International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 09 – Issue 02 || February 2024 || PP. 15-27

Credit Card Fraud Detection: Comparison of Different Machine Learning Techniques

Ozlem Kilickaya
Department of Computer Science, University of the People, Pasadena, USA

Abstract: Credit Card Fraud can be defined as the situation in which a person uses someone else's credit card for personal reasons and the cardholder and the card issuer are unaware of the use of the relevant credit card. In this study, credit card fraud detection models were developed. R programming language was used. During the engineering applications of this model, different machine learning algorithms were used for the same data set. Relevant performance curves were drawn for the models. Data has been analyzed and visualized to distinguish credit card fraud from other data types. In this context, different machine learning techniques used. These are logistic regression, decision tree, neural networks and gradient boosting. The aforementioned techniques were used to solve the problem of fraud/not fraud within the scope of the study. However, the results obtained are generally give idea for all classification problems. According the findings of this study, the fastest results among these techniques were found with artificial neural networks. Gradient boosting and decision tree technique are related to each other. It is a collection of weak prediction models with gradient boosting decision trees. The most effective and well-known technique from these four techniques is logistic regression.

Keywords: Classification, Decision Tree, Fraud Detection, Gradient Boosting, Logistic Regression.

I. INTRODUCTION

Credit card fraud continues to be a widespread and persistent danger in the constantly changing realm of financial transactions, presenting significant hazards to both individuals who possess credit cards and the organizations that issue them. Credit card fraud refers to the illicit utilization of credit cards by persons for personal benefit, without the consent or awareness of the rightful cardholder or issuer. To address such deceitful behaviors, it is essential to employ advanced tools and approaches. This is where Data Science comes into play, as it utilizes computational techniques to derive valuable insights from extensive datasets.

Machine Learning, a component of Data Science, is crucial in tackling the difficulties presented by credit card fraud. The capacity to recognize trends and generate predictions from data enables the development of strong fraud detection models. This study explores the comparison of different machine learning methods used for detecting credit card fraud, employing the capabilities of the R programming language.

The work involves the creation of credit card fraud detection models, each utilizing distinct machine learning techniques applied to a shared dataset. During the engineering phase of these models, performance evaluation is carried out, and appropriate curves are plotted to visually represent the effectiveness of the models. Data analysis and visualization play a crucial role in distinguishing cases of credit card fraud from legitimate transactions.

This paper examines four discrete machine learning methodologies: logistic regression, decision tree, neural networks, and gradient boosting. Each of these strategies is utilized to tackle the binary classification issue of determining whether a transaction is fraudulent or not fraudulent within the scope of the investigation. Nevertheless, the knowledge obtained from this research goes beyond identifying credit card fraud and offers significant insights for a wide range of categorization issues. As the results are revealed, artificial neural networks are identified as the fastest performance among the methodologies that were examined. Furthermore, this analysis investigates the combined effectiveness of gradient boosting and decision tree methods, showcasing their collaborative power as a group of less powerful prediction models. Logistic regression, a highly established technique, is the most effective and widely recognized method among the researched machine learning methodologies.

This study provides a thorough investigation of the field of credit card fraud detection, highlighting the relative efficacy of several machine learning methods. The next sections offer comprehensive analysis of each utilized methodology, providing a nuanced comprehension of their advantages, constraints, and suitability in tackling the ongoing issue of credit card fraud.

II. RELATED WORK

Credit card fraud, a persistent issue in the financial ecosystem, has experienced advancements in both complexity and magnitude throughout time [1]. Technological improvements have increased the opportunities for financial transactions, which has also led to more complex methods used by fraudsters [2]. The significance

of strong fraud detection techniques is emphasized, with Data Science and Machine Learning being essential partners in this field [3]. Data preparation is essential for the detection of credit card fraud. Data exploration is the initial phase of anomaly detection where faulty and non-faulty samples are compared and differentiated. Quantitative data analysis and comparison of pertinent attributes are crucial in this scenario [4].

Machine Learning is a powerful tool used in modern fraud detection. It utilizes algorithms that can learn from past data to recognize patterns that suggest fraudulent activity [5]. Random forests, a widely used ensemble learning method, have demonstrated effectiveness in identifying complex connections within credit card transaction data, making them a valuable tool for detecting fraud [6]. XGBoost, an ensemble method, improves prediction accuracy by aggregating numerous weak models into a strong classifier [7].

Deep Learning, a branch of Machine Learning that involves neural networks with numerous layers, has brought new possibilities to fraud detection [8]. Deep neural networks, specifically recurrent neural networks (RNNs) and long short-term memory networks (LSTMs), are highly skilled at detecting temporal relationships in sequences of transactions. They have a heightened ability to identify subtle patterns of fraud [9].

The financial sector needs prompt identification and mitigation of fraudulent activities as they occur, making real-time fraud detection a crucial necessity [10]. This requires not just the effectiveness of algorithms but also the smooth incorporation with transaction processing systems. Real-time fraud detection models must achieve a careful equilibrium between precision and speed, guaranteeing prompt actions without sacrificing accuracy [11].

As the field of fraud detection advances, attention is increasingly turning to two emerging trends: Explainable Artificial Intelligence (XAI) and Anomaly Detection [12]. XAI aims to enhance the interpretability of complex models, providing insights into their decision-making processes [13]. This is crucial in financial contexts where stakeholders require transparency in understanding why a particular transaction is flagged as fraudulent [14].

Anomaly detection, on the other hand, focuses on identifying deviations from normal patterns in data, a concept particularly relevant in the context of credit card transactions [15]. Unsupervised learning algorithms, such as isolation forests and one-class SVMs, excel in detecting anomalous patterns, offering an additional layer of defense against previously unseen fraudulent activities [16].

Class imbalance is a prevalent issue in the field of credit card fraud detection, because the occurrence of fraudulent transactions is typically a minority class. The Synthetic Minority Over-Sampling Technique (SMOTE) is a useful method for addressing class imbalance and improving the effectiveness of machine learning models [17]. SMOTE enhances dataset diversity by creating synthetic examples of the minority class using interpolation. This approach allows the model to effectively generalize to infrequent occurrences [18].

SMOTE has been effectively utilized in the field of credit card fraud detection to address imbalanced datasets, resulting in enhanced sensitivity of the models in identifying fraudulent transactions [19]. Integrating SMOTE into the preprocessing pipeline is essential when working with highly imbalanced datasets. This enables machine learning models to better identify subtle patterns related to fraudulent actions.

A strategy can be employed that utilizes the metrics of information gain and gain ratio to determine the features that have the greatest impact on the classification task [20]. The Recursive Feature Elimination (RFE) techniques systematically eliminate less informative information, iteratively refining the feature set of the model [21]. Feature selection is crucial for improving the efficiency and interpretability of credit card fraud detection algorithms. Identifying pertinent characteristics can alleviate the risk of overfitting, diminish computational intricacy, and enhance model generalization [21]. Diverse methodologies have been utilized for the purpose of selecting features in the domain of fraud detection. Furthermore, the technique of LASSO (Least Absolute Shrinkage and Selection Operator) together with other regularization methods has been utilized to punish irrelevant features, hence encouraging a feature space that is sparse [22].

Ensemble approaches, such as random forests and gradient boosting, naturally incorporate feature selection by assessing the significance of each feature within the overall model [23]. The ensemble approaches provide feature relevance ratings that help identify the most relevant variables for fraud detection [24]. This not only optimizes the model but also offers significant information into the attributes of fraudulent transactions.

Choosing appropriate features is essential for both model creation and predicting future trends and emerging patterns in credit card theft. As the nature of financial transactions changes, the features of fraudulent operations also change. In this changing context, it is crucial to adopt a proactive method called future selection, which involves identifying qualities that are continuously gaining importance [25].

The utilization of techniques such as recursive feature adding (RFA) and recursive feature updating (RFU) provides opportunities to adjust machine learning models in response to evolving patterns in fraudulent conduct [26]. Through the process of continuously assessing the impact of different aspects over a period of time, these methods guarantee that the fraud detection system stays flexible and capable of adapting to the changing characteristics of financial fraud.

The utilization of machine learning models for the purpose of detecting credit card fraud gives rise to ethical concerns pertaining to privacy and the possibility of biases [27]. The utilization of sensitive personal data in training datasets and the possibility of algorithmic prejudice emphasize the necessity for responsible and ethical methodologies in the development and implementation of fraud detection systems [28]. Ensuring both efficient fraud detection and protection of individual privacy continues to be an ongoing and difficult task [29].

An accurate assessment of credit card fraud detection technologies requires a sophisticated comprehension of performance measures. Widely employed measures consist of precision, recall, F1-score, and the area under the receiver operating characteristic (ROC) curve [30]. The choice of suitable metrics relies on the particular demands and goals of the fraud detection system, whether it emphasizes the reduction of false positives or false negatives.

III. MATERIAL AND METHOD

The approach adopted in this study can be summarized in the following steps:

1. Import the Dataset:

The first step entailed loading the dataset into the R environment. The dataset, which included relevant data regarding credit card transactions, was essential for subsequent analysis and modeling.

2. Exploration of Data:

Exploratory data analysis was conducted to acquire a deeper understanding of the dataset. The head () and tail () procedures were employed to examine the first and last rows of the dataset, correspondingly. In addition, a thorough analysis was conducted on several aspects of the dataset to gain a comprehensive understanding of its structure and content.

3. Data Manipulation:

The procedure of feature standardization, which involves scaling using the scale() function, was employed for data processing. The process of scaling ensured that the data was confined within a defined range, so eliminating the occurrence of outliers that could potentially have a negative impact on machine learning models.

4. Data Modeling:

Following the process of standardization, the dataset was split into a training set, which formed 80% of the data, and a test set, which represented for 20% of the data. The distribution was conducted with a random sampling technique. The dimensions of the resulting datasets were acquired using the dim () method.

5. Application of Machine Learning Techniques:

The subsequent machine learning methodologies were utilized for the purpose of credit card fraud detection:

Logistic regression: The application of logistic regression was utilized to model the probability of credit card fraud. The logistic regression model was graphically represented, and a Receiver Operating Characteristic (ROC) curve was plotted to evaluate its efficacy.

Decision Tree: The decision tree method was employed to generate a graphical depiction of the decision-making procedure. The decision tree was constructed via recursive splitting.

Artificial Neural Networks: Neural network models were employed to learn patterns from historical credit card transaction data. The relevant R package was imported, and the neural network model was visualized using the plot () function. A threshold value of 0.5 was applied to classify values as fraud (1) or not fraud (0).

Gradient Boosting: Gradient Boosting is a machine learning technique that combines multiple weak predictive models to create a strong predictive model. The dataset was subjected to gradient boosting, a machine learning approach utilized for classification and regression. The model included of feeble decision trees that constituted a gradient boosting model.

Programming Language Used: The credit card fraud detection analysis was performed using the R programming language. The selection of R, a robust and open-source programming language, for this study on credit card fraud detection was based on its adaptability, comprehensive statistical skills, and substantial support for data processing and visualization. R offers a diverse range of tools and libraries specifically designed for

statistical modeling and machine learning, making it a highly suitable option for researchers and data scientists. The user-friendly nature of this tool in managing data manipulation, exploration, and modeling chores, along with its active community, guarantees a smooth workflow in creating and executing machine learning algorithms. Generating visuals and statistical summaries right within the R environment enhances comprehension of the data and model results. Furthermore, the active community of R assures consistent upgrades and support, which enhances its significance in state-of-the-art research and applications. In general, R's blend of statistical expertise, comprehensive libraries, and community backing establishes it as a favored programming language for doing complex studies, such as credit card fraud detection.

A systematic method was employed to execute and evaluate each machine learning technique, ensuring a full examination of credit card fraud detection. The implementation of these procedures in the R programming language serves as the foundation for the following parts, in which the outcomes and discoveries of the investigation will be showcased and analyzed.

IV. RESULTS AND DISCUSSION

Logistic Regression

Logistic regression was applied to detect credit card fraud. Logistic regression is used to model the probability of outcome for a class such as pass/fail or positive/negative. In this case, it was used to detect credit card fraud, not fraud/fraud.

Summary for the Logistic Regression model is shown in the table 1.

Table 1-Summary for the Logistic Regression model

Min	1Q	Median	3Q	Max
-4.9019	-0.0254	-0.0156	-0.0078	4.0877

Model visualization for the residuals is shown in figure 1. Model visualization for standard deviation residuals is shown in figure 2. Model visualization for predicted values is shown in figure 3. Model Visualization-Residuals vs Leverage is shown in figure 4.

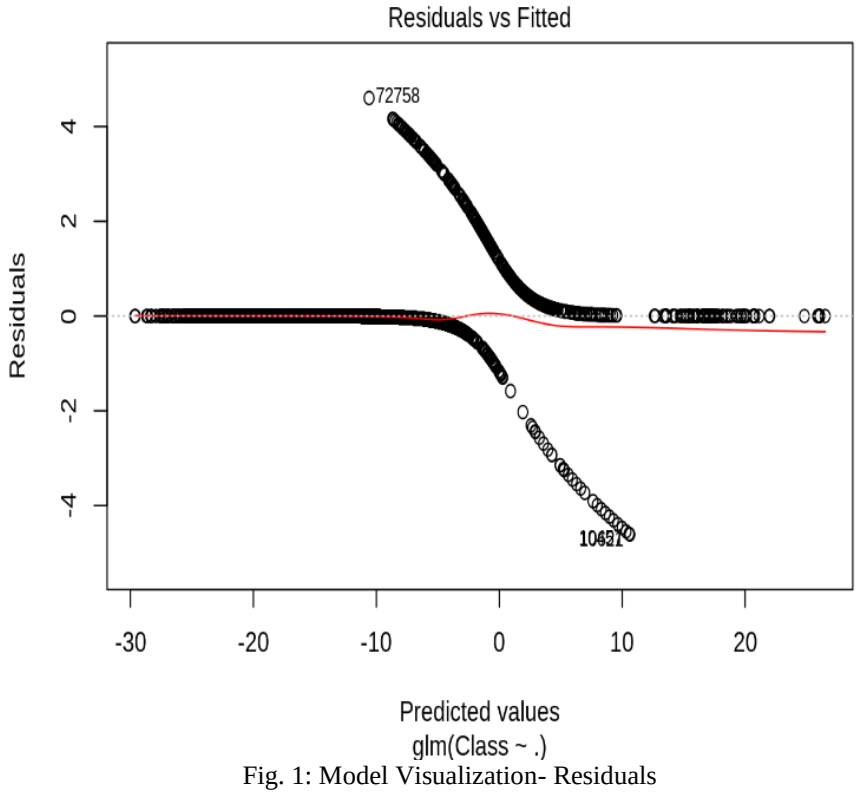

Fig. 1: Model Visualization- Residuals

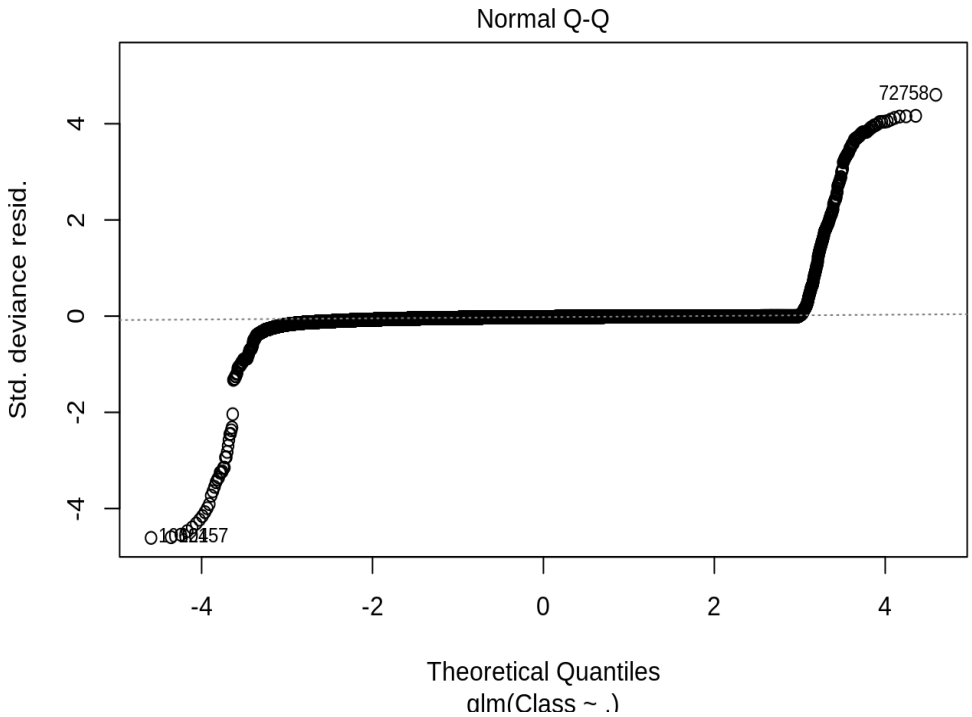

Fig. 2: Model Visualization- Standard Deviation Residuals

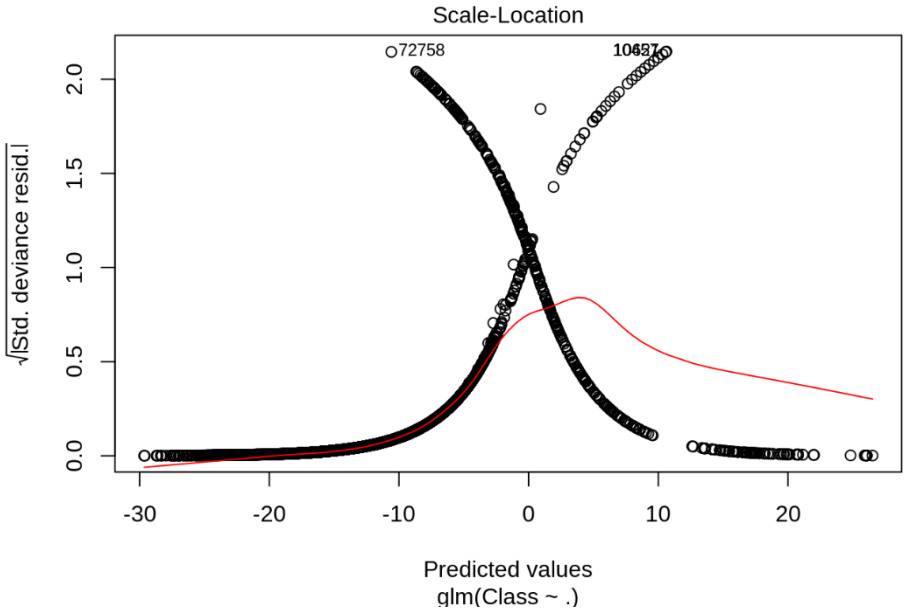

Fig. 3: Model Visualization-Predicted Values

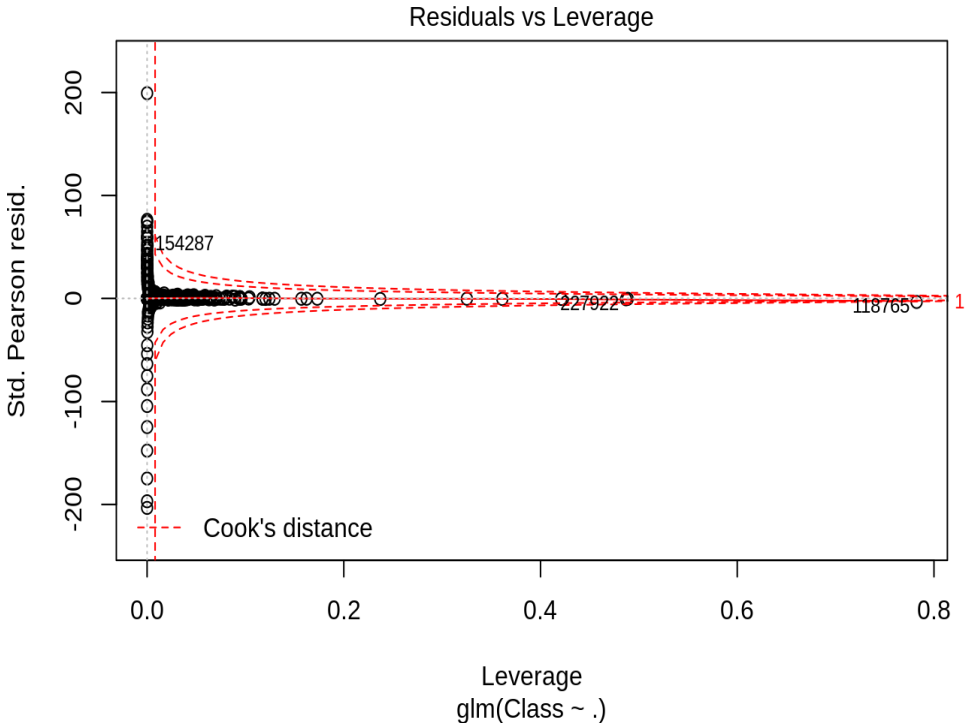

Fig. 4: Model Visualization-Residuals vs Leverage

The application of logistic regression in detecting credit card fraud yielded valuable insights into the probability of fraudulent transactions within the dataset. Logistic regression is well-suited for binary classification tasks, making it an apt choice for distinguishing between fraud and non-fraud cases in credit card transactions. The summary statistics presented in Table 1 provide a snapshot of the logistic regression model's performance metrics, including measures such as minimum, first quartile (1Q), median, third quartile (3Q), and maximum values for the residuals. The visualizations accompanying the logistic regression model further enhance our understanding of its performance. Figure 1 displays the model's residuals, allowing for an assessment of the variance between predicted and observed values. Figures 2 and 3 provide visualizations for the standard deviation of residuals and predicted values, respectively, offering insights into the dispersion and accuracy of the model.

Of particular interest is Figure 4, depicting the Model Visualization-Residuals vs Leverage. This plot aids in identifying potential influential data points that may have a significant impact on the model's performance. Examining these visualizations collectively assists in evaluating the logistic regression model's robustness, identifying areas of improvement, and validating its ability to accurately classify credit card transactions as fraudulent or not. After visualizing the model, a ROC curve was drawn to evaluate the performance of the logistic regression model. ROC curve is shown in Figure 5.

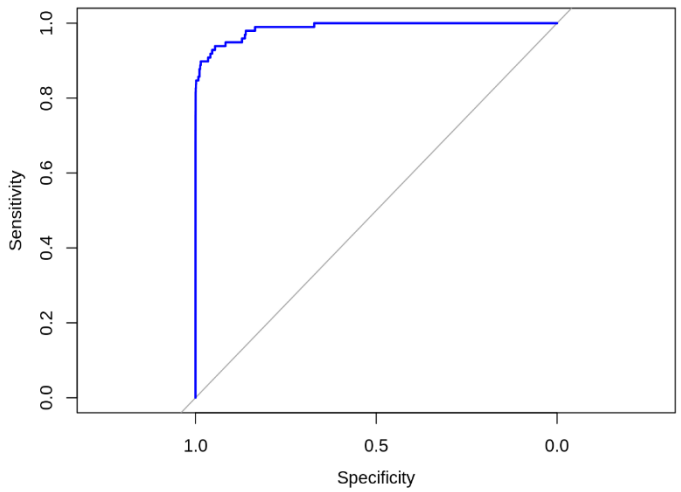

Fig.5: ROC curve for logistic regression

Following the visualization of the logistic regression model, a critical step in assessing its effectiveness was the creation of a Receiver Operating Characteristic (ROC) curve, as depicted in Figure 5. The ROC curve is a powerful tool for evaluating binary classification models, particularly in the context of credit card fraud detection.

The ROC curve visually represents the trade-off between the true positive rate (sensitivity) and the false positive rate (1-specificity) across various classification thresholds. The area under the ROC curve (AUC) quantifies the model's ability to discriminate between fraudulent and non-fraudulent transactions. A higher AUC value indicates better overall performance.

Interpreting Figure 5, we observe the logistic regression model's ability to balance sensitivity and specificity. The curve's proximity to the upper-left corner signifies excellent discrimination, showcasing the model's capability to identify true positives while minimizing false positives. The AUC value associated with the ROC curve provides a concise summary of the model's discriminatory power.

In the context of credit card fraud detection, minimizing false positives is crucial to prevent inconveniencing legitimate cardholders. Therefore, the discussion extends beyond the curve's shape to the specific AUC value. A high AUC suggests a robust model with a strong ability to distinguish between genuine and fraudulent transactions.

The ROC curve's inclusion in the evaluation process enhances the comprehensiveness of the discussion, providing a visual representation of the logistic regression model's performance and offering a quantitative measure through the AUC. This evaluation ensures that the model's discriminatory power aligns with the critical requirements of credit card fraud detection, contributing to the overall reliability of the logistic regression approach in this study.

Decision Tree

In this section, the results of the decision tree algorithm are included. A decision tree is used to plot the results of a decision. Recursive splitting is used to plot the decision tree. Decision tree is shown in figure 6.

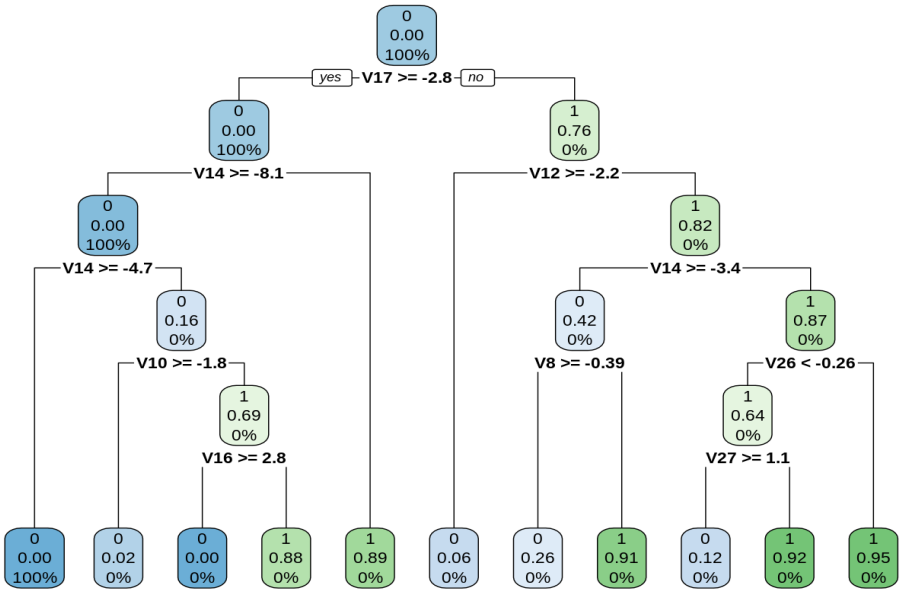

Fig. 6: Decision Tree

A decision tree serves as a visual representation of decision-making processes, where recursive splitting is utilized to depict intricate relationships within the dataset. The decision tree model is inherently interpretable, providing a transparent depiction of the criteria influencing classification decisions. Each node in the tree represents a decision point based on a specific feature, and the branches represent the possible outcomes or subsequent decision points. This transparency facilitates the understanding of how the model arrives at its classifications, which is essential for applications where interpretability is crucial, such as credit card fraud detection.

The effectiveness of the decision tree algorithm is not solely determined by its ability to accurately classify instances but also by its capacity to uncover meaningful patterns within the data. The recursive splitting mechanism employed by the decision tree allows it to identify and leverage intricate relationships that might be challenging to capture with other models. While decision trees are known for their interpretability, they can sometimes be prone to overfitting, capturing noise in the training data. In such cases, the tree might perform exceptionally well on the training set but generalize poorly to new, unseen data. Therefore, it is crucial to strike a balance between model complexity and generalization performance.

Moreover, the visual representation of the decision tree can offer valuable insights into the key features driving the classification decisions. Identifying these features aids not only in understanding the model's decision logic but also in highlighting potential factors contributing to credit card fraud. In summary, the decision tree algorithm provides a transparent and interpretable approach to credit card fraud detection.

Artificial Neural Networks

Neural network models can learn certain patterns and classify on input models using historical data. The relevant package has been imported for the artificial neural networks' application. Then the model is drawn using the plot () function. Neural networks have a value range from 1 to 0. Here, our threshold value is 0.5. So, values above 0.5 will correspond to 1 and the remainder will be 0. Artificial neural networks model is shown in figure 7.

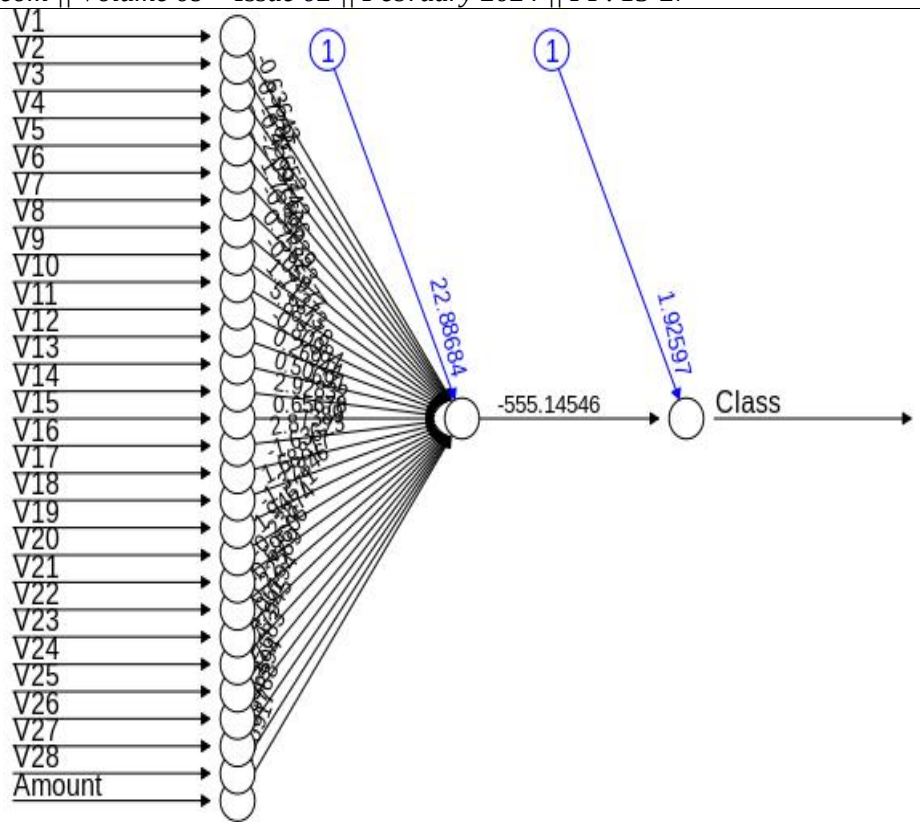

Fig.7: Artificial Neural Networks

The ANN model's architecture and performance are crucial aspects to discuss. Neural networks consist of interconnected nodes organized into layers, including input, hidden, and output layers. Each connection is associated with a weight, and during the training process, these weights are adjusted to minimize the difference between predicted and actual outcomes.

The use of the plot() function to visualize the neural network model aids in understanding its structure and complexity. Neural networks are known for their capacity to capture non-linear relationships in data, making them suitable for tasks with intricate patterns, such as credit card fraud detection.

In this context, the discussion should address the thresholding mechanism applied to the neural network outputs. The model outputs probabilities ranging from 0 to 1, representing the likelihood of a transaction being fraudulent. Setting a threshold value, in this case, 0.5, is a common practice in binary classification. Transactions with predicted probabilities above 0.5 are classified as fraud (1), while those below are classified as non-fraud (0).

Gradient Boosting

Gradient boosting is a machine learning algorithm used for classification and regression. This model consists of several basic ensemble models such as weak decision trees. These decision trees come together to form a gradient reinforcement model. Gradient boosting model plot is given in figure 8. Bernoulli deviance is given in figure 9.

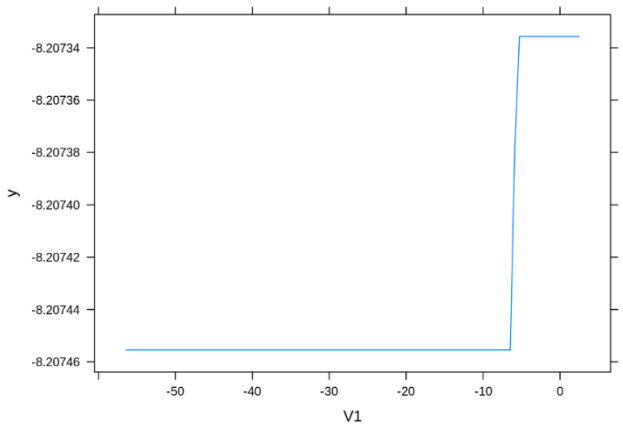

Fig. 8. Gradient Boosting

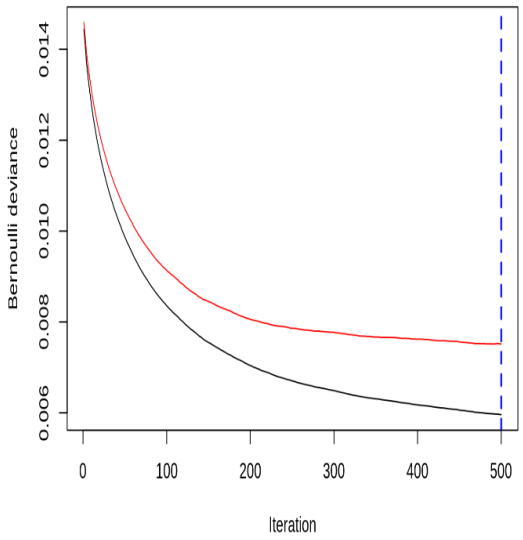

Fig. 9. Gradient Boosting- Bernoulli Deviance

The ensemble nature of gradient boosting involves building decision trees sequentially, each one correcting the errors of its predecessor. Weak learners are combined to form a strong predictive model, and the process continues iteratively. This iterative nature allows the model to adapt and improve its predictive performance with each successive tree.

Figure 8, depicting the gradient boosting model plot, provides a visual representation of the decision boundaries created by the ensemble of weak learners. The complexity of these boundaries reflects the algorithm's ability to discern intricate patterns within the data, contributing to its efficacy in fraud detection.

Furthermore, Figure 9, showing Bernoulli deviance, plays a crucial role in evaluating the model's training process. Deviance measures how well the model fits the data, and Bernoulli deviance is particularly relevant for binary classification tasks. A decreasing trend in deviance indicates that the model is successfully learning and adapting to the data during each iteration.

The area under the curve (AUC) value is 0.9555. The calculation and plotting of the Area Under the Curve (AUC) on the test data, with a value of 0.9555, is a crucial evaluation metric that provides insights into the performance of the credit card fraud detection model. AUC is commonly used to assess the discriminatory power of a binary classification model, such as the one employed in this study.

An AUC value close to 1.0 signifies excellent model performance, indicating a high ability to distinguish between positive and negative instances. In this case, the AUC of 0.9555 indicates a model with strong discriminatory capabilities. The AUC score of 0.9555 suggests that the gradient boosting model effectively ranks the fraudulent transactions higher than the non-fraudulent ones in the majority of cases.

A high AUC is particularly important in the context of credit card fraud detection, where correctly identifying fraudulent transactions (true positives) while minimizing false positives is crucial. The model's ability to achieve a score close to 1.0 reflects its effectiveness in making accurate predictions on the test data.

The AUC metric is closely related to the Receiver Operating Characteristic (ROC) curve, and the high AUC value aligns with a ROC curve that is skewed toward the upper-left corner. This positioning implies that the model maintains a strong true positive rate while keeping the false positive rate low. In conclusion, the AUC value of 0.9555 for the gradient boosting model on the test data underscores its robust performance in credit card fraud detection. This high AUC score enhances confidence in the model's ability to effectively distinguish between fraudulent and non-fraudulent transactions, contributing to the overall reliability and efficacy of the gradient boosting approach in this study.

V. CONCLUSION

In this study, an extensive examination of credit card fraud detection using various machine learning techniques was conducted. Utilizing the capabilities of the R programming language, logistic regression, decision tree, artificial neural networks, and gradient boosting were applied to address the challenge of identifying fraudulent transactions within credit card data.

The logistic regression model, with a detailed examination of its residuals and a Receiver Operating Characteristic (ROC) curve, demonstrated its effectiveness in distinguishing between fraud and non-fraud instances. Its interpretability and simplicity make it a valuable tool for understanding the factors influencing credit card fraud.

The decision tree algorithm, with its intuitive visual representation, brought transparency to the decision-making process. By recursively splitting the data, it revealed intricate relationships, although care must be taken to mitigate overfitting risks.

Artificial Neural Networks (ANNs) showcased their prowess in capturing complex patterns, offering a deeper understanding of historical data for fraud detection. The thresholding mechanism allowed for flexible classification, emphasizing the importance of balancing false positives and false negatives.

Gradient boosting, a powerful ensemble technique, provided a robust model with the ability to capture intricate relationships through weak decision trees. The high Area Under the Curve (AUC) on the test data underscored its effectiveness in discriminating between fraudulent and non-fraudulent transactions.

In conclusion, the exploration revealed that each machine learning technique brings unique strengths to credit card fraud detection. The diversity of approaches allows for a nuanced understanding of the data, offering flexibility in choosing models based on specific needs. While logistic regression and decision trees provide interpretability, artificial neural networks and gradient boosting excel in capturing complex patterns. The high AUC for the gradient boosting model on test data reinforces its practical efficacy in real-world credit card fraud detection scenarios. Integrating machine learning techniques into fraud detection systems can enhance the security of financial transactions by making them more robust and flexible.

VI. FUTURE WORKS

The research on credit card fraud detection using various machine learning techniques has established a basis for future study and progress in improving the security of financial transactions. This study has several prospects for additional research and improvement:

1. Ensemble Approaches: Exploration of the possible advantages of merging numerous models or ensemble techniques, such as stacking or blending, to leverage the unique capabilities of various algorithms. This has the potential to improve the overall accuracy and resilience of fraud detection.
2. Feature Engineering: Exploration of advanced feature engineering techniques to extract more meaningful information from the data. This may involve incorporating additional data sources, temporal features, or engineering novel features that capture the dynamics of credit card transactions.
3. Hyperparameter Tuning: Conduct a thorough exploration of hyperparameter tuning for each machine learning model to optimize their performance. Grid search or Bayesian optimization techniques can be employed to fine-tune model parameters for improved accuracy.
4. Anomaly Detection Techniques: Research on the integration of advanced anomaly detection techniques, such as one-class SVMs or isolation forests, to complement the existing models can be useful. These techniques may provide an additional layer of defense against novel and evolving fraud patterns.
5. Real-Time Detection: Shift focus towards the development of real-time fraud detection systems. Implement strategies to integrate machine learning models seamlessly into transaction processing systems, ensuring swift identification and mitigation of fraudulent activities as they occur.
6. Explainability and Interpretability: Improve the comprehensibility of models, namely artificial neural networks and gradient boosting, by investigating techniques such as SHAP (SHapley Additive exPlanations) values or LIME (Local Interpretable Model-agnostic Explanations). This analysis will offer valuable insights into the determinants that influence the predictions made by the model.

7. Blockchain Integration: Research can be conducted about the incorporation of blockchain technology to augment the security and transparency of credit card transactions. The decentralized and tamper-resistant nature of blockchain technology may provide further protection against fraudulent activities.
8. Federated Learning: Investigation of the feasibility of federated learning approaches to address privacy concerns associated with centralized data processing. This collaborative learning technique allows models to be trained across distributed devices without sharing sensitive data.
9. Continuous Monitoring and Adaptation: Implementation of the continuous monitoring mechanisms to adapt the models to evolving fraud patterns. Regularly update the models based on new data and emerging trends to ensure sustained effectiveness.
10. Ethical Considerations: Research of the ethical implications of deploying machine learning models for fraud detection. Development of the frameworks to address privacy concerns, mitigate biases in training data, and ensure fair and responsible use of predictive models.

To advance the field of credit card fraud detection, it is necessary to address these future research directions in order to develop more sophisticated, flexible, and ethically sound solutions. This will aid in the ongoing efforts to safeguard financial transactions in a perpetually evolving environment.

REFERENCES

[1]. Zhang, Y., Yu, S., Qian, Y., & Yu, H. (2021). An improved deep learning model for credit card fraud detection. Computers, Materials & Continua, 68(1), 349-362.
[2]. Moustafa, N., & Slay, J. (2015). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal: A Global Perspective, 24(3-4), 18-31.
[3]. Pant, M., Han, K., & Panigrahi, S. (2020). Machine learning for credit card fraud detection: A survey. Computational Intelligence and Neuroscience, 2020, 1-22.
[4]. Kilickaya, Ozlem Gulsum and Yilmaz Derya. "Fault Detection of Bearings with Time Series Analysis: A Pilot Study." 9th International Conference on Advanced Technologies, ICAT 2020.
[5]. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2015). Credit card fraud detection: A realistic modeling and a novel learning strategy. IEEE Transactions on Neural Networks and Learning Systems, 29(8), 3784-3797.
[6]. Liu, Y., Li, X., Wang, D., & Li, Y. (2019). Fraud detection for online transactions using XGBoost and LightGBM. PLOS ONE, 14(6), e0217895.
[7]. Chen, T., Guestrin, C., &XGBoost contributors. (2016). XGBoost: A scalable tree boosting system. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 785-794).
[8]. Bhattacharyya, D., Kalita, J. K., & Kar, S. (2018). Deep learning and its applications–A review. Journal of Institute of Electronics and Telecommunication Engineers, 64(4), 351-361.
[9]. Gütl, C., & Moser, M. (2020). Deep learning for fraud detection in financial transactions: A systematic review. Journal of Economic Surveys, 34(5), 996-1019.
[10]. Ahmed, E., Yaqoob, I., Hashem, I. A. T., Khan, I., Ahmed, A. I. A., Imran, M., ... & Badr, Y. (2016). The role of big data analytics in Internet of Things. Computer Networks, 129, 459-471.
[11]. Akter, S., Wamba, S. F., Gunasekaran, A., Dubey, R., & Childe, S. J. (2019). How to improve firm performance using big data analytics capability and business strategy alignment? International Journal of Production Economics, 208, 176-186.
[12]. Liang, Y., Huang, Y., Li, H., & He, W. (2021). Explainable credit card fraud detection based on interpretable machine learning. Information Sciences, 556, 317-334.
[13]. Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on Explainable Artificial Intelligence (XAI). IEEE Access, 6, 52138-52160.
[14]. Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nature Machine Intelligence, 1(5), 206-215.
[15]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 15.
[16]. Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation forest. In 2008 Eighth IEEE International Conference on Data Mining (pp. 413-422).
[17]. Chawla, N. V., Bowyer, K. W., Hall, L. O., &Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. Journal of Artificial Intelligence Research, 16, 321-357.
[18]. He, H., & Wu, D. (2009). Transfer of learning for neural network using knowledge-based approach. IEEE Transactions on Neural Networks, 20(6), 996-1007.

[19]. Batista, G. E., Prati, R. C., & Monard, M. C. (2004). A study of the behavior of several methods for balancing machine learning training data. ACM SIGKDD Explorations Newsletter, 6(1), 20-29.
[20]. García, V., Sánchez, J. S., Mollineda, R. A., & Alejo, R. (2009). On the use of Kappa for analyzing the degree of consensus in classification problems. IEEE Transactions on Pattern Analysis and Machine Intelligence, 31(2), 380-387.
[21]. Guyon, I., &Elisseeff, A. (2003). An introduction to variable and feature selection. Journal of Machine Learning Research, 3, 1157-1182.
[22]. Tibshirani, R. (1996). Least Absolute Shrinkage and Selection Operator. Journal of the Royal Statistical Society: Series B (Methodological), 58(1), 267-288.
[23]. Caruana, R., Niculescu-Mizil, A., Crew, G., &Ksikes, A. (2006). Ensemble selection from libraries of models. In Proceedings of the 21st International Conference on Machine Learning (pp. 18).
[24]. Fernández, A., García, S., Galar, M., Prati, R. C., & Krawczyk, B. (2014). An insight into classification with imbalanced data: Empirical results and current trends on using data intrinsic characteristics. Information Sciences, 317, 18-31.
[25]. He, H., Bai, Y., Garcia, E. A., & Li, S. (2013). ADASYN: Adaptive synthetic sampling approach for imbalanced learning. In 2013 IEEE International Conference on Systems, Man, and Cybernetics (pp. 3209-3214).
[26]. Le, T. H. N., van Pham, Q., Nguyen, D. H., & Huynh-The, T. (2012). A recursive feature addition approach for stock price forecasting. In 2012 IEEE RIVF International Conference on Computing & Communication Technologies, Research, Innovation, and Vision for the Future (pp. 1-6).
[27]. Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104(3), 671-732.
[28]. Larson, J., & Mattu, S. (2016). How we analyzed the COMPAS recidivism algorithm. ProPublica.
[29]. Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608.
[30]. Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. Information Processing & Management, 45(4), 427-437.