engineering proceedings

MDPI

Proceeding Paper

Dynamic Feature Engineering for Adaptive Fraud Detection †

Ajay Sharma [1,*], Shamneesh Sharma [2], Arun Malik [1], Rajeev Sobti [1] and Anang Suryana [3]

[1] School of Computer Science and Engineering, Lovely Professional University, Jalandhar 144411, Punjab, India; arunmalikhisar@gmail.com (A.M.); rajeev.sobti@lpu.co.in (R.S.)
[2] Customer Success and Quality Control, byteXL TechEd Private Limited, Hyderabad 500081, Telangana, India; shamneesh.sharma@gmail.com
[3] Department of Electrical Engineering, Nusa Putra University, Sukabumi 43152, West Java, Indonesia; anang.suryana@nusaputra.ac.id
* Correspondence: ajaysharmadharmani@gmail.com
† Presented at the 7th International Global Conference Series on ICT Integration in Technical Education & Smart Society, Aizuwakamatsu City, Japan, 20–26 January 2025.

Abstract

In today's digital economy, electronic payments are essential to supporting financial transactions. However, the danger of fraud also rises with company complexity and volume. This study uses machine learning and advanced analytics to investigate fraud detection in electronic payments. Using business tools like accounts, account types, and balance sheets, we spot patterns and trends connected to illicit activities. To detect and identify fraud, our study uses pre-existing data, machine learning algorithms, and infrastructure. The author has assessed the performance of several models, such as logistic regression, random forests, and k-nearest neighbor models, using criteria like accuracy, precision, and recall. To determine the most important characteristics for fraud detection, the author also conducts a significance analysis and examines the model's interpretability. According to the current study's findings, financial institutions and payment systems will be able to identify fraud more efficiently and gain an improved knowledge of the traits of commercial fraud.

Keywords: payment gateway; algorithms; fraudulent; detection; transactions; machine learning; deep learning

check for updates

Academic Editors: Debopriyo Roy, George F. Fragulis and Peter Ilic

Published: 8 September 2025

Citation: Sharma, A.; Sharma, S.; Malik, A.; Sobti, R.; Suryana, A. Dynamic Feature Engineering for Adaptive Fraud Detection. *Eng. Proc.* **2025**, *107*, 68. https://doi.org/10.3390/engproc2025107068

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the introduction of electronic payments (e-payments), financial transactions have been carried out in a different, faster, and more convenient manner for businesses and customers worldwide. Electronic commerce has grown to be a vital component of the modern economy, encompassing Peer-to-Peer (P2P) transactions, contactless payments, internet shopping, and mobile commerce [1]. There are hazards associated with digital payments as well, including the possibility of fraud. E-payments have fundamentally transformed the landscape of financial transactions, enabling them to be conducted in a manner that is not only different from traditional methods but also significantly faster and more convenient for businesses across the globe. This shift has been driven by advancements in technology, which have facilitated the development of various e-payment systems that are now integral to the daily operations of both individuals and enterprises.

One of the most significant impacts of e-payments has been on the speed and efficiency of transactions. Earlier, financial transactions often involved physical exchanges of currency and the manual processing of checks, which could take days or even weeks to complete.

Today, with the advent of e-payments, transactions can be carried out almost instantaneously, regardless of geographical location. This proximity improved the efficiency of businesses by accelerating cash flow and reducing the time required to settle payments, but has also enhanced the customer experience by providing a seamless, convenient way to make purchases or transfer funds.

The rise in electronic payments has also been closely linked to the growth of electronic commerce, which has become a vital component of the modern economy. E-commerce encompasses a wide range of activities, including P2P transactions, contactless payments, online shopping, and mobile commerce, all of which rely heavily on electronic payment systems. P2P transactions, e.g., allow individuals to transfer money directly to each other without the need for intermediaries like banks. This is possible through digital platforms that facilitate such exchanges in real time, often at a lower cost than traditional banking methods [2–4]. Contactless payments, which allow customers to purchase by touching their cards or mobile devices at a point-of-sale terminal, have gained widespread adoption due to their convenience and speed. This form of payment has become particularly popular in retail environments, where reducing transaction time is crucial for both businesses and customers. Online shopping (e-commerce) has also seen exponential growth, with electronic payments playing a central role in enabling consumers to purchase goods and services from the comfort of their homes. Mobile commerce (m-commerce) extends the reach of e-payment by allowing transactions to be conducted via smartphones and tablets, making it possible for consumers to shop and pay for services anytime and anywhere [5–7].

The numerous benefits of electronic payments are not without risks. One of the most significant hazards associated with digital payments is the potential for fraud. Fraudsters employ a range of strategies, such as identity theft, money laundering, and illicit transactions, to exploit weaknesses in payment systems. Stakeholders in the financial industry are increasingly concerned about identifying and combating fraud as the volume and complexity of electronic trade rise [8]. As more transactions move online, cybercriminals have increasingly targeted electronic payment systems, seeking to exploit vulnerabilities for financial gain. Fraudulent activities, such as identity theft, phishing attacks, and unauthorized transactions, result in substantial financial losses for both individuals and businesses. The necessity for rigorous security measures to safeguard confidential financial information and preserve transaction integrity has been underscored by the increase in cybercrime associated with electronic payments.

For instance, phishing attacks involve fraudsters impersonating legitimate businesses, such as financial institutions and payment service providers, and deceiving consumers into disclosing their personal information, such as login credentials and credit card numbers. Once this information is obtained, it can be used to make unauthorized transactions, even steal an individual's identity, leading to severe financial and personal losses [9]. The potential for identity fraud is another significant concern with online payment systems. Criminals can perpetrate identity theft by creating fake accounts, loan applications, and purchase records in the name of another individual as a result of the theft of sensitive personal information. The theft of your personal information can have a long-term, catastrophic effect on your financial stability and credit. Due to the simplicity with which digital information can be copied and disseminated, identity theft is particularly challenging to prevent or limit. Unauthorized transactions are yet another form of fraud that can occur with electronic payments [10]. These transactions might be the result of hacked accounts, stolen payment information, or even insider fraud within an organization. The complexity of tracing unauthorized transactions across digital platforms and multiple jurisdictions can make it difficult for victims to recover their lost funds [11].

To address the payment processors, financial institutions are increasingly relying on sophisticated analytics and machine learning (AI/ML) techniques to enhance their capacity for fraud detection. By using the volume of data exchanged (no. of transactions) and using ML algorithms to find out the trends and abnormalities, these systems can identify fraud more accurately at a lower risk. To mitigate the risks, businesses and payment service providers have implemented a variety of security measures. Encryption technology (SHA), for instance, plays a crucial role in safeguarding transaction data by encoding information so that it can only be accessed by authorized parties. Two-factor authentication (2FA) is increasingly being used to add a supplementary layer of protection, demanding users prove their identity by a second mechanism, text code, or biometric scan before completing a transaction [12,13]. Despite certain measures, the threat of fraud remains ever-present, requiring continuous advancements in security technologies and practices. Consumers, too, must remain vigilant, adopting best practices such as constantly monitoring their accounts for unusual activity, using strong and unique passwords, and being vigilant of unsolicited communications that request personal information. The introduction of e-payments transformed the way payments are handled, bringing unrivaled speed, convenience, and efficiency. It has also introduced new risks, particularly the potential for fraud. As electronic commerce continues to grow and evolve, the ongoing challenge will be to balance the benefits of digital payments with the need for robust security measures that protect against cyber threats [14,15].

2. Literature Review

Ali et al. underscore the escalating threat of financial fraud and the insufficiency of conventional detection techniques. The analysis of approximately 93 papers reveals that support vector machines (SVM) and artificial neural networks (ANN) are the most prevalent machine learning approaches employed to address fraud, particularly emphasizing credit card theft. Valuation measures, including accuracy, precision, recall, and AUC/ROC (Area Under the Receiver Operating Characteristic Curve), are frequently employed to evaluate model performance. Key challenges include data imbalance, feature selection, real-time detection capabilities, and model interpretability. The paper suggests that future research should focus on improving data quality, developing hybrid models, enabling real-time detection, enhancing model interpretability to address these gaps, and improving fraud detection systems [16,17].

In this study, the author has explored techniques for generating pertinent characteristics, pre-processing business data, and developing predictive models for fraud detection. The author will assess the efficacy of various learning methods, significance, and interpretability of various learning methods. Through the analysis of fraud patterns and trends, financial institutions and payment systems can enhance their resilience and flexibility in fraud detection. The project seeks to enhance the security of electronic payments and combat fraud in the digital age. This is the initial application of the model to detect fraudulent transactions [17]. The entity associated with a transaction is extracted from the dataset and incorporated into the model to generate predictions. Feedback is a critical factor in the development of a robust prediction model, and updates to the feature engineering (ML model) are contingent upon it [17,18].

The authors Bolton et.al [2] have investigated the multifaceted issue of fraud and the development of detection methods in response to the advancement of technology in their seminal paper. The author has used the statistical method for fraud detection. The author commences by defining fraud as "criminal deception," as defined by the *Concise Oxford Dictionary*. Note that fraud is an age-old issue, but modern technological advancements have expanded the methods and ease with which it can be perpetrated. False advertising is

employed to gain an unwarranted advantage. Traditional fraudulent activities, such as the laundering of currency, have been simplified, while new forms of theft, such as computer infiltration and mobile phone scams, have emerged [3,4,19].

The author has offered an anomaly-based detection method based on machine learning as a way to overcome the problems that come with traditional blacklisting when it comes to finding unknown malicious URLs. This all-around method finds and sorts different types of attacks, like phishing, spamming, and malware infections, by using a wide range of distinguishing factors, including textual patterns, network structures, content structure, DNS data, and network traffic. The study focuses on how useful new features like lexical, DNS, and link fame are for finding malicious URLs and specific types of attacks. Avoidance methods like redirects, link manipulation, and fast-flux hosting cannot evade this method. By being able to spot attacks, effective and proper defenses can be put in place, leading to better threat management. The high accuracy rates of the work are shown by the results, which are based on about 42,000 good URLs and about 33,000 bad URLs from the internet. The system can find harmful URLs over 98% of the time and tell the difference between attack types over 93% of the time [4,6,7].

The increasing exploitation of unauthorized credit card information by fraudsters, especially when financial institutions extend their services to semi-urban and rural areas, has led to significant financial loss and decreased user trust. This is the reason financial institutions are prioritizing the development of effective fraud detection systems. The efficacy of five distinct ML methods for the detection of credit card fraud is assessed in this study. Examples of these include Naive Bayes (NB), Random Forest (RF), Support Vector Machines (SVM), and Logistic Regression (LR). The study corrects the dataset's class mismatch and assesses the algorithm's efficacy with and without the Synthetic Minority Over-sampling Technique (SMOTE). The technique was developed and verified in Python using an API built using Flask and Streamlit, illustrating the models' practical use in the real world. The work adds value by emphasizing the necessity of resolving data imbalance in fraud detection and demonstrating the higher performance of the RF classifier when boosted with SMOTE [4].

The paper "Isolation Forest" addresses the critical need for effective anomaly detection algorithms across various application domains. Anomalies are data patterns deviating from normal instances that hold significant relevance in detecting fraudulent activities and identifying discoveries. Existing model-based techniques for anomaly identification frequently create profiles of typical occurrences and discover abnormalities based on deviations from these profiles. However, as the author has highlighted, such approaches have limitations, including suboptimal detection performance, computational complexity [20–23] in high-dimensional data, and large datasets. The quantitative properties of anomalies are minority instances with attribute values significantly different from normal instances. The proposed method constructs a tree structure (Isolation Tree or iTree) to effectively isolate each instance. Anomalies, being 'few and unusual,' are isolated closer to the tree's root, whereas regular points are isolated at deeper layers. The Isolation Forest technique produces a collection of iTrees for a given dataset and detects anomalies as cases characterized by short average path lengths. The approach is efficient and scalable, requiring just two parameters: the number of trees to generate and the sub-sampling length [24–26].

3. Research Methodology for the Proposed Work

This section covers the comprehensive approach used to look at fraud detection in electronic payment systems. Data collection, preprocessing methods, machine learning algorithms, model assessment measures, and validation processes are all included in the methodology (Figure 1).

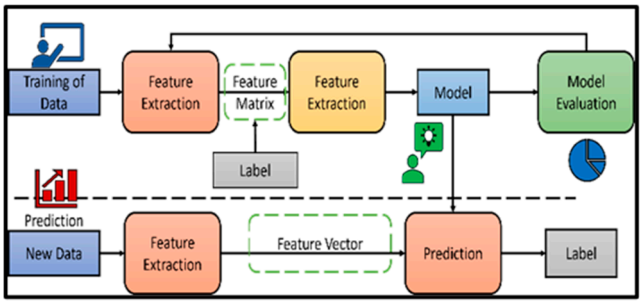


Figure 1. Flowchart of a supervised learning workflow, which shows how an algorithm is trained on labeled data and subsequently utilized to predict labels for new data.

The study utilizes an extensive artificial dataset comprising past transaction records extracted from electronic payment systems. The dataset encompasses various parameters, including transaction amount, type (e.g., cash-out or transfer), timestamp, sender (originator), and recipient (destination) details. The information is sourced from a reputable financial institution or payment processor, ensuring the legitimacy and reliability of the transactional data. The dataset includes a binary target variable indicating whether fraud occurred in each transaction or not. The dataset comprises a Range Index of 63,62,620 entries, ranging from 0 to 63,62,619, with a total of 11 columns.

3.1. Data Processing Techniques

To improve its quality and usefulness for modeling, the raw transactional data is rigorously pre-processed before analysis. Data preparation entails the following crucial steps [22,23]:

- Data Cleaning: Data cleaning procedures are used to correct mistakes, missing values, and inconsistencies that may be present in raw transactional data. In the dataset, the missing values are imputed using suitable techniques such as mean imputation or interpolation. The author identifies and handles anomalies and outliers to keep them from distorting the analysis's conclusions.
- Feature Engineering: Feature engineering is the procedure of adding new features or changing already existing features to extract useful data for fraud detection. This includes eliminating extraneous elements like transaction pace, frequency, and value relative to the account. To normalize numerical characteristics and lower the variance of variables, scaling and normalization procedures are applied.
- Feature Selection: The process of identifying the key characteristics that help in the detection of fraud occurs at specific stages of feature selection. To ascertain their significance, this technique combines statistical analysis, correlation analysis, and domain expertise [27]. To improve the efficacy and efficiency of the model, it eliminates irrelevant or unused elements from the data.

3.2. Machine Learning Algorithms

The study creates prediction models for fraud detection using a variety of machine-learning methods. Among these algorithms are as following:

- Logistic Regression (LR): Logistic regression is a traditional linear model that is applied to tasks involving binary classification [28]. The model calculates the likelihood that a transaction is fraudulent by analyzing its input data. LR is a statistical approach for simulating the chance that an input will fall into a certain class in binary classification. It represents the input for the various probabilities of 0,1 using the LR, commonly known as the sigmoid function. Logistic regression is different from linear regression, as shown in Figure 2.

- K-Nearest Neighbor (KNN): KNN is a popular machine learning technique for classification and regression applications. The basic notion underlying KNN is that related data points will have similar labels or values, as shown in Figure 3. During the training phase, KNN does not generate an explicit model but saves the complete training dataset. During the process of generating predictions, the method makes use of a particular distance metric, such as the Manhattan distance or the Euclidean distance, to determine the distance that exists between each point in the training dataset and the input data. After that, the method locates the 'k' places that are closest to the output label or value and then uses those locations to determine the output label or value [23].
- Random Forest: Random forests use ensemble learning techniques to boost prediction accuracy and resilience against overfitting by mixing many decision trees, as shown in Figure 4. The technique uses many decision trees to reduce complexity and improve prediction. Every tree in the forest is trained using a random subset of characteristics and a random portion of training data. The outputs of each tree are combined (e.g., by mean regression or voting for classification) to produce the final forecast during prediction. Decision trees are less obtrusive, less flexible, and less resilient than random forests [9].
- Support Vector Machines: SVM finds the ideal hyperplane in the feature space that separates fraudulent from legitimate transactions, as shown in Figure 5. SVM maximizes the margin between classes. SVM is a sophisticated supervised method of learning that may be employed in classification and regression. Figuring out which hyperplane splits the classes in each space, the best guarantees class separation [10]. The SVM algorithm controls decision parameters in an environment by using the kernel function to map input to the height of the class separation. In high-domain circumstances, SVM is useful, especially when there are more features than samples.

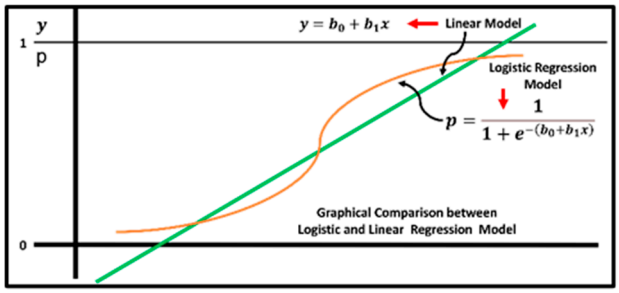


Figure 2. A comparison between linear and logistic regression models. Linear regression models the connection between a dependent variable and one or more independent variables.

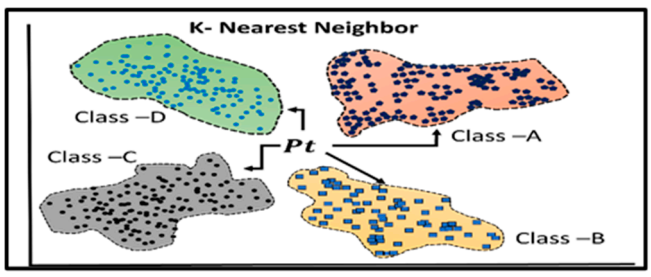


Figure 3. Representation of the K-Nearest Neighbor (KNN) technique, which may be used for classification or regression problems.

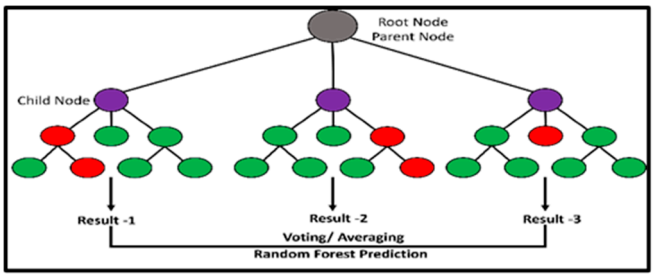


Figure 4. A simplified diagram of a random forest algorithm. Random forests are ensemble learning approaches that mix numerous decision trees to increase prediction accuracy while avoiding overfitting.

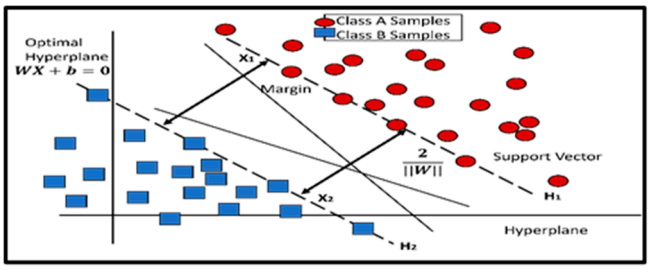


Figure 5. A visualization of a Support Vector Machine (SVM) with an optimal hyperplane, support vectors, and margin. Learning methods that combine multiple decision trees to improve prediction accuracy and avoid overfitting.

3.3. Model Evaluation Metrics and Validation Techniques

The performance and capacity for generalization of fraud detection algorithms are evaluated using a range of metrics and validation methods based on the following [24]:

- Accuracy: One of the most important assessment criteria is accuracy, which is the percentage of correctly identified transactions (fraudulent and lawful).
- Precision: The ratio of real positive predictions to all positive predictions indicates how well the model prevents false positives.
- Recall: The ratio of true positive forecasts to the total number of actual positive events is used to compute how well the algorithm detects fraudulent transactions.

3.4. Model Training and Hyperparameter Tuning

After the dataset has been feature-engineered and preprocessed, the next step is to train ML models on the prepared data. A training and validation set is created from a subset of the dataset that is reserved for model evaluation. The next step is hyperparameter optimization, which aims to optimize the model's performance. Grid search is an optimization strategy that finds the collection of hyperparameters that produces the highest performance by first looking at the hyperparameter space.

3.5. Interpretation of Results and Model Selection

The best model for fraud detection is chosen based on performance analysis assessment indicators. On performance measurement, select the optimal fraud testing model. Accuracy is simply one factor in the model selection process; other factors include recall trade-offs between accuracy and other factors.

4. Challenges

The current research on fraud detection faces several challenges. Imbalanced datasets, where fraudulent transactions are much less common than legitimate ones, can lead to biased models. Techniques such as under-sampling, oversampling, and artificial data

creation are used to balance the dataset, along with robust evaluation metrics like accuracy, recall, and F1-score. Extracting relevant features from raw data to create useful features for fraud detection can be complex. Exploratory data analysis (EDA), domain expertise, and feature selection methods such as dimensionality reduction or correlation analysis are leveraged to select meaningful features. Machine learning models may lack interpretability, making understanding the reasoning behind fraud predictions difficult [6].

Explainable models like decision trees (DT) and logistic regression (LR) techniques to explain model predictions, visualize decision boundaries, and feature importance are employed to understand model behavior. Maintaining low latency and high throughput while processing large volumes of transaction data in real time is challenging. Distributed computing frameworks such as Apache Spark, scalable algorithms, cloud-based solutions for hardware acceleration, and elastic scalability are implemented for computationally intensive tasks. Balancing the detection of fraudulent transactions with minimizing false alarms is a crucial step [5]. Anomaly detection algorithms are used to reduce false positives while maintaining high fraud detection rates. Regular updates to fraud detection algorithms, robustness techniques such as adversarial training, and anomaly detection algorithms are employed to identify patterns with the highest test accuracy (95.72%) out of the three models.

The research work has significant consequences for the identification of electronic payment fraud, utilizing machine learning algorithms and business data analysis to deepen our understanding of fraud indicative of adversarial attacks. Ensuring transparency and accountability of fraud detection [9]. Model development and decision-making processes, providing clear explanations of model predictions, ensuring fairness and transparency in model design and deployment, and validating models to ensure compliance with legal and ethical guidelines are necessary to address these challenges [10].

5. Results and Discussion

The results, as shown in Tables 1 and 2, of our analysis provide insight into the characteristics of fraud in electronic payments. Through a comprehensive dataset analysis, the author uncovered key themes, patterns, and relationships that characterize fraud and its detection. The analysis revealed that fraudulent transactions are more common during periods of peak business activity, suggesting that fraudsters may exploit these times to conceal their activities. A positive correlation was found between the destination's new and old balances and remittances, indicating the presence of uncertainty in fraudulent financial transactions.

Table 1. Training and test accuracy comparison between various algorithms.

Sr. No.	AI/ML/DL Algorithms		
	Algorithms	**Training Accuracy**	**Test Accuracy**
1	Logistic Regression	72.50%	71.27%
2	K-Neighbor Classifier	85.91%	75.51%
3	Random Forest (Default Algorithm)	85.91%	75.51%
4	Random Forest (Tuned Algorithm)	86.58%	78.72%
5	SVM	68.61%	69.15%
6	Decision Tree	75.14%	77.67%

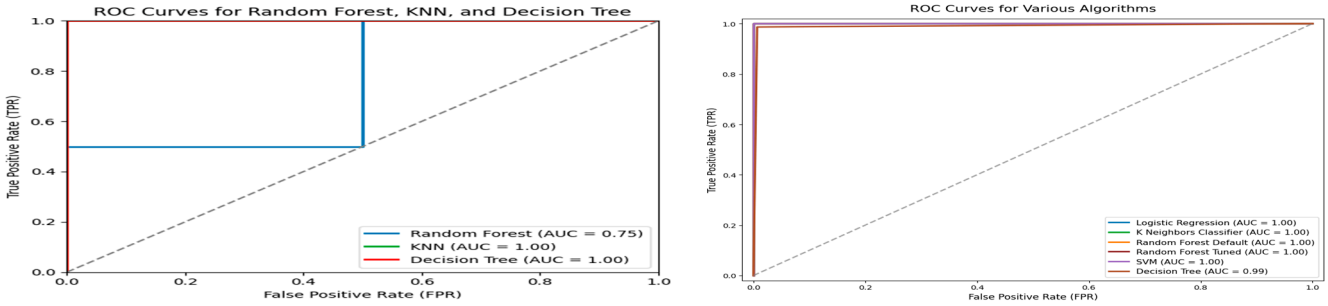
Table 2. Table showing the comparative analysis of different datasets: Random Forest, KNN, and Decision Tree.

	Random Forest	**KNN**	**Decision Tree**
Training Accuracy	93.87%	96.36%	96.87%

Table 2. *Cont.*

	Random Forest	KNN	Decision Tree
Test Accuracy	93.25%	95.37%	95.72%
Precision (Class 0)	0.98	0.98	0.97
Recall (Class 0)	1.00	0.98	0.99
F1 Score (Class 0)	0.99	0.99	0.99
Precision (Class 1)	0.98	0.92	0.97
Recall (Class 1)	0.87	0.92	0.96
F1 Score (Class 1)	0.92	0.91	0.93

Various machine learning algorithms, such as Logistic Regression, Decision Trees, Random Forests, Support Vector Machines (SVMs), and gradient boosting machines (GBMs), were trained and tested for fraud detection. Models were evaluated using performance criteria such as accuracy, precision, recall, F1 score, and AUC-ROC to establish their usefulness in detecting fraudulent activity, as shown in Figure 6, with random forests and GBMs consistently yielding superior results. Feature engineering significantly improved model performance, with features like exchange rates, balances, and business types contributing to better fraud detection. Despite the promising performance of machine learning models, challenges such as data inconsistencies, updated fraud strategies, and complex interpretation systems remain. By interpreting these results, we can identify viable solutions to reduce fraud and enhance the stability of the financial industry. The addition of features based on domain expertise and recognition of pertinent business traits, such as transaction rates, balances, and types, increases the distinctiveness of machine learning models.



(**a**) (**b**)

Figure 6. (**a**). The ROC and AUC show different algorithms: Random Forest, KNN, and Decision Tree. (**b**). The figure shows different AUC ROC for LR, KNN, RF, SVM, and Decision Tree.

Models like RF and GBM have shown high accuracy, precision, recall, AUC/ROC scores, and the importance of employing advanced methods to stay ahead of evolving fraud and prevent monetary losses. Our study contributes to existing literature by providing empirical evidence of ML models' effectiveness in fraud detection and assessing various algorithms. This aligns with industry practices that utilize ML and advanced analytics to detect unusual activities, supporting the industry's shift to data-driven fraud prevention. Our findings are practically significant, offering insights into effective fraud detection elements and procedures, useful for businesses aiming to boost security. The study's reliance on specific data poses limitations, as it may not fully represent the diversity of fraud in electronic payments. Given the constantly evolving nature of fraud, some changes may not be reflected in our dataset. Our multidimensional feature engineering method strengthens the model's discriminative capability and enhances its capacity to identify sophisticated fraud, suggesting that combining DL, vulnerability detection, and ML offers a robust approach to improving fraud detection.

6. Conclusions and Future Scope

Our study focuses on the use of machine learning and advanced analytics in the identification of electronic payment fraud. By examining company data and assessing the efficacy of diverse machine learning algorithms, we have discerned crucial characteristics and techniques effective in identifying fraudulent attempts. The goals of our research were to investigate the characteristics of commercial fraud, evaluate the efficacy of machine learning models in detecting fraud, and provide recommendations for developing fraud detection tools. Our findings suggest alternative approaches to fraud detection, addressing issues such as biased sampling. Practical applications include developing and applying fraud detection solutions leveraging advanced analytics and machine learning techniques to prevent financial losses in electronic payments. By sharing our expertise with organizations, we aim to reduce financial fraud risk and improve the security and integrity of electronic payments. Our research provides empirical data on the effectiveness of machine learning systems in identifying dubious transactions, optimizing algorithms for fraud detection.

Future research opportunities include developing more insightful intelligence models to comprehend the decision-making process behind fraud, enhancing transparency, and confidence. The author proposes examining online learning techniques to automatically update fraud detection technologies, exploring deep learning for fraud detection, improving data preprocessing to handle noisy or missing data, and creating a robust system for continuous monitoring and adjustment to accommodate new fraud strategies.

Author Contributions: A.S. (Ajay Sharma) conceptualized and supervised; S.S. contributed to analysis and validation; A.M. assisted in methodology and drafting; R.S. reviewed and edited; A.S. (Anang Suryana) supported validation and resources. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Available on request from the corresponding author.

Conflicts of Interest: The author Shamneesh Sharma was employed by the company byteXL TechEd Private Limited, Hyderabad, India. The authors A.S, A.M & R.S are employed in LPU Phagwara, Jalandhar, Punjab, India. The author Anang Suryana is employed in the Department of Electrical and Engineering, Nusa Putra University (Indonesia). All authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Modi, K.; Dayma, R. Review on fraud detection methods in credit card transactions. In Proceedings of the 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India, 23–24 June 2017; IEEE: Piscataway, NJ, USA, 2018; Volume 2018, pp. 1–5.
2. Bolton, R.J.; Hand, D.J. Statistical Fraud Detection: A Review. *Stat. Sci.* **2002**, *17*, 235–255. [CrossRef]
3. Ikeda, C.; Ouazzane, K.; Yu, Q.; Hubenova, S. New feature engineering framework for deep learning in financial fraud detection. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 10–21. [CrossRef]
4. Fayaz, F.A.; Malik, A.; Batra, I.; Ansarullah, S.I. A resilient overlay for human emotion recognition using mixed frameworks in machine-human interactions. *SN Comput. Sci.* **2024**, *5*, 414. [CrossRef]
5. Breiman, L. Random forests. *Mach. Learn.* **2001**, *45*, 5–32. [CrossRef]
6. Alshudukhi, K.S.; Ashfaq, F.; Jhanjhi, N.; Humayun, M. Blockchain-enabled federated learning for longitudinal emergency care. *IEEE Access* **2024**, *12*, 137284–137294. [CrossRef]
7. Ninama, H.; Raikwal, J.; Ravuri, A.; Sukheja, D.; Bhoi, S.K.; Jhanjhi, N.Z.; Elnour, A.A.H.; Abdelmaboud, A. Computer vision and deep transfer learning for automatic gauge reading detection. *Sci. Rep.* **2024**, *14*, 23019. [CrossRef] [PubMed]

8. Esenogho, E.; Mienye, I.D.; Swart, T.G.; Aruleba, K.; Obaido, G. A neural network ensemble with feature engineering for improved credit card fraud detection. *IEEE Access* **2022**, *10*, 16400–16407. [CrossRef]
9. Alkhalil, Z.; Hewage, C.; Nawaf, L.; Khan, I. Phishing attacks: A recent comprehensive study and a new anatomy. *Front. Comput. Sci.* **2021**, *3*, 563060. [CrossRef]
10. Gupta, B.B.; Tewari, A.; Jain, A.K.; Agrawal, D.P. Fighting against phishing attacks: State of the art and future challenges. *Neural Comput. Appl.* **2017**, *28*, 3629–3654. [CrossRef]
11. Alabdan, R. Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet* **2020**, *12*, 168. [CrossRef]
12. Dmitrienko, A.; Liebchen, C.; Rossow, C.; Sadeghi, A.R. On the (in)security of mobile two-factor authentication. In *Lecture Notes in Computer Science*; Springer: Berlin, Germany, 2014; Volume 8437, pp. 365–383. [CrossRef]
13. Sharma, A.; Guleria, V.; Jaiswal, V. The future of blockchain technology: Recent advancement and challenges. In *Studies in Big Data*; Springer: Cham, Switzerland, 2022; Volume 105, pp. 329–349. [CrossRef]
14. Sharma, A.; Pal, T.; Naithani, U.; Gupta, G.; Jaiswal, V. Emerging trends of big data in bioinformatics and challenges. In *Intelligent Data Analytics for Bioinformatics and Biomedical Systems*; Wiley: Hoboken, NJ, USA, 2024; pp. 265–290. [CrossRef]
15. Sharma, A.; Kala, S.; Kumar, A.; Sharma, S.; Gupta, G.; Jaiswal, V. Deep learning in genomics, personalized medicine, and neurodevelopmental disorders. In *Intelligent Data Analytics for Bioinformatics and Biomedical Systems*; Wiley: Hoboken, NJ, USA, 2024; pp. 235–264. [CrossRef]
16. Al-Hashedi, K. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Pattern Recognit. Lett.* **2021**, *40*, 100402. [CrossRef]
17. Choi, H.; Zhu, B.; Lee, H. Detecting malicious web links and identifying their attack types. In Proceedings of the 2nd USENIX Conference on Web Application Development (WebApps 11), Portland, OR, USA, 15–16 June 2011; Available online: https://www.usenix.org/events/webapps11/tech/final_files/Choi.pdf (accessed on 30 August 2024).
18. Cavusoglu, H.; Mishra, B.; Raghunathan, S. The effect of internet security breach announcements on market value. *Int. J. Electron. Commer.* **2004**, *9*, 70–104. [CrossRef]
19. Baesens, B.; Höppner, S.; Verdonck, T. Data engineering for fraud detection. *Decis. Support Syst.* **2021**, *150*, 113492. [CrossRef]
20. Noto, K.; Brodley, C.; Slonim, D. Anomaly detection using an ensemble of feature models. In Proceedings of the IEEE International Conference on Data Mining (ICDM), Sydney, Australia, 13–17 December 2010; pp. 953–958. [CrossRef]
21. Fawcett, T. An introduction to ROC analysis. *Pattern Recognit. Lett.* **2006**, *27*, 861–874. [CrossRef]
22. Sharma, A.; Kumar, R.; Jaiswal, V. Classification of heart disease from MRI images using a convolutional neural network. In Proceedings of the IEEE International Conference on Signal Processing, Computing and Control, Solan, India, 7–9 October 2021; pp. 358–363.
23. Sharma, A.; Kaur, D.; Gupta, A.; Jaiswal, V. Application and analysis of hyperspectral imaging. In Proceedings of the IEEE International Conference on Signal Processing, Computing and Control, Solan, India, 10–12 October 2019; pp. 30–35.
24. Lankadasu, N.V.Y.; Pesarlanka, D.B.; Sharma, A.; Sharma, S.; Gochhait, S. Skin cancer classification using a convolutional neural network: An exploration into deep learning. In Proceedings of the ASU International Conference on Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS 2024), Manama, Bahrain, 28–29 January 2024; pp. 1047–1052. [CrossRef]
25. Aldughayfiq, B.; Ashfaq, F.; Jhanjhi, N.Z.; Humayun, M. YOLO-based deep learning model for pressure ulcer detection and classification. *Healthcare* **2023**, *11*, 1222. [CrossRef] [PubMed]
26. Aldughayfiq, B.; Ashfaq, F.; Jhanjhi, N.Z.; Humayun, M. Explainable AI for retinoblastoma diagnosis: Interpreting deep learning models with LIME and SHAP. *Diagnostics* **2023**, *13*, 1932. [CrossRef] [PubMed]
27. Aherwadi, N.; Mittal, U.; Singla, J.; Jhanjhi, N.Z.; Yassine, A.; Hossain, M.S. Prediction of fruit maturity, quality, and its life using deep learning algorithms. *Electronics* **2022**, *11*, 4100. [CrossRef]
28. Ray, S.K.; Sinha, R.; Ray, S.K. A smartphone-based post-disaster management mechanism using WiFi tethering. In Proceedings of the 2015 10th IEEE Conference on Industrial Electronics and Applications (ICIEA), Auckland, New Zealand, 15–17 June 2015; pp. 966–971. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.