Safeguarding against Cyber Threats: Machine Learning-Based Approaches for Real-Time Fraud Detection and Prevention †

Vikas R. Shetty, Pooja R. and Rashmi Laxmikant Malghan *

Department of Data Science and Computer Applications, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, Karnataka, India; shettyvikas03@gmail.com (V.R.S.); poojar9199@gmail.com (P.R.)
* Correspondence: rashmi.malghan@manipal.edu; Tel.: +91-9742739015
† Presented at the International Conference on Recent Advances in Science and Engineering, Dubai, United Arab Emirates, 4–5 October 2023.

Abstract: The proliferation of internet services in various industries, especially the financial sector, has increased financial fraud. Fraud detection and prevention are critical to protecting both individuals and organizations from significant financial loss. However, the lack of publicly available datasets containing fraud is a major challenge. This study aims to address these issues using advanced machine learning techniques. Known for their ability to provide insight into data, decision trees are used for real-time fraud detection. In addition, deep learning techniques and artificial neural networks (ANN) are used to detect complex fraud patterns, while logistic regression is used to model the probability of fraudulent events. The accuracy of these methods, including decision trees, logistic regression, and ANN, is fully evaluated, with accuracies of 99.8%, 99.9%, and 99.94%, respectively. These findings provide valuable guidance for companies on choosing effective anti-fraud strategies and shed light on the adaptability of algorithms to real financial contexts, contributing to machine learning-based fraud detection.

Keywords: cyber security; fraud detection; artificial neural networks; logistic regression; machine learning

1. Introduction

Over the past few years, businesses, online services, and internet users have all grown significantly [1]. Online bill payment services, debit and credit card systems, and internet banking systems have all become essential parts of our lives because they make transactions convenient and eliminate the need for cash [2,3]. However, there is a significant risk of financial fraud and unauthorized payments despite the benefits of online transactions. Due to many financial scams, such as money laundering, fraud of insurance, identity fraud, fraudulent banking transactions, and others, users of the internet and online banking continue to experience challenges [4]. It is difficult and sophisticated to identify fraudulent financial activities. As innovation keeps on progressing, monetary fakes are likewise advancing, prompting an expansion in their event. Financial systems encounter a variety of deceptive activities, such as counterfeit accounts, fraudulent schemes, phishing attempts, the falsification of documents, deceptive loans, credit card deceptions, and internet banking swindles [5]. Financial institutions suffer from a decline in both customer confidence and financial stability as a result of these fraud offenses, which annually cost them millions of dollars [6].

The importance and uses of technologies like big data, cloud computing, and artificial intelligence (AI) have been heavily debated on a variety of platforms. However, their true value and capacity to successfully address problems in the real world are frequently unclear. The process of developing intelligent devices that can mimic human behavior and learn from experience is known as artificial intelligence (AI). Because of its distinctive qualities,
such as adaptability, scalability, and the ability to swiftly adapt to new and unfamiliar obstacles, machine learning techniques have found usage in a wide range of scientific domains. These methods have been used to solve a wide range of research problems by utilizing their inherent properties, and they have been implemented with success in numerous fields of science. The Table 1 below presents the literature review conducted for the study.

Table 1. Literature review.

<table>
<thead>
<tr>
<th>Paper Number</th>
<th>Dataset Used</th>
<th>Model Used</th>
<th>Reported Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[7]</td>
<td>Real-time credit card fraud detection</td>
<td>Convolution Neural Network</td>
<td>99%</td>
</tr>
<tr>
<td>[8]</td>
<td>Fraud Credit Card Identification Dataset</td>
<td>Naive Bayes</td>
<td>96.1%</td>
</tr>
<tr>
<td>[9]</td>
<td>Fraud Credit Card Identification Dataset</td>
<td>Logistic Regression</td>
<td>94.8%</td>
</tr>
<tr>
<td>[10]</td>
<td>NSL-KDD dataset</td>
<td>Restricted Boltzmann machine</td>
<td>97.5%</td>
</tr>
<tr>
<td>[11]</td>
<td>Fraud Credit Card Identification Dataset</td>
<td>K-Nearest Neighbor (KNN)</td>
<td>95.89%</td>
</tr>
<tr>
<td>[12]</td>
<td>Fraud Credit Card Identification Dataset</td>
<td>Random Forest</td>
<td>97.58%</td>
</tr>
<tr>
<td>[13]</td>
<td>Fraud Credit Card Identification Dataset</td>
<td>Sequential Convolutional Neural Network</td>
<td>92.3%</td>
</tr>
<tr>
<td>[14]</td>
<td>Credit card fraud detection dataset</td>
<td>Long Short-Term Memory</td>
<td>99.5%</td>
</tr>
<tr>
<td>[15]</td>
<td>a commercial bank B2C online transaction data</td>
<td>Convolutional Neural Network</td>
<td>91%</td>
</tr>
<tr>
<td>[16]</td>
<td>NSL-KDD</td>
<td>Deep Neural Network</td>
<td>75.75%</td>
</tr>
<tr>
<td>[17]</td>
<td>IEEE 118-bus and IEEE 300-bus</td>
<td>Conditional deep belief network</td>
<td>99.54%</td>
</tr>
<tr>
<td>[18]</td>
<td>KDD Cup 1999 dataset</td>
<td>Self-Taught Learning</td>
<td>98%</td>
</tr>
<tr>
<td>[19]</td>
<td>KDD Cup 1999 dataset</td>
<td>Denoising auto-encoder</td>
<td>95%</td>
</tr>
<tr>
<td>[20]</td>
<td>NS-3 traffic and NSL-KDD dataset</td>
<td>Deep belief network</td>
<td>99.43%</td>
</tr>
<tr>
<td>[21]</td>
<td>The credit card transaction dataset</td>
<td>DDNN</td>
<td>99.9422</td>
</tr>
</tbody>
</table>

2. Materials and Methods/Methodology

Financial data fraud detection is a critical cybersecurity challenge that both enterprises and people must face. Financial fraud has increased significantly as a result of the widespread use of online services and digital transactions, resulting in significant financial losses and potential harm to businesses and customers. To safeguard financial systems and maintain trust in digital transactions, it has become crucial to detect and prevent fraudulent activities in real time. This research, with a specific emphasis on logistic regression, decision trees, and artificial neural networks (ANN), is aimed at developing effective fraud detection models through the application of machine learning techniques. We want to use these algorithms to make fraud detection more accurate and efficient. This will make it possible to spot fraudulent activities early and take preventative measures to lessen their impact. In this study, the models’ performance is assessed by considering a range of metrics including the F1 score, accuracy, precision, and recall. The purpose of these metrics is to evaluate how well the models can correctly differentiate between fraudulent and non-fraudulent transactions. This evaluation offers a complete comprehension of their effectiveness. The analysis delves into investigating the influence of distinct characteristics and parameters on the overall performance of multiple models. Furthermore, it carries out a comparative evaluation to determine their respective effectiveness. The main focus of the study is to develop and evaluate fraud detection models using decision trees, logistic regression, and artificial neural networks. The main goal is to improve the accuracy and efficiency of fraud detection in financial data by using machine learning techniques on the Financial Fraud Dataset. This will ultimately lead to a better understanding and identification of fraudulent activities. The results of this study will aid in improving fraud prevention methods,
enabling timely identification and prevention of fraudulent activities for organizations and individuals. The purpose of this measure is to guarantee the safety of financial systems while upholding consumer confidence in online transactions.

2.1. Dataset Information

The “Financial Fraud Dataset” from Kaggle is a rich source of transaction details, account balances, transaction types, and fraud indicators. To build accurate and reliable fraud detection models, we employed essential feature engineering techniques, including numerical feature scaling, categorical variable encoding, handling missing data, and creating domain knowledge-driven derived features. This dataset offers a diverse array of attributes, including transaction type, oldbalanceOrg, newbalanceOrig, oldbalanceDest, and newbalanceDest. Its substantial size enables in-depth analysis of financial fraud activities. However, potential issues like class imbalance and missing data should be noted. This dataset empowers the training, evaluation, and comparison of effective fraud detection algorithms.

2.2. Feature Engineering

Feature engineering is essential for successful fraud detection in the “Financial Fraud Dataset”. We tackled missing values using regression-based imputation or K-nearest neighbors. Categorical variables like transaction types are one-hot encoded. To ensure consistent model performance, we scaled numerical attributes and created informative derived features based on domain knowledge, such as the transaction-to-balance ratio. Time-based features capture temporal patterns, enhancing detection. Accuracy, precision, recall, and F1-score parameters are taken into account during this iterative process. Overall, feature engineering boosts the data’s discriminatory power, improving fraud detection models by capturing crucial patterns and relationships.

2.3. Model Building

In the “Financial Fraud Dataset” phase of our fraud detection project, we wanted to build accurate and dependable machine learning models that can spot fraudulent transactions. We looked into three possible algorithms for this purpose: decision trees, logistic regression, and artificial neural networks (ANN). To build reliable fraud detection models, we make use of each algorithm’s advantages and traits.

2.3.1. Decision Trees

Decision trees are a widely used machine learning technique used for both classification and regression tasks. They provide a systematic method for selecting a set of inputs. This method results in a model that looks like a tree, where each internal node represents a function, each branch represents a decision based on that function, and each leaf node corresponds to a class label or predicted value.

The primary idea behind decision trees is to divide the data by the values of different features, with the goal of creating subsets that are as similar to the target variable as possible. The best split point for the most informative feature at each internal node is selected during this partitioning procedure.

Entropy and Gini Impurity

Take a look at a dataset called D, which has samples of k classes and Pi is the probability of a sample belonging to class I at a given node. The following is the definition of the D Gini impurity:

\[
Gini(D) = 1 - \sum_{i=1}^{k} p_i^2
\] (1)
A node with a uniform class distribution has the highest degree of impurity, while the lowest impurity is achieved when all records belong to the same class. The attribute with the least Gini impurity is chosen to split the node.

The Gini impurity is characterized as follows when a dataset, referred to as D, is divided into two subsets called D1 and D2 using an attribute A. The sizes of these subsets are denoted as n1 and n2.

\[
Gini_A(D) = \frac{n1}{n} Gini(D_1) + \frac{n2}{n} Gini(D_2)
\]  

(2)

In decision tree learning, a node is split by choosing the smallest GiniA(D) attribute. The branch impurity is subtracted from the original impurity to achieve attribute information gain, and the ideal distribution can also be identified by Gini gain. The Gini score is calculated according to the following formula:

\[
\Delta Gini(A) = Gini(D) - Gini_A(D)
\]

(3)

2.3.2. Logistic Regression

A popular binary classification statistical model that forecasts the likelihood of events falling into a particular class is logistic regression. It employs a sigmoid function with the formula:

\[
f(z) = \frac{1}{1 + e^{-z}}
\]

Here, z is a linear combination of the input variable and the weights (W1X1 W2X2...wnxn b) that correspond to them. It converts the input into a probability range of 0–1, interpreting it as the probability of belonging to the positive category. Practicing logistic regression involves finding the optimal weights and biases by minimizing the logarithmic loss, L (y, \(\hat{y}\)) = −[y × log (\(\hat{y}\)) (1 − y) × log (1 − \(\hat{y}\))]. Here, y is the right sign and \(\hat{y}\) is the probability of the predicted variable. For this purpose, maximum likelihood estimation (MLE) is often used, which optimizes parameters by gradient descent to iteratively update weights and biases. This basic algorithm has applications in various industries, making it a fundamental binary classification in machine learning.

Logistic regression, a popular binary classification algorithm, uses regularization techniques such as L1 (Lasso) and L2 (Crest) to avoid overfitting. L1 increases the penalty based on absolute weights, which favors sparsity and feature selection, while L2 increases the penalty based on squared weights, which favors lighter weights and reduces the influence of less informative features. Logistic regression produces interpretable results with coefficients, indicating the effect of the trait on the positive logarithms of the class. Evaluation metrics include precision, accuracy, recall, and receiver operating characteristic (ROC) curve. This method uses a sigmoid function to model the class probability, estimate optimal weights and biases using maximum likelihood estimation, and minimize log loss.

2.3.3. Neural Networks (ANN)

Artificial neural network (ANN), a subset of deep learning models inspired by biological neural networks, excels at tasks such as prediction and pattern recognition. ANNs consist of interconnected artificial neurons that process input data. Neurons or perceptions weigh the inputs, calculate the weighted sum, and pass it through an activation function due to non-linearity. Activation functions commonly used are ReLU, sigmoid, tanh, and Softmax. In propagation, data passes through the input, hidden, and output layers, and each neuron uses an activation function. During backpropagation, errors are propagated backward; gradients of weights and biases are calculated to update them using optimization algorithms such as gradient descent, improving network efficiency by avoiding over-configuration through regularization, pruning, and early termination.

To summarize, at the model construction stage of our technique, models for fraud detection were developed using artificial neural networks, decision trees, and logistic
regression. We optimized the hyperparameters, assessed the performance of the models using the right metrics, and made use of the advantages of each method in order to increase the accuracy of fraud detection. We were able to develop reliable models that are able to effectively identify fraudulent transactions and reduce financial risks thanks to this comprehensive approach.

3. Results

After constructing the models with decision trees, logistic regression, and artificial neural networks (ANN), we examined their performance and derived useful insights from the findings. A comprehensive overview of the observations and analysis produced by evaluating these models on the financial fraud dataset is provided in this section.

Several assessment criteria, including accuracy, recall, precision, and the F1 score, were utilized for evaluating the performance of the models for binary classification tasks. Accuracy evaluates overall correctness, precision represents the percentage of genuine positives among true positives, and recall assesses the proportion of correctly identified true positives. The F1 score provides a balanced average between precision and recall. A comprehensive examination of these measures was conducted to formulate the performance of the different models and identify their advantages and disadvantages. Cross-validation and hypothesis testing are examples of statistical tests that are used to see if one model performs significantly better than the others. Figure 1 below displays the confusion matrix for logistic regression and decision tree, while Figure 2 illustrates the training and validation accuracy for the artificial neural network (ANN), and Table 2 below shows the comparison of different models against different performance matrices.

![Figure 1. Confusion matrix for logistic regression and decision tree.](image1)

![Figure 2. Training and validation accuracy for ANN.](image2)
Table 2. Comparison of different models against different performance matrices.

<table>
<thead>
<tr>
<th></th>
<th>Decision-Tree</th>
<th>Logistic-Regression</th>
<th>ANN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>99.89%</td>
<td>99.90%</td>
<td>99.94%</td>
</tr>
<tr>
<td>F1 score</td>
<td>62.21%</td>
<td>79.49%</td>
<td>75.67%</td>
</tr>
<tr>
<td>Recall/Sensitivity</td>
<td>99.89%</td>
<td>99.93%</td>
<td>64.43%</td>
</tr>
<tr>
<td>Specificity</td>
<td>85.71%</td>
<td>72.51%</td>
<td>99.99%</td>
</tr>
<tr>
<td>Precision</td>
<td>99.99%</td>
<td>99.97%</td>
<td>91.66%</td>
</tr>
<tr>
<td>False Positive Rate</td>
<td>14.28%</td>
<td>27.48%</td>
<td>0.0077%</td>
</tr>
<tr>
<td>Negative Predictive Value</td>
<td>14.28%</td>
<td>49.79%</td>
<td>99.95%</td>
</tr>
<tr>
<td>False Discovery Rate</td>
<td>0.0025%</td>
<td>0.026%</td>
<td>8.33%</td>
</tr>
</tbody>
</table>

In conclusion, the model comparison and performance metrics offer valuable insights into the efficiency of the implemented strategies. The assessment criteria emphasize the models’ accuracy, recall, F1 score, and precision, providing a quantitative evaluation of their predictive capabilities. The comprehensive analysis enables an objective comparison of the models, which aids in determining the most effective strategy for detecting and preventing fraud. The foundation for future enhancements and advancements in the field of fraud detection is laid by the outcomes of these analyses, which both contribute to an overall comprehension of the performance of the models.

4. Conclusions

The subject of this research paper’s conclusion was “Safeguarding Against Cyber Threats: Methods Based on Machine Learning for Preventing and Detecting Fraud in Real Time”. The widespread use of online services and the rapid development of technology have both increased the likelihood of financial fraud but have also brought about significant benefits. It has been found that traditional rule-based methods for detecting fraud cannot keep up with the changing strategies used by cybercriminals. As a result, cutting-edge strategies that make use of machine learning algorithms have emerged as crucial tools in the fight against this growing threat.

The current study examined various machine learning techniques, including random forest, ANN, and logistic regression, with the goal of developing effective models for real-time fraud detection and prevention. The research made use of the Kaggle dataset on financial fraud, which provided useful insights into financial fraud activities. The dataset was utilized, and feature engineering methods were used to extract meaningful features that aid in accurately identifying fraudulent transactions.

In the experimentation phase, machine learning models including decision trees, ANNs, and logistic regression were built and trained using the chosen features. These models generated promising findings in terms of very accurate fraud detection and prediction. The decision trees method gave principles that could be comprehended for the aim of identifying fraud, whereas ANN exhibited its capacity to grasp complicated patterns and non-linear correlations in the data. The effectiveness of logistic regression in determining the likelihood of a fraudulent transaction was demonstrated. This study’s findings demonstrate the usefulness of machine learning-based fraud detection and prevention strategies. Organizations can improve their ability to detect and respond to fraudulent activities in real time, minimizing financial losses and safeguarding the interests of individuals and businesses by utilizing advanced algorithms and feature engineering techniques.

However, it is essential to keep in mind that there is no single strategy that can guarantee success against all forms of fraud. In order to stay ahead of emerging fraud strategies, continuous monitoring, model updates, and the incorporation of new data sources are essential. Any fraud detection system also ought to incorporate ethical considerations, privacy protection, and legal compliance.

The significance of machine learning-based strategies in the ongoing battle against financial fraud and cyber risks is highlighted by this study. Organizations can strengthen their defenses, safeguard their assets, and create a safer digital environment for individuals.
and businesses alike by combining the power of technology with robust algorithms. The future of fraud detection and prevention will be shaped by further research and development in this area by incorporating a hybrid approach and big data technologies, resulting in a more secure and resilient financial environment.

**Author Contributions:** Conceptualization, V.R.S. and R.L.M.; Methodology, P.R. and V.R.S.; Writing—Original Draft, V.R.S. and P.R.; Writing—Review and Editing, R.L.M.; Supervision, R.L.M.; Critical Revisions and Insights, R.L.M. 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:** Data are contained within the article.

**Conflicts of Interest:** The authors declare no conflicts of interest.

**References**


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.