood, Asma Tariq, Fawad Nasim, Umar Farooq, Syed Asad Ali Naqvi, and Hamayun Khan. "Critical Evaluation of Data Privacy and Security Threats: An Intelligent Federated Learning-based Intrusion Detection System Poisoning Attack and Defense for Cyber-Physical Systems its Issues and Challenges Related to Privacy and Security in IoT." The Asian Bulletin of Big Data Management 5, no. 1 (2025): 73-84.
6. Arif, Aftab, Muhammad Ismaeel Khan, and Ali Raza A. Khan. "An overview of cyber threats generated by AI." International Journal of Multidisciplinary Sciences and Arts 3, no. 4 (2024): 67-76.
7. GUPTA, A. B., AKTER, S., ISLAM, M., JABED, M. M. I., & FERDOUS, J. (2023). Smart Defense: AI-Powered Adaptive IDs for Real-Time Zero-Day Threat Mitigation.
8. Khan, M. I., A. Arif, and A. R. A. Khan. "AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity." BIN: Bulletin of Informatics 2, no. 2 (2024): 248-61.
9. Nasim MF, Anwar M, Alorfi AS, Ibrahim HA, Ahmed A, Jaffar A, Akram S, Siddique A, and Zeeshan HM (2025). Cognitively inspired sound-based automobile problem detection: A step toward explainable AI (XAI). International Journal of Advanced and Applied Sciences, 12(8): 1-15
10. Gadam, H., & Upadhyay, A. (2024). INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.
11. Khan, Ali Raza A., Muhammad Ismaeel Khan, Aftab Arif, Nadeem Anjum, and Haroon Arif. "Intelligent Defense: Redefining OS Security with AI." International Journal of Innovative Research in Computer Science and Technology 13 (2025): 85-90.
12. Zainab, Hira, A. Khan, Ali Raza, Muhammad Ismaeel Khan, and Aftab Arif. "Integration of AI in Medical Imaging: Enhancing Diagnostic Accuracy and Workflow Efficiency." Global Insights in Artificial Intelligence and Computing 1, no. 1 (2025): 1-14.
13. Zainab, Hira, Ali Raza A. Khan, Muhammad Ismaeel Khan, and Aftab Arif. "Innovative AI Solutions for Mental Health: Bridging Detection and Therapy." Global Journal of Emerging AI and Computing 1, no. 1 (2025): 51-58.
14. Khan, Ali Raza A., Muhammad Ismaeel Khan, and Aftab Arif. "AI in Surgical Robotics: Advancing Precision and Minimizing Human Error." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 1 (2025): 17-30.
15. Delamaire, Linda, H. A. H. Abdou, and John Pointon. "Credit card fraud and detection techniques: a review." *Banks and Bank Systems* 4.2 (2009).
16. Khan, Muhammad Ismaeel, Aftab Arif, and Ali Raza A. Khan. "AI's Revolutionary Role in Cyber Defense and Social Engineering." International Journal of Multidisciplinary Sciences and Arts 3, no. 4 (2024): 57-66.
17. Zainab, Hira, Muhammad Ismaeel Khan, Aftab Arif, and Ali Raza A. Khan. "Development of Hybrid AI Models for Real-Time Cancer Diagnostics Using Multi-Modality Imaging (CT, MRI, PET)." Global Journal of Machine Learning and Computing 1, no. 1 (2025): 66-75.
18. Tariq, Muhammad Arham, Muhammad Ismaeel Khan, Aftab Arif, Muhammad Aksam Iftikhar, and Ali Raza A. Khan. "Malware Images Visualization and Classification With

Parameter Tunned Deep Learning Model." Metallurgical and Materials Engineering 31, no. 2 (2025): 68-73.https://doi.org/10.63278/1336.

19. Arif, Aftab, Muhammad Ismaeel Khan, Ali Raza A. Khan, Nadeem Anjum, and Haroon Arif. "AI-Driven Cybersecurity Predictions: Safeguarding California's Digital Landscape." International Journal of Innovative Research in Computer Science and Technology 13 (2025): 74-78.
20. Zainab, Hira, Muhammad Ismaeel Khan, Aftab Arif, and Ali Raza A. Khan. "Deep Learning in Precision Nutrition: Tailoring Diet Plans Based on Genetic and Microbiome Data." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 1 (2025): 31-42.
21. Itoo, Fayaz, Meenakshi, and Satwinder Singh. "Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection." *International Journal of Information Technology* 13.4 (2021): 1503-1511.
22. Najadat, Hassan, et al. "Credit card fraud detection based on machine and deep learning." *2020 11th International Conference on Information and Communication Systems (ICICS)*. IEEE, 2020.
23. Khan, Muhammad Ismaeel. "Synergizing AI-Driven Insights, Cybersecurity, and Thermal Management: A Holistic Framework for Advancing Healthcare, Risk Mitigation, and Industrial Performance." Global Journal of Computer Sciences and Artificial Intelligence 1, no. 2: 40-60.
24. Syeda, Farjana, Farabi., Mani, Prabha, Ro., Md., Mahabub, Alam., Md., Shorif, Hossan., Md, Ariful., Md., Rafiqul, Islam., Aftab, Uddin., MAH, Bhuiyan., Manindra, Nath, Biswas. "Enhancing Credit Card Fraud Detection: A Comprehensive Study of Machine Learning Algorithms and Performance Evaluation." Journal of Business and Management Studies, undefined (2024). doi: 10.32996/jbms.2024.6.13.21
25. Khan, Muhammad Ismaeel, Aftab Arif, Ali Raza A. Khan, Nadeem Anjum, and Haroon Arif. "The Dual Role of Artificial Intelligence in Cybersecurity: Enhancing Defense and Navigating Challenges." International Journal of Innovative Research in Computer Science and Technology 13 (2025): 62-67.
26. Khan, Muhammad Ismaeel, Aftab Arif, and Ali Raza A. Khan. "The Most Recent Advances and Uses of AI in Cybersecurity." BULLET: Jurnal Multidisiplin Ilmu 3, no. 4 (2024): 566-578.
27. Arif, Aftab, Fadia Shah, Muhammad Ismaeel Khan, Ali Raza A. Khan, Aftab Hussain Tabasam, and Abdul Latif. 2023. “Anomaly Detection in IoHT Using Deep Learning: Enhancing Wearable Medical Device Security.” Migration Letters 20 (S12): 1992–2006.
28. Mohsen, Omar Rajab, Ghalia Nassreddine, and Mazen Massoud. "Credit Card Fraud Detector Based on Machine Learning Techniques." *Journal of Computer Science and Technology Studies* 5.2 (2023): 16-30.
29. Lakshmi, S. V. S. S., and Selvani Deepthi Kavilla. "Machine learning for credit card fraud detection system." *International Journal of Applied Engineering Research* 13.24 (2018): 16819-16824

30. Minjun, Dai. "Multiple Machine Learning Models on Credit Card Fraud Detection." BCP business & management, undefined (2023). Doi: 10.54691/bcpbm.v44i.4839.
31. A Review: Credit Card Fraud Detection in Banks using Machine Learning Algorithms." undefined (2023). doi: 10.14293/s2199-1006.1.sor-.ppfi7p0.v2
32. Omega, John, Unogwu., Youssef, Filali. "Fraud Detection and Identification in Credit Card Based on Machine Learning Techniques." Wasit Journal of Computer and Mathematics Science, undefined (2023). doi: 10.31185/wjcms.185
33. Iqra, Shahzad., Amna, Sajid., Maira, Anwar., Nosheen, Anwar. (2023). Fraud Detection of Credit Cards Using Supervised Machine Learning Techniques. Pakistan Journal of Emerging Science and Technologies (PJEST), doi: 10.58619/pjest.v4i3.114
34. Varmedja, Dejan, et al. "Credit card fraud detection-machine learning methods." 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH). IEEE, 2019.
35. Muhammad, Zohaib, Khan., Sarmad, Ahmed, Shaikh., Muneer, Ahmed, Shaikh., Kamlesh, Kumar, Khatri., Ayesha, Kalhoro., Muhammad, Adnan. "The Performance Analysis of Machine Learning Algorithms for Credit Card Fraud Detection." International Journal of Online Engineering (ijoe), undefined (2023). doi: 10.3991/ijoe.v19i03.35331
36. Jia, Xia. "Credit Card Fraud Detection Based on Support Vector Machine." Highlights in Science, Engineering, and Technology, undefined (2022). doi: 10.54097/hset.v23i.3202
37. Tesfahun, Berhane., Assaye, Walelign. "A Hybrid Convolutional Neural Network and Support Vector Machine-Based Credit Card Fraud Detection Model." Mathematical Problems in Engineering, undefined (2023). doi: 10.1155/2023/8134627
38. Jabed, M. M. I. (2022). Self-Supervised Learning for Efficient and Scalable AI: Towards Reducing Data Dependency in Deep Learning Models. *International Journal of Intelligent Systems and Applications in Engineering*, *10*(10).
39. Arif, A., A. Khan, and M. I. Khan. "Role of AI in Predicting and Mitigating Threats: A Comprehensive Review." JURIHUM: Jurnal Inovasi dan Humaniora 2, no. 3 (2024): 297-311.
40. Hassan, M. M., Jabed, M. M. I., Islam, M., Islam, S. N., & Arif, M. I. From Formalism to Functionality: Leveraging AI and Ml to Advance Foundational Computer Science Paradigms.
41. M. F. Khan, "Explainable Ai and Machine Learning Models for Transparent and Scalable Intrusion Detection Systems," *J. Inf. Syst. Eng. Manag.*, vol. 9, no. 4s, pp. 1576–1588, Dec. 2024, doi: 10.52783/jisem.v9i4s.12115
42. L. Akter, "Quantum-Inspired Machine Learning for Zero-Trust Cybersecurity: A Paradigm beyond Classical Intrusion Detection," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 20s, pp. 1070–1080, Apr. 2024.
43. S. Ferdous, "Energy-Aware AI and Machine Learning Approaches for Next-Generation IDS," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 23s, pp. 3601–3615, Oct. 2024.