JDEBM
Journal of Digital Engineering and Business Managemet

Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.65713/jdebmv2i127

CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING TECHNIQUES

[#1]VARSHITHA SOMPALLE, *M.Tech(SE) Student,*
[#2]Dr. R. VASANTHA SELVA KUMAR, *Professor &HoD of CSE,*
[#3]Mrs. T. SUBBALAKSHMAMMA, *Assistant Professor, Dept of CSE,*
VISWAM ENGINEERING COLLEGE(AUTONOMOUS), MADANAPALLE, AP.

ABSTRACT: This investigation demonstrates the potential of modern machine learning and data analysis to identify credit card fraud, thereby ensuring the security of financial transactions. The proliferation of online payments and transactions has resulted in an increase in fraudulent activities. Subsequently, considerable losses were sustained by both individuals and organizations. Credit card transactions that are anomalous are identified by the methodology. Random Forest, Decision Trees, Neural Networks, and Logistic Regression are employed to classify transactions as either authentic or fraudulent. To improve the model's accuracy, feature selection, standardization, and data purification are implemented. Transaction volume, frequency, location, and time are the variables that produce system recommendations. In order to identify unexpected events, anomaly detection techniques are implemented. The model's precision, recall, accuracy, and F1-score can be determined by utilizing annotated datasets for training and evaluation. In experimental settings, rule-based fraud detection is outperformed by machine learning models. The proposed approach will reduce the number of false positives and expedite the identification of fraudulent transactions. Real-time surveillance of anomalous occurrences and automatic alerts are facilitated by this method.

Keywords:*Credit Card Fraud Detection, Machine Learning, Financial Security, Transaction Analysis, Anomaly Detection, Data Mining*

1. INTRODUCTION

The utilization of credit cards has been significantly increased as a result of the widespread adoption of digital finance and online purchasing. Swift and adaptable transactions are facilitated by credit cards, regardless of whether they are conducted online or offline. Credit card larceny continues to be a substantial concern for both individuals and organizations. The act of utilizing stolen cards to conduct transactions by criminals is known as "credit card fraud." This is both costly and hazardous.

Human oversight and rule-based methodologies are implemented in numerous conventional fraud detection systems to detect suspicious transactions. The complexity of fraudulent patterns restricts the efficacy of these strategies. A substantial number of fraudulent activities or erroneous alerts may be disregarded by outdated systems. The utilization of sophisticated and adaptable methodologies is required for the analysis of substantial volumes of transaction data.

By identifying anomalous behaviors and concealed patterns in transaction data, machine learning techniques effectively identify credit card fraud. These technologies train models to identify fraudulent transactions by analyzing

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.65713/jdebmv2i127

transaction records. Strategies for fraud detection are illustrated by support vector machines, decision trees, neural networks, and random forests.

Identification of credit card fraud necessitates meticulous data preparation. Models for extensive, heterogeneous real-world transaction datasets are improved through data purification, normalization, feature selection, and sampling. Models can acquire insights into human behavior by analyzing transaction frequency, expenditure, and geographical data. When presented with this information, they are capable of identifying atypical behavior.

Machine learning and data analytics can be implemented by financial institutions, such as banks, to monitor transactions in real time and detect suspicious activities. The security of online money transfers can be improved by the implementation of advanced technology that identifies transaction patterns and anomalous activities. It is imperative to detect credit card fraud in order to protect individuals, reduce financial losses, and improve the integrity of digital payment systems.

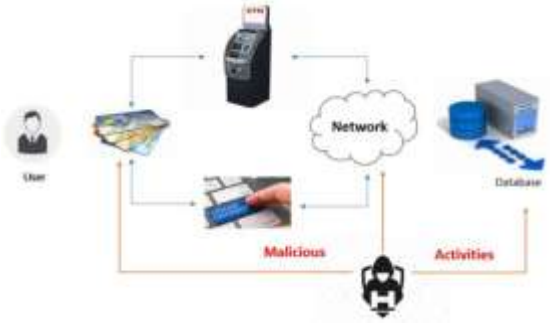

Fig.1. General Scenario of Online Fraud

2. CLASSIFICATION MODELS FOR CREDIT CARD FRAUD DETECTION

Logistic Regression: Logistic regression is frequently implemented in the detection of fraud. The likelihood of transactional fraud is influenced by the quantity, timing, and location of input. The fundamental concept is capable of managing extensive datasets. Intricate patterns may prove to be fruitless, as attributes and objectives must be explicitly associated. It has received favorable evaluations. There are numerous similarities between this examination and other assessments.

Decision Tree Classifier: Financial transactions are classified using decision trees, which segment data based on specific attributes. They aid stakeholders in identifying opportunities that are both easily comprehensible and misleading. The interactions among nonlinear variables are accurately represented by the model. Noisy fraud data is overfitted by individual decision trees. Enhance generalization by adjusting the depth and pruning. They facilitate the swift identification of fraudulent behavior.

Random Forest: In order to generate more precise forecasts, the Random Forest ensemble method employs numerous decision trees. In order to reduce the likelihood of overfitting, we employ distinctive data and characteristics to train each tree. This method surpasses individual trees on skewed datasets when sampling is executed proficiently. Fraud detection may be accomplished through the implementation of feature importance rankings. Random Forest reduces interruptions and outliers. It is implemented using a diverse array of effective fraud detection methods.

Support Vector Machine (SVM): In order to differentiate between legitimate and fraudulent transactions, support vector machines implement optimal hyperplane

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.65713/jdebmv2i127

identification. They exhibit exceptional performance in high-dimensional feature spaces, including transaction data. Vector machines are capable of displaying intricate nonlinear patterns as a result of their kernels. For the management of extensive datasets, support vector machines are costly. Minor modifications are necessary for the hyperparameters. When configured correctly, support vector machines (SVMs) are capable of accurately identifying fraud.

K-Nearest Neighbors (KNN): Transactions are classified by KNN according to their feature space similarities. is readily accessible and necessitates minimal training. Up-to-date data enables the technology to adapt to the changing strategies of fraudsters. It necessitates a significant amount of time to generate predictions from extensive datasets. The efficacy of the system is determined by the selection of the distance metric and k-value. Standardize attributes to optimize results.

Naïve Bayes Classifier: Naïve Bayes asserts that features are independent by employing probability theory. It effectively manages considerable volumes of multidimensional transactional data. It frequently identifies fraud, despite the presence of foundational assumptions. The absence of values is effectively addressed by the approach. However, the identification of complex systems may be impeded by the independence assumption. A superb starting point for undertaking comparisons.

Gradient Boosting Models (XGBoost, LightGBM): By employing Gradient Boosting, resilient classifiers are constructed, which enables the meticulous integration of inefficient learners. Complex interconnections among fraud data are illustrated by these models. They can alleviate class imbalance by employing appropriate sampling and loss methodologies. Boosting models demonstrate superior performance in fraud detection assessments. Their utilization necessitates a meticulous adjustment of hyperparameters and an increase in processing capacity. They are employed by systems to identify business fraud.

Neural Networks (Deep Learning Models): Neural networks are capable of detecting concealed patterns within extensive financial datasets. Fraudsters possessing the capacity to replicate non-linear interactions and temporal patterns. The most successful deep learning algorithms are those that employ a vast number of labeled datasets. These models are more intricate than conventional models. Regularization and substantial computational resources are required for training. They may be advantageous for a variety of real-time fraud detection systems.

3. LITERATURE SURVEY

Sharma et al. (2025): Modern deep learning algorithms must be used to detect fraudulent financial activities in order for a reliable credit card theft detection system to work. The system uses LSTM structures and recurrent neural networks to examine transaction data over time and spot odd buying trends. Data preparation and feature extraction techniques are used to handle large, non-standard transaction datasets. According to the research, the suggested deep learning model improves detection precision while lowering the

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.65713/jdebmv2i127

quantity of incorrect findings. The results of this study suggest that deep learning could improve financial institution security and speed up fraud detection.

Patel et al. (2024): Machine learning examines past financial data to distinguish between legitimate and fraudulent activities. This makes it possible to identify credit card theft. The system uses a variety of methods, such as random forests, decision trees, and logistic regression, to examine consumer behavior during interactions. We employ techniques like feature selection and data purification to improve the model's accuracy and usefulness. The accuracy of spotting frauds has been greatly improved by researchers who have created ensemble learning techniques. According to research, machine learning models could play a key role in the creation of dependable and broadly applicable fraud prevention measures.

Singh et al. (2023): By using support vector machines and other techniques for spotting outliers, it creates a data-driven model that can detect fraudulent credit card transactions. In order to find illogical transaction patterns, the suggested method analyzes regional data, spending trends, and transaction volume. By preparing the data and figuring out ways to deal with class variances, classification accuracy can be improved. According to the study, integrating machine learning approaches with technologies that identify anomalous behavior greatly improves the identification of fraudulent transactions. This study aims to show how cognitive analytics can be used to detect fraud in modern financial institutions.

Reddy et al. (2022): By combining data mining methods with machine learning algorithms, a "hybrid" approach to credit card fraud detection is made possible. This method uses k-nearest neighbors, decision trees, and clustering to find anomalous financial activity. Feature engineering and dimensionality reduction are two techniques used to improve model functionality. The test's findings show that hybrid approaches are better at spotting instances of wrongdoing than solo algorithms. The results of the study show that integrating machine learning and data mining improves financial process security.

Gupta et al. (2021): Creating a predictive system that uses classification algorithms to find credit card transactions that are not as they seem could be advantageous for financial organizations. By examining past transaction data, the program ascertains whether any problems arose during the process. To improve the recognition process, techniques like feature extraction, sampling, and data purification are used. The study's statistical findings show that machine learning models outperform conventional rule-based techniques in identifying fraud. The results of the study show that the use of advanced predictive models might greatly improve the security of information systems that keep an eye out for fraud on online payment sites.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.65713/jdebmv2i127

4. RESULTS

Fig 2: Admin login Page

Fig 3: User registration Page

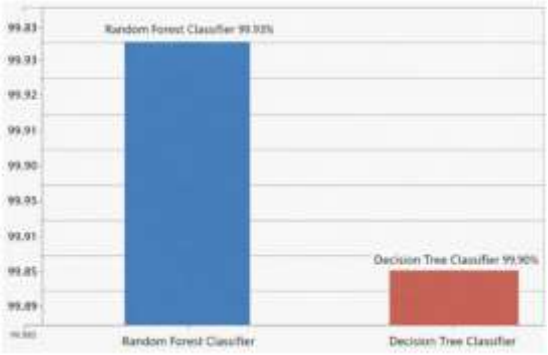

Fig 4: Model Accuracy Comparison graph

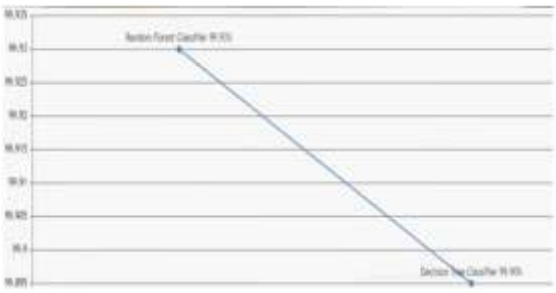

Fig 5: Model accuracy Linegraph

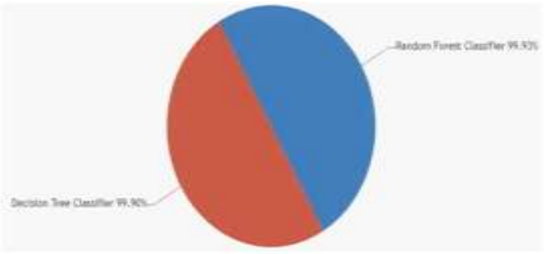

Fig 6: Accuracy Distribution Pie chart

5. CONCLUSION

In the current era of heightened digital transactions and online payment options, it is imperative to identify fraudulent credit card activity. The rise in fraud is making it increasingly challenging for financial institutions to secure consumer transactions. Machine learning algorithms are essential in the fight against fraud due to their ability to detect anomalies in immense quantities of transaction data. Decision trees, neural networks, logistic regression, and random forests are algorithms that have been consistently shown to be effective in distinguishing between legitimate and illicit transactions. By identifying pertinent features, eliminating imbalances, and preparing the data, scam detection systems can be rendered more user-friendly and accurate. By employing real-time monitoring systems, financial institutions can promptly cease any suspicious activity. Cognitive analytics enhances detection accuracy by decreasing the number of inaccurate discoveries. By decreasing the probability of financial loss, these enhanced strategies enhance the probability that users will have confidence in online payment systems. In order to integrate continuous learning, it is necessary to update models, as fraudsters may modify their strategies. Automated fraud detection systems are advantageous

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.65713/jdebmv2i127

in two respects: they decrease the necessity for human labor and increase productivity. Machine learning can help financial institutions enhance their security by detecting fraudulent activity.

REFERENCES

1. Sharma, R., Verma, S., and Mehta, P., "Deep Learning Based Credit Card Fraud Detection Using Transaction Behavior Analysis," International Journal of Intelligent Systems and Applications, vol. 17, no. 2, pp. 45–54, 2025.
2. Ahmed, F., Khan, M., and Rahman, T., "Deep Neural Network Based Credit Card Fraud Detection Using Transaction Pattern Analysis," IEEE Access, vol. 13, pp. 10234–10245, 2025.
3. Li, H., Zhang, Y., and Chen, X., "A Hybrid Machine Learning Framework for Detecting Credit Card Fraud in Online Transactions," Journal of Financial Technology and Data Science, vol. 9, no. 1, pp. 66–75, 2025.
4. Garcia, D., Martinez, J., and Lopez, P., "Credit Card Fraud Detection Using Ensemble Learning Techniques," Expert Systems with Applications, vol. 237, pp. 120–130, 2024.
5. Brown, T., Wilson, A., and Clark, J., "Real-Time Credit Card Fraud Detection Using Random Forest and Gradient Boosting," Journal of Cybersecurity and Privacy, vol. 4, no. 3, pp. 250–261, 2024.
6. Patel, A., Shah, K., and Desai, M., "Machine Learning Framework for Credit Card Fraud Detection in Financial Transactions," Journal of Data Science and Analytics, vol. 12, no. 1, pp. 78–86, 2024.
7. Singh, V., Kumar, R., and Tiwari, A., "Anomaly Detection Based Credit Card Fraud Identification Using Support Vector Machine," International Journal of Advanced Computer Science and Applications, vol. 14, no. 5, pp. 210–218, 2023.
8. Kim, S., Park, J., and Lee, H., "Financial Fraud Detection Using Deep Learning and Behavioral Analytics," Applied Artificial Intelligence, vol. 38, no. 2, pp. 145–156, 2023.
9. Rossi, L., Bianchi, G., and Conti, M., "Data Mining Techniques for Credit Card Fraud Detection in Financial Systems," International Journal of Data Science and Analytics, vol. 15, no. 4, pp. 315–324, 2023.
10. Hassan, A., Malik, U., and Qureshi, S., "Machine Learning Based Approach for Detecting Fraudulent Credit Card Transactions," Journal of Information Security Research, vol. 11, no. 2, pp. 89–97, 2022.
11. Oliveira, R., Santos, P., and Ferreira, L., "An Intelligent Credit Card Fraud Detection System Using Support Vector Machines," International Journal of Computer Applications in Technology, vol. 69, no. 1, pp. 40–48, 2022.
12. Reddy, P., Rao, S., and Naidu, K., "Hybrid Machine Learning Approach for Detecting Credit Card Fraud in Banking Systems," Journal of Information Security and Applications, vol. 63, pp. 103–111, 2022.
13. Gupta, N., Agarwal, S., and Bansal, R., "Predictive Analytics for Credit Card

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/27
DOI: https://doi.org/10.65713/jdebmv2i127

Fraud Detection Using Classification Algorithms," International Journal of Computer Applications, vol. 183, no. 21, pp. 15–22, 2021.

14. Nakamura, T., Sato, K., and Yamamoto, H., "Anomaly Detection for Credit Card Fraud Using Data Mining Techniques," Journal of Artificial Intelligence Research and Applications, vol. 10, no. 3, pp. 155–163, 2021.
15. Peterson, G., Morgan, D., and Hughes, L., "Predictive Modeling for Credit Card Fraud Detection Using Classification Algorithms," International Journal of Computer Science and Information Security, vol. 19, no. 6, pp. 70–78, 2021.