International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 11, Issue 4, 2023

Fraud Detection in Banking Transactions Using Multi-Layer Perceptron and Recursive Feature Elimination

[1]**Chaitanya Vasamsetty**
Engineer sr,
Elevance Health, Atlanta USA
chaitanyavasamsetty1007@gmail.com
[2]**Sunil Kumar Alavilli**
Senior Engineer, Sephora USA
San Francisco, CA, USA
sunil.alavilli@gmail.com

[3]**Bhavya Kadiyala**
Business Intelligence Specialist,
Parkland Health and Hospital System,
Dallas, TX, USA
kadiyalabhavyams@gmail.com

[4]**Rajani Priya Nippatla**
Kellton Technologies Inc, Texas, USA
rnippatla@gmail.com

[5]**Subramanyam Boyapati**
American Express, Arizona, USA
subramanyam.boyapati86@gmail.com

[6]**Punitha Palanisamy**
Tagore Institute of Engineering and Technology,
Salem,India
Punithapalanisamy93@gmail.com

ABSTRACT:

Fraud detection in financial transactions is a critical task for ensuring security and trust in banking systems. With the increasing volume and complexity of transactions, detecting fraudulent activities requires sophisticated machine learning techniques that can identify subtle patterns indicative of fraud. This study introduces a Multi-Layer Perceptron (MLP) augmented by Recursive Feature Elimination (RFE) fraud detection model for banking transactions. Finding fraudulent transactions based on important characteristics including transaction amount, customer information, payment method, and transaction time is the main goal. By removing redundant or unnecessary variables, RFE is used to choose the most pertinent features, greatly enhancing the model's performance. After using RFE, the accuracy increased significantly from 0.95 to 0.97 and Cohen's Kappa improved from 0.89 to 0.92. Furthermore, recall and precision rise, suggesting improved fraud transaction detection. The study shows that among the most important characteristics in fraud detection are transaction type, transaction value, and client age. Besides establishing the foundation for advanced feature selection research for the forthcoming trend in fraud, this paper emphasizes the importance of feature selection to improve model performance.

Keywords: Cohen's Kappa, Fraud Detection, Multi-Layer Perceptron, Recursive Feature Elimination, Transaction Classification, Stochastic Gradient Descent.

1. INTRODUCTION

The increasingly sophisticated nature of fraudulent activities and the much wider reach of digital transactions has made detection of fraud in financial transactions very difficult for banks [1], [2]. It is difficult for traditional rule-based systems to detect the complexity of frauds engineered through the vast outreach of internet-based banking, mobile payments, and e-commerce [3], [4]. Institutions are under great pressure to detect fraud and act upon it in a timely manner to protect customers' funds and maintain confidence. [5], [6]. However, available approaches are often ineffective in recognizing new schemes of fraud or in adapting to the clever tactics employed by the devious criminal. [7] There is therefore a need for advance, data-driven techniques that can ensure security and integrity of financial transactions due to their capability to provide better effective fraud detection.

Existing fraud detection systems in the banking sector primarily rely on rule-based approaches, which use predefined rules to flag potentially fraudulent activities [8], [9]. These systems, while effective in detecting known types of fraud, struggle to adapt to evolving fraud patterns and emerging threats. Machine learning (ML)

techniques have been increasingly adopted in recent years [10]. Supervised learning models, such as decision trees, logistic regression, and support vector machines, are commonly used to classify transactions as legitimate or fraudulent based on historical data [11], [12]. Unsupervised learning techniques like clustering and anomaly detection have been explored to identify novel fraud patterns without relying on labelled data [13], [14]. While these methods have shown improvements in detecting fraud, they often require manual feature engineering and may suffer from issues like overfitting and high false positive rates. Recent efforts focus on optimizing these techniques and integrating more sophisticated algorithms to improve accuracy and adaptability in real-world applications.

Many problems still reduce the efficiency of machine learning techniques in real-world applicability despite the increasing number of applications in fraud detection [15], [16]. The main issue here is the dependence on handcrafted features that may not appropriately characterize the complex and ever-changing nature of fraud. Moreover, many models suffer from a poor generalization; they may fit well to training data but fail to recognize fraud patterns that remain hidden from view [17]. Besides, high false-positive rates are yet another issue that leads to needless alerts and damages user confidence [18]. Most systems also suffer from class imbalance, which causes the model to be biased toward the majority class since fraudulent transactions constitute only a small minority of the overall data [19], [20]. Such weaknesses signify urgency to create a model that is more robust and flexible for learning from data, thereby reducing reliance on human intervention in feature selection. Hence, this work presents a fraud detection methodology-a combination of Recursive Feature Elimination and Multi-Layer Perceptron-to enhance detection performance and automatically identify the most relevant features. This approach aims to reduce false positives, enhance classification performance, and be scalable to accommodate changing fraud scenarios.

Moreover, the integration of feature selection techniques such as Recursive Feature Elimination (RFE) with advanced neural network models like Multi-Layer Perceptrons (MLP) offers a promising direction to address these challenges by improving model interpretability and computational efficiency [21]. Feature selection not only helps in reducing the dimensionality of the data but also enhances the generalization capability of the model by eliminating noisy or irrelevant attributes [22]. This is particularly important in fraud detection, where the data is often high-dimensional and imbalanced, and where subtle changes in feature importance can significantly impact the identification of fraudulent transactions [23]. Recent studies have demonstrated that combining feature selection with deep learning approaches leads to better detection rates and lower false positive alerts, which are crucial for operational effectiveness and customer trust [24]. Therefore, this paper's methodology leveraging RFE and MLP aligns with the evolving landscape of fraud detection research, aiming to develop more adaptive, accurate, and scalable models [25].

The proposed approach also addresses the critical issue of class imbalance by focusing on the most relevant features, which improves the detection of rare fraudulent instances without overwhelming the model with majority class data [26]. By prioritizing important transaction characteristics, the model can more effectively learn from limited fraud examples and reduce false alarms [27]. Additionally, incorporating Recursive Feature Elimination aids in streamlining the computational process, making the model more efficient for real-time fraud detection scenarios [28]. This efficiency is essential for banks that require prompt responses to suspicious activities to minimize financial losses and customer inconvenience [29]. Ultimately, the combination of MLP and RFE represents a significant advancement toward more reliable and scalable fraud detection systems capable of adapting to evolving fraudulent behaviors [30].

1.1. Problem statement

Conventional models face difficulties while processing huge volumes of complex, unbalanced transaction data, and many of the traditional methods are unable to detect minute patterns and irregularities indicative of fraud [31]. Another difficulty faced by the existing models is overfitting, where a model learns patterns from the training data too well and fails to generalize on data it has never seen [32]. Also, traditional methods' lack of automated feature selection techniques can lead to inefficiencies since redundant and irrelevant features might hamper computation efficiency and performance [33], [34].

1.2. Objective

- Develop a Multi-Layer Perceptron (MLP) model for fraud detection in banking transactions, focusing on capturing complex patterns indicative of fraudulent activity.
- Utilize Recursive Feature Elimination (RFE) to select the most relevant features from transaction data, optimizing the model's performance and reducing overfitting.
- Enhance the accuracy and efficiency of fraud detection by minimizing false positives and false negatives, improving the security of banking transactions.

The rest of the paper is organized as follows. Section 1 with the introduction. Section 2 will discuss the Theoretical Background. Section 3 presents the Methodology and Section 4 highlights the results. Section 5 concludes.

2. LITERATURE REVIEW

With artificial intelligence, machine learning, and cloud computing creating new paradigms, healthcare, finance, and cybersecurity are among those industries that have recently assumed importance in these developments [35]. Deep learning approaches have shown significant advances in performance metrics such as accuracy and efficiency over classical methods [36]. Interpretability and prediction accuracy in healthcare data analysis have been enhanced by developing cloud-based architectures along with machine learning models like Generalized Additive Models and Stochastic Gradient Boosting [37]. Mixed-method studies analyzed access and cost reductions in urban and rural economies using regression models and financial inclusion indices to assess the impact of cloud-based digital banking on income equality [38]. Machine learning combined with econometric modeling has been applied to study the effect of internet-inclusive finance on rural economies and financial inclusion through mobile internet access [39].

Cybersecurity in cloud computing has received increased attention [40]. Data security issues have been studied through authentication and access control techniques such as biometric identification, role-based access control, and multi-factor authentication [41]. Minimizing risks in cloud environments can be approached via machine learning-based anomaly detection and blockchain-based access control [42]. Complex anomaly detection systems using SE-PSO-enhanced Sigmoid-LeCun Temporal Convolutional Networks embedded within Attribute-Based K-Anonymity for data anonymization have been proposed [43]. Methods like Cluster Evaluation Method and Identity-Chain Technology aim to enhance performance and security of cloud-based financial systems [44]. These studies highlight the growing reliance on AI-based techniques for data security and cyberthreat mitigation in cloud environments [45].

Various approaches have been applied to financial analytics to improve risk and fraud prediction [46]. Deep learning models such as CNNs and RNNs have been shown to enhance fraud detection by analyzing large financial datasets [47]. Fused machine learning architectures combining neural networks, decision trees, and support vector machines have been developed to optimize accuracy in e-commerce fraud detection [48]. Integrations of Monte Carlo simulation, deep belief networks, and Bayesian signal processing have improved financial risk modeling in cloud applications [49]. To handle class imbalance in fraud detection, Attention-Based Isolated Forest integrated with ensemble machine learning algorithms like Random Forest and AdaBoost has been employed [50].

The potential of IoT and federated learning methodologies has been explored in various fields [51]. Optimization of IoT analytics focusing on reduced latency, improved model accuracy, and cost effectiveness has been achieved through federated learning and robust workflow orchestration [52]. Hybrid neural-fuzzy learning models have been developed for enhancing diagnostic accuracy using real-time IoT data on cloud platforms [53]. Cloud finance models for sustainable smart city growth have been studied using Principal Component Analysis and Confirmatory Factor Analysis to improve resource management [54]. Integrated AI and machine learning frameworks for secure financial data sharing over hybrid cloud platforms have enhanced fraud detection, decision-making, and regulatory compliance [55].

Research has also focused on the role of cloud IoT-enabled digital financial inclusion in mitigating income inequality and supporting sustainable urban development [56]. Cloud-based financial analytics platforms deploying techniques like ELECTRA, t-SNE, CatBoost, and Genetic Algorithms have been applied to optimize real-time financial decision-making [57]. Fraud detection models combining neural networks with algorithms such as Harmony Search have achieved near-perfect classification using sequential models and decision tree classifiers [58]. Cutting-edge technologies have been utilized to streamline eCommerce, finance, and cloud computing processes [59]. Studies employing blockchain, smart networks, and cloud computing indicate improvements in resource management and transaction security [60]. Trustworthiness of Infrastructure as a Service platforms has been enhanced through real-time monitoring, predictive maintenance, and AI-driven anomaly detection to reduce financial risks [61]. AI-driven decision-making processes using Hierarchical Event-Driven Stochastic Networks, Covariance Matrix Adaptation Evolution Strategy, and Self-Organizing Neural Networks have demonstrated increased scalability and adaptability in cloud computing and finance [62].

3. PROPOSED METHODOLOGY

The proposed methodology for detecting fraud in financial transactions serves as a systematic organized procedure is shown in Fig. 1. The method includes collection of information from banking transaction records, which in turn serves as the basis of the whole procedure. Here, the notion is that thorough data preparation is the act of preparing acquired data for modeling through actions like cleansing data, feature engineering, or encoding categorical variables. Feature selection is then conducted using RFE to eliminate redundant or unnecessary features in order to ensure that only the most crucial features are used for model training. Subsequently, it deploys the model on AWS for high availability and scalability.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 4, 2023

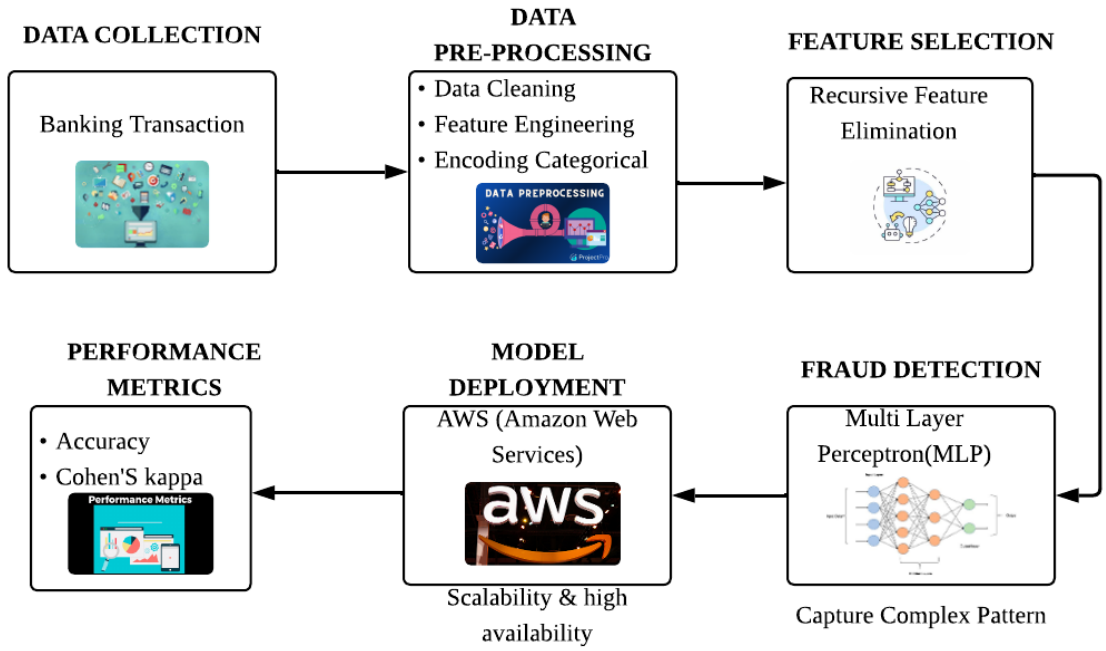

Figure 1: Fraud Detection System Workflow

The detection of fraud is performed using an MLP that learns complex patterns in the data and classifies transactions as fraudulent or non-fraudulent. This model performance is evaluated using metrics such as accuracy and Cohen's Kappa that lend insight into fraud detection capabilities. Thus, this mechanism guarantees a very reliable and scalable mechanism for real-time detection of fraud in financial transactions.

3.1. Data Collection:

Data collection is perceived as the first and most important phase of any machine learning process. This phase focuses on gathering financial transaction data from a variety of sources, including bank systems, transaction logs, or client activity logs. The important characteristics of these data usually include:- Transaction ID: acting as a unique identifier for each transaction; Customer Information: including Customer ID, Age, Account Type, and which adds context about the customer involved; Transaction Amount: denoting the monetary value of each transaction, with larger amounts being possible indicators of fraud; Payment Method: indicating whether the transaction was made using a debit card, credit card, or bank transfer, with regard to the possibility of each method being prone to fraud risk; and Fraud Indicator: a binary target label indicating 0 for legitimate transaction and 1 for fraudulent transaction.

3.2. Data Pre processing

3.2.1 Data Cleaning : Addressing problems that can skew machine learning model training, such as duplicates, missing data, and outliers, is known as data cleaning. Resolving these problems is essential to guaranteeing precise model predictions.

Managing Missing Data: Prior to training a model, it is necessary to resolve missing values, which are prevalent in real-world datasets. Various methods can be employed to impute or eliminate missing data, depending on whether the characteristic is categorical or numerical.

Median Imputation: The median of the non-missing values can be used to fill in the missing values for numerical features. When the missing information is random and does not induce bias, this method is straightforward but effective.

$$\text{Imputed Value} = \frac{\sum \text{Non-missing Values}}{\text{Number of Non-missing Values}} \quad (1)$$

Eliminate Outlier: Outliers could also bias statistical analysis and affect model training. To find outliers, the z-score is calculated:

Z-score method: Outliers are defined as any data points that fall below the definite threshold.

$$Z = \frac{(X - \mu)}{\sigma} \quad (2)$$

3.2.2 Feature Engineering

Feature Engineering preparing input data while feature engineering converts unstructured data into useful features that may help the model in pattern recognition, particularly in the case of fraud detection. Feature

engineering includes the creation of new features or the modification of existing ones to better performance of models and help the algorithm identify some of the significant indicators of fraudulent activity.

Transaction Frequency: Transaction Frequency is one of the most important scannable components of fraud detection; it might also be understood as the number of transactions a customer has made within a specified period. A fraudster often does more transactions within a short time span to test out several types of indicated fraud operations. Thus, this feature might also act as a warning sign of the abnormal activity.

Transaction frequency is the number of transactions by a customer in a particular timeframe, for example: in a day, week, or month, etc.

$$\text{Transaction Frequency} = \frac{\text{Number of Transactions}}{\text{Time Period}} \quad (3)$$

3.2.3 Encoding Categorical Variables

Categorical variables (such as Payment Method or Customer Type) must be converted to numerical format since most machine learning methods require numerical input. Popular means of encoding categorical variables are One-Hot Encoding and Label Encoding. In One-Hot Encoding a binary column (0 or 1) is created for every category in a categorical feature. For example, the three categories of the payment method variable-banking transfer, debit card, and credit card-would have been converted into three columns. Hence, a payment method of "Credit Card" will get encoded into [1,0,0]; "Debit Card" will be [0, 1, 0]; and "Bank Transfer" will be [0, 0, 1].

$$\text{Payment Method (Credit Card)} = [1,0,0] \quad (4)$$

3.3. Feature Selection

Recursive Features Elimination (RFE)

In kind of decision, RFE is a feature selection technique that eliminates features from the model recursively and checks the performance for each removal. The procedure begins with all features and removes the least important ones until the desired number of features is reached. In this way, RFE helps keep only the most important features to ensure that the model works well without overfitting.

The RFE procedure: First start from every feature in the model, meaning all features have been included in the model, and RFE evaluates how important each feature is with respect to the model's performance.

Performance analysis: RFE creates a model and assesses the strength of that model with some performance metric such as cross-validation score, accuracy, or F1-score. This is then trained on the former store of features to be evaluated.

Shed the least significant feature: The feature that would have the least impact on the performance of the model is then discarded.

Repeat: This process is repeated, rebuilding the model with the remaining features until the maximum number of features required is reached.

Feature Ranking :

Evaluation for RFE - In RFE, the weight of each feature was used to assess its significance (for linear models like the logistic regression model). The coefficient associated with the feature in a model is often called the weight in case of a logistic regression model. For instance, for logistic regression, a feature's importance is exactly proportional to the size of its weight.

$$\text{Feature Importance} = |\ \text{Weight}_i\ | \quad (5)$$

Weight_i is the term that corresponds to feature i in the model.

The absolute value of weight represents the importance of the feature. Features are considered important when their weights are absolutely greater.

RFE ranks features based on these feature weights in order to identify the least significant ones, which are eliminated in subsequent iterations.

3.4. Fraud Detection Model:

The MLP is a fraud detection model. A MLP is applied in this process stage depending on selected characteristics to detect fraudulent transactions. It is one of the prettiest and most popular feedforward neural network types in machine learning, and MLP is also very good in the extraction of really complex patterns from tabular data. With its exceptional ability to capture non-linear relationships between input data, it can be excellent for fraud detection applications because many times the complex interactions between features actually indicate the presence of a fraudulent action.

Multi-Layer Perceptron based Fraud Detection:

Input Layer: Transaction amount, client details, transaction time, payment method, and all feature-engineered characteristics are currently included in the features fed into the input layer of MLP. Within this layer, each neuron corresponds to one input variable and each similarly relates to another neuron. The model may thus develop more complicated relations between the input features by linking these neurons with the neurons in the

hidden layers. The input layer contains all the data that a model needs for further discovery and prediction as it forms the starting point from which data moves through the neural network.

Hidden Layer: Hidden layers in an MLP extract complex representations and patterns from the input data. These layers transform the data so that the model can recognize complex and often non-linear interactions. The weights w_{ij} define how strongly a neuron in a given hidden layer is connected to every neuron in the layer above it. The activation function applied, such as Sigmoid, imparts non-linearity to the network, allowing the model to gain an understanding of more complex patterns.

The output of a hidden layer neuron is expressed as:

$$h_i = \sigma\left(\sum_{j=1}^{n} w_{ij}x_j + b_i\right) \tag{6}$$

The output h_i for the i-th hidden neuron. The input feature x_j and the hidden neuron h_i with weight w_{ij}. The bias term associated with the i-th neuron is b_i. The activation function, σ, is the Sigmoid and adds the non-linearity in managing complex relationships. Since fraud usually generates non-linear patterns, applications of Sigmoid help guarantee that the model is equipped to find non-linearities in the data, absolutely fundamental for identifying fraudulent activities.

Output Layer: In the output layer, a binary classification represents a transaction as being either fraudulent (1) or not (0). The output layer has only one neuron because fraud detection is a binary classification task. The weighted sum of its inputs is converted into a probability from 0 to 1 by the application of the Sigmoid function by this output neuron. This probability indicates the possibility of fraudulence, where a value close to 1 means higher chances of fraud and closer to 0 means a valid transaction.

The equation for the output layer is:

$$\hat{y} = \sigma\left(\sum_{i=1}^{m} w_i h_i + b\right) \tag{7}$$

This is the expected probability $\hat{y}$ of fraud in a range of 0-1. The prior hidden layer output and the weights are denoted as h_i and w_i. The bias term for the output neuron is denoted as b. The input combinations that are passed through the Sigmoid activation function σ to produce a probability are defined by

The definition of the sigmoid function is:

$$\sigma(x) = \frac{1}{1 + e^{-x}} \tag{8}$$

It ensures that its output would be restricted to between 0 and 1 probability values, where 0 presents a case of no fraud while a case of a score close to 1 represents high possibilities of fraudulently obtaining what was honest-to-goodness earned.

The training of an MLP involves the adoption of a Stochastic Gradient Descent (SGD) optimisation to adjust the weights w_{ij} and biases b_i. In binary classification problems like fraud detection, a loss function typically Binary Cross-Entropy needs to be minimized.

The Binary Cross-Entropy Loss is computed as follows:

$$\mathcal{L} = -[y\log(\hat{y}) + (1 - y)\log(1 - \hat{y})] \tag{9}$$

The loss function measures the distance between the predicted outcome and the actual labels, and the model adjusts weights and biases to minimize this error. y denotes the actual label (0 for non-fraudulent and 1 for fraudulent); $\hat{y}$ indicates the predicted likelihood of fraud.

4. RESULTS AND DISCUSSIONS:

In the Results and Discussion section, the efficacy of the fraud detection model is validated considering a dataset of banking transactions where transaction amount, client particulars, payment types, and transaction time are there. The results show that model accuracy and performance have been improved using feature selection methods such as RFE. The dataset was then used to analyze these transactions to determine whether they were fraudulent.

Table 1: Feature Importance Scores

Feature	Importance Score
Transaction Amount	0.45
Transaction Type	0.38
Customer Age	0.3
Payment Method	0.25
Transaction Time	0.22

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 4, 2023

Previous Fraud History	0.18

Table 1 and Figure 2 summarize the importance score to the fraud detection model. According to the table, the highest rank of 0.45 in fraud detection belongs to transaction amount. Following this, the most important among factors is transaction type, with a score of 0.38. Likewise, customer age is 0.3 and payment method is 0.25. The least relevant is an 0.18, previous fraud history; next is transaction time; and so on. This distribution highlights the features most relevant to the detection of fraudulent transactions.

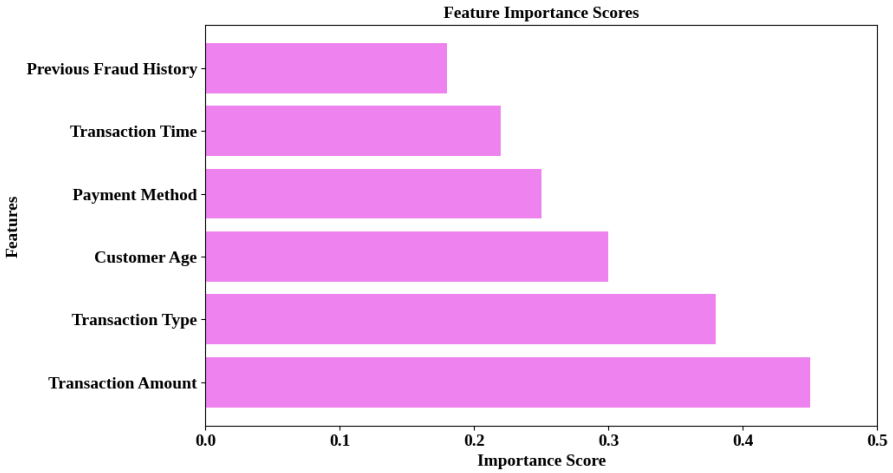

Figure 2: Feature Importance Score**.**

Table 2: **Performance Evaluation**

	Without RFE	With RFE
Accuracy	0.95	0.97
Cohen's Kappa	0.89	0.92
Precision	0.94	0.96
Recall	0.92	0.95
F1-Score	0.93	0.95
AUC-ROC	0.96	0.98

Both Tab. 2 and Fig. 3 display a comparison of the performance of the fraud detection model with and without RFE. Under all of the metrics used, the recursive feature elimination model outperformed the one without RFE processing. An increase in accuracy from 0.95 to 0.97 indicates an overall better performance of feature selection. The increase in Cohen's Kappa from 0.89 to 0.92 indicates greater agreement between actual and projected values.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 4, 2023

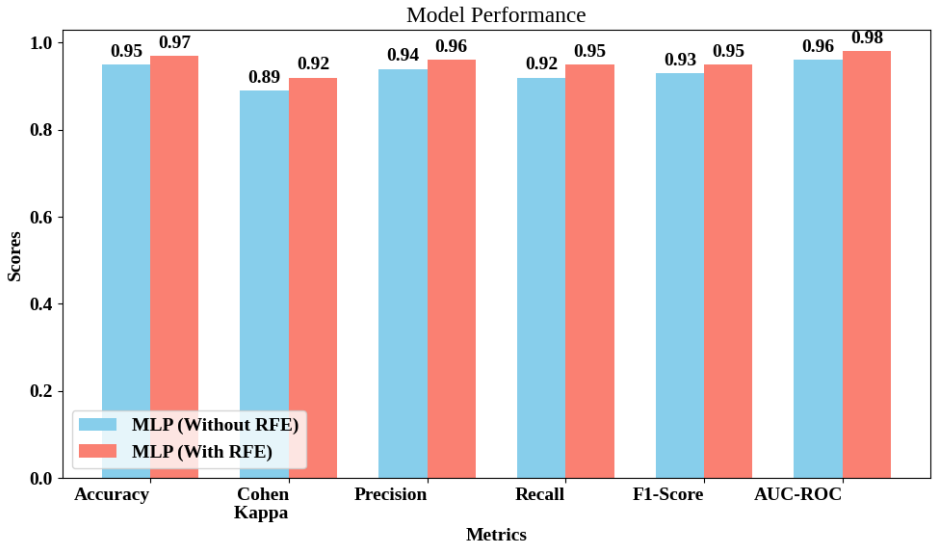

Figure 3: Performance Evaluation

In parallel, improved performance in precision, from 0.94 to 0.96, and in recall, from 0.92 to 0.95, indicates enhanced balance concerning false positives and false negatives. More support for the argument that RFE has improved model performance comes from an increase in F1-Score, from 0.93 to 0.95, and in AUC-ROC score, from 0.96 to 0.98.

5. CONCLUSIONS

This study demonstrates RFE improves the performance of a MLP model for fraud detection in banking transactions. The model was facilitated in improving its fraud detection capabilities by focusing on the most significant features as proved by the significant increase in accuracy from 0.95 to 0.97 and Cohen's Kappa from 0.89 to 0.92 due to RFE. The results indicate that transaction type, transaction value, and age of the client were found to be the most important characteristics, thus emphasizing the pivotal role of these in distinguishing between genuine and fraudulent transactions. For real-time fraud detection systems, the use of feature selection was instrumental in providing better generalization and lesser data complexity. RFE enhancing performance shows the importance of feature engineering and selection with respect to forecast accuracy. In the future, the work will focus on evolving even better techniques to prevent the model from fading with new fraud configurations in dynamic financial settings, combining advanced feature selection techniques like LASSO regularization or genetic algorithms.

REFERENCES

[1] Rawat, S., Rawat, A., Kumar, D., & Sabitha, A. S. (2021). Application of machine learning and data visualization techniques for decision support in the insurance sector. International Journal of Information Management Data Insights, 1(2), 100012.

[2] Srinivasan, K., Chauhan, G. S., Jadon, R., Budda, R., Gollapalli, V. S. T., & Kurunthachalam, A. (2022). Secure healthcare data storage and access control in cloud computing environments using AES and ECC encryption. International Journal of Information Technology & Computer Engineering, 10(3).

[3] Hewiagh, A., Ramakrishnan, K., Yap, T. T. V., & Tan, C. S. (2021). Waste management system fraud detection using machine learning algorithms to minimize penalties avoidance and redemption abuse. Recycling, 6(4), 65.

[4] Radhakrishnan, P., & Padmavathy, R. (2019). Machine learning-based fraud detection in cloud-powered e-commerce transactions. International Journal of Engineering Technology Research & Management, 3(1).

[5] Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. Sensors, 22(19), 7162.

[6] Musham, N. K., & Aiswarya, R. S. (2019). Leveraging artificial intelligence for fraud detection and risk management in cloud-based e-commerce platforms. International Journal of Engineering Technology Research & Management, 3(10)

[7] Mallidi, M. K. R., & Zagabathuni, Y. (2021). Analysis of Credit Card Fraud detection using Machine Learning models on balanced and imbalanced datasets. International Journal of Emerging Trends in Engineering Research, 9(7).

[8] Musam, V. S., & Rathna, S. (2019). Firefly-optimized cloud-enabled federated graph neural networks for privacy-preserving financial fraud detection. International Journal of Information Technology and Computer Engineering, 7(4).

[9] Ameli, A., Ayad, A., El-Saadany, E. F., Salama, M. M., & Youssef, A. (2020). A learning-based framework for detecting cyber-attacks against line current differential relays. IEEE Transactions on Power Delivery, 36(4), 2274-2286.
[10] Deevi, D. P., & Padmavathy, R. (2019). A hybrid random forest and GRU-based model for heart disease prediction using private cloud-hosted health data. International Journal of Applied Science Engineering and Management, 13(2).
[11] Singh, A., & Jain, A. (2019). Adaptive credit card fraud detection techniques based on feature selection method. In Advances in Computer Communication and Computational Sciences: Proceedings of IC4S 2018 (pp. 167-178). Springer Singapore.
[12] Vallu, V. R., & Arulkumaran, G. (2019). Enhancing compliance and security in cloud-based healthcare: A regulatory perspective using blockchain and RSA encryption. Journal of Current Science, 7(4).
[13] Alharbi, A., Alshammari, M., Okon, O. D., Alabrah, A., Rauf, H. T., Alyami, H., & Meraj, T. (2022). A novel text2IMG mechanism of credit card fraud detection: A deep learning approach. Electronics, 11(5), 756.
[14] Gudivaka, R. L., & Mekala, R. (2018). Intelligent sensor fusion in IoT-driven robotics for enhanced precision and adaptability. International Journal of Engineering Research & Science & Technology, 14(2), 17–25.
[15] Xiuguo, W., & Shengyong, D. (2022). An analysis on financial statement fraud detection for Chinese listed companies using deep learning. Ieee Access, 10, 22516-22532.
[16] Basani, D. K. R., & RS, A. (2018). Integrating IoT and robotics for autonomous signal processing in smart environment. International Journal of Computer Science and Information Technologies, 6(2), 90–99. ISSN 2347–3657.
[17] Shobana, G., & Umamaheswari, K. (2021, January). Forecasting by machine learning techniques and econometrics: A review. In 2021 6th international conference on inventive computation technologies (ICICT) (pp. 1010-1016). IEEE.
[18] Peddi, S., & Aiswarya, RS. (2018). Securing healthcare in cloud-based storage for protecting sensitive patient data. International Journal of Information Technology and Computer Engineering, 6(1)
[19] Sourabh, & Arora, B. (2022). A Review of Credit Card Fraud Detection Techniques. Recent Innovations in Computing: Proceedings of ICRIC 2021, Volume 1, 485-496.
[20] Natarajan, D. R., & Kurunthachalam, A. (2018). Efficient Remote Patient Monitoring Using Multi-Parameter Devices and Cloud with Priority-Based Data Transmission Optimization. Indo-American Journal of Life Sciences and Biotechnology, 15(3), 112-121.
[21] Mahmoud, B. S., & Garko, A. B. (2022). A machine learning model for malware detection using recursive feature elimination (RFE) for feature selection and ensemble technique. IOS Journals.
[22] Bobba, J., & Prema, R. (2018). Secure financial data management using Twofish encryption and cloud storage solutions. International Journal of Computer Science Engineering Techniques, 3(4), 10–16.
[23] Gangadhar, K. S. N. V. K., Kumar, B. A., Vivek, Y., & Ravi, V. (2022). Chaotic variational auto encoder based one class classifier for insurance fraud detection. arXiv preprint arXiv:2212.07802.
[24] Kethu, S. S., & Thanjaivadivel, M. (2018). SECURE CLOUD-BASED CRM DATA MANAGEMENT USING AES ENCRYPTION/DECRYPTION. International Journal of HRM and Organizational Behavior, 6(3), 1-7.
[25] Javadian Kootanaee, A., Poor Aghajan, A. A., & Hosseini Shirvani, M. (2021). A hybrid model based on machine learning and genetic algorithm for detecting fraud in financial statements. Journal of Optimization in Industrial Engineering, 14(2), 169-186.
[26] Vasamsetty, C., & Rathna, S. (2018). Securing digital frontiers: A hybrid LSTM-Transformer approach for AI-driven information security frameworks. International Journal of Computer Science and Information Technologies, 6(1), 46–54. ISSN 2347–3657.
[27] Hisham, S., Makhtar, M., & Aziz, A. A. (2022). A comprehensive review of significant learning for anomalous transaction detection using a machine learning method in a decentralized blockchain network. International Journal of Advanced Technology and Engineering Exploration, 9(95), 1366.
[28] Ganesan, S., & Kurunthachalam, A. (2018). Enhancing financial predictions using LSTM and cloud technologies: A data-driven approach. Indo-American Journal of Life Sciences and Biotechnology, 15(1).
[29] Sirajul Islam, M., Rouf, M. A., Shahariar Parvez, A. H. M., & Podder, P. (2022). Machine Learning-Driven Algorithms for Network Anomaly Detection. In Inventive Computation and Information Technologies: Proceedings of ICICIT 2021 (pp. 493-507). Singapore: Springer Nature Singapore.
[30] Kushala, K., & Rathna, S. (2018). Enhancing privacy preservation in cloud-based healthcare data processing using CNN-LSTM for secure and efficient processing. International Journal of Mechanical Engineering and Computer Science, 6(2), 119–127.
[31] Gaber, T., El-Ghamry, A., & Hassanien, A. E. (2022). Injection attack detection using machine learning for smart IoT applications. Physical Communication, 52, 101685.

[32] Bhadana, D., & Kurunthachalam, A. (2020). Geo-cognitive smart farming: An IoT-driven adaptive zoning and optimization framework for genotype-aware precision agriculture. International Journal in Commerce, IT and Social Sciences, 7(4).
[33] Khan, Z. A., & Namin, A. S. (2022). A survey of DDoS attack detection techniques for IoT systems using Blockchain technology. Electronics, 11(23), 3892.
[34] Ramar, V. A., & Rathna, S. (2018). Implementing Generative Adversarial Networks and Cloud Services for Identifying Breast Cancer in Healthcare Systems. Indo-American Journal of Life Sciences and Biotechnology, 15(2), 10-18.
[35] Zhang, Y., & Trubey, P. (2019). Machine learning and sampling scheme: An empirical study of money laundering detection. Computational Economics, 54(3), 1043-1063.
[36] Garikipati, V., & Pushpakumar, R. (2019). Integrating cloud computing with predictive AI models for efficient fault detection in robotic software. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(5).
[37] Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022). The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex & Intelligent Systems, 8(2), 1763-1780.
[38] Ayyadurai, R., & Kurunthachalam, A. (2019). Enhancing financial security and fraud detection using AI. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(1).
[39] Jayalaxmi, P. L. S., Saha, R., Kumar, G., & Kim, T. H. (2022). Machine and deep learning amalgamation for feature extraction in Industrial Internet-of-Things. Computers & Electrical Engineering, 97, 107610.
[40] Basani, D. K. R., & Bharathidasan, S. (2019). IoT-driven adaptive soil monitoring using hybrid hexagonal grid mapping and kriging-based terrain estimation for smart farming robots. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(11).
[41] Aksu, D., & Aydin, M. A. (2022). MGA-IDS: Optimal feature subset selection for anomaly detection framework on in-vehicle networks-CAN bus based on genetic algorithm and intrusion detection approach. Computers & Security, 118, 102717.
[42] Kodadi, S., & Purandhar, N. (2019). Optimizing secure multi-party computation for healthcare data protection in the cloud using hybrid garbled circuits. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(2).
[43] Alani, M. M., & Awad, A. I. (2022). Paired: An explainable lightweight android malware detection system. IEEE Access, 10, 73214-73228.
[44] Devarajan, M. V., & Pushpakumar, R. (2019). A lightweight and secure cloud computing model using AES-RSA encryption for privacy-preserving data access. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(12).
[45] Sayakkara, A., Miralles-Pechuán, L., Le-Khac, N. A., & Scanlon, M. (2020). Cutting through the emissions: feature selection from electromagnetic side-channel data for activity detection. Forensic Science International: Digital Investigation, 32, 300927.
[46] Allur, N. S., & Thanjaivadivel, M. (2019). Leveraging behavior-driven development and data-driven testing for scalable and robust test automation in modern software development. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(6).
[47] Sahu, A., Mao, Z., Davis, K., & Goulart, A. E. (2020, May). Data processing and model selection for machine learning-based network intrusion detection. In 2020 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR) (pp. 1-6). IEEE.
[48] Bobba, J., & Kurunthachalam, A. (2020). Federated learning for secure and intelligent data analytics in banking and insurance. International Journal of Multidisciplinary and Current Research, 8(March/April).
[49] Lu, Q., Xie, X., Parlikad, A. K., & Schooling, J. M. (2020). Digital twin-enabled anomaly detection for built asset monitoring in operation and maintenance. Automation in Construction, 118, 103277.
[50] Gollavilli, V. S. B. H., & Pushpakumar, R. (2020). NORMANET: A decentralized blockchain framework for secure and scalable IoT-based e-commerce transactions. International Journal of Multidisciplinary and Current Research, 8(July/August)
[51] Gressel, G., Hegde, N., Sreekumar, A., Radhakrishnan, R., Harikumar, K., & Achuthan, K. (2021). Feature importance guided attack: A model agnostic adversarial attack. arXiv preprint arXiv:2106.14815.
[52] Grandhi, S. H., & Arulkumaran, G. (2020). AI solutions for SDN routing optimization using graph neural networks in traffic engineering. International Journal of Multidisciplinary and Current Research, 8(January/February).
[53] Jayashree, P., Laila, K., Santhosh Kumar, K., & Udayavannan, A. (2022). Social network mining for predicting users' credibility with optimal feature selection. In Intelligent Sustainable Systems: Proceedings of ICISS 2021 (pp. 361-373). Springer Singapore.
[54] Nippatla, R. P., & Palanisamy, P. (2020). Optimized cloud architecture for scalable and secure accounting systems in the digital era. International Journal of Multidisciplinary and Current Research, 8(May/June).

[55] Lin, K., Xu, X., & Xiao, F. (2022). MFFusion: A multi-level features fusion model for malicious traffic detection based on deep learning. Computer Networks, 202, 108658.
[56] Kushala, K., & Thanjaivadivel, M. (2020). Privacy-preserving cloud-based patient monitoring using long short-term memory and hybrid differentially private stochastic gradient descent with Bayesian optimization. International Journal in Physical and Applied Sciences, 7(8).
[57] Fei, K., Li, Q., Zhu, C., Dong, M., & Li, Y. (2022). Electricity frauds detection in Low-voltage networks with contrastive predictive coding. International Journal of Electrical Power & Energy Systems, 137, 107715.
[58] Garikipati, V., & Bharathidasan, S. (2020). Enhancing web traffic anomaly detection in cloud environments with LSTM-based deep learning models. International Journal in Physical and Applied Sciences, 7(5).
[59] Alshahrani, S. M., Khan, N. A., Almalki, J., & Al Shehri, W. (2022). URL Phishing Detection Using Particle Swarm Optimization and Data Mining. Computers, Materials & Continua, 73(3).
[60] Kodadi, S., & Pushpakumar, R. (2020). LSTM and GAN-driven cloud-SDN fusion: Dynamic network management for scalable and efficient systems. International Journal in Commerce, IT and Social Sciences, 7(7).
[61] Taqvi, S. A. A., Zabiri, H., Tufa, L. D., Uddin, F., Fatima, S. A., & Maulud, A. S. (2021). A review on data-driven learning approaches for fault detection and diagnosis in chemical processes. ChemBioEng Reviews, 8(3), 239-259.
[62] Gollavilli, V. S. B., & Thanjaivadivel, M. (2018). Cloud-enabled pedestrian safety and risk prediction in VANETs using hybrid CNN-LSTM models. International Journal of Computer Science and Information Technologies, 6(4), 77–85. ISSN 2347–3657.