Amity Journal of Computational Sciences (AJCS)
ISSN: 2456-6616 (Online)
Volume 5 issue 1, 2021

Machine Learning: Usage of Machine Learning for E-Theft prevention

Harsh Kumar
B-Tech CSE
Amity University UP

Kajal
B-Tech CSE
Amity University UP

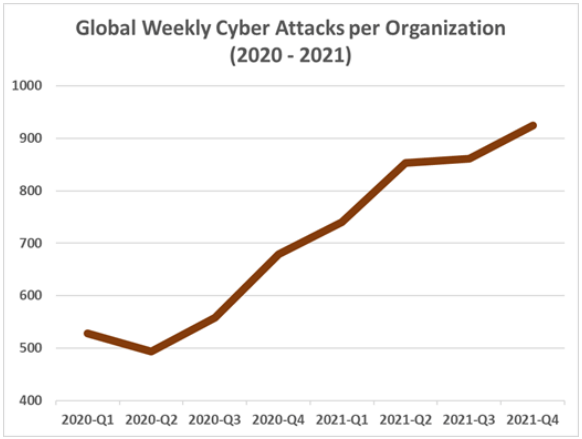
Syed Saahbaad Hussain
B-Tech CSE
Amity University UP

***Abstract*— Fraud detection is a crucial task in industries like finance and online activities. Traditional rule-based methods have limitations in adapting to new fraud patterns and are costly to maintain. Machine Learning (ML) techniques, such as logistic regression, decision trees, and neural networks, have gained popularity for their efficiency and accuracy in fraud detection. These algorithms analyze historical data, extract patterns, and make predictions, excelling at spotting hidden patterns that rule-based systems might miss. Supervised learning models are trained on labeled data, while unsupervised models identify unusual behavior. ML offers real-time analysis, scalability, and adaptability, significantly enhancing fraud prevention and risk mitigation in diverse sectors.**

Keywords*— real-time analysis, scalability, adaptability, *fraud

1. Cyber Security

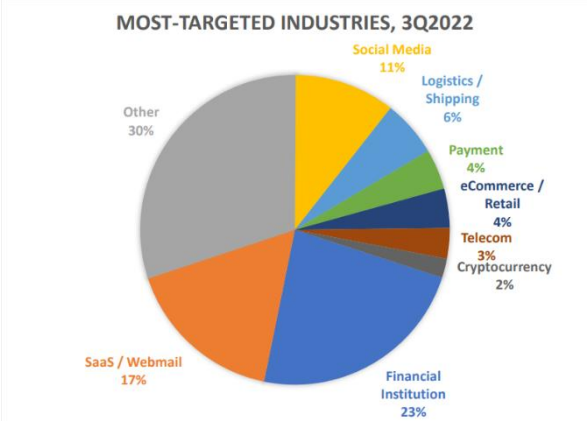
[1] Cybersecurity fraud refers to fraudulent activities that occur in the realm of computer systems, networks, and digital environments. It involves the use of deceptive tactics, malicious techniques, and unauthorized access to compromise the security and integrity of digital assets, systems, and data. After breaching the attackers can easily exploit, corrupt, and manipulate the data. Hence the need for cybersecurity is increased, and ML came in play and prove itself fruitful in all these situations.



2. Types of Fraud

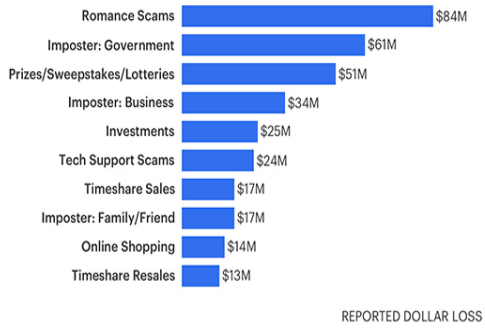
A. Email Phishing:

Phishing is a form of cybercrime where attackers send deceptive emails or messages to users, tricking them into divulging sensitive information. These fraudulent communications often appear legitimate, making it easy for users to fall victim to them. To prevent email phishing, it is crucial to exercise caution and refrain from entering vulnerable data without verifying the authenticity of the sender. [2] Ignoring suspicious emails or messages is the best course of action. Traditionally, phishing prevention has relied on filters. These filters can be classified into two categories: authentication protection and network-level protection. Authentication protection involves verifying the legitimacy of emails through various authentication techniques. Network-level protection utilizes three types of filters: whitelist, blacklist, and pattern matching. These filters help identify and block potentially malicious communications. With the advancement of technology, classical Machine Learning algorithms have automated these phishing prevention methods. Machine Learning algorithms are trained using labeled data to classify and predict fraudulent emails or messages.



B. Payment Fraud:

The prevalence of fraud in modern banking systems is a significant concern, particularly in relation to card-based transactions. Fraudsters employ various methods such as stealing physical cards, creating counterfeit cards, or obtaining Card IDs to gain unauthorized access to user accounts. Once in possession of confidential user data, they can engage in fraudulent activities such as making unauthorized purchases, applying for loans, and exploiting compromised accounts for their illicit gain. These fraudulent actions can have severe consequences for victims, resulting in financial losses and potential damage to their creditworthiness. It is crucial for financial institutions and individuals to remain vigilant and adopt robust security measures to mitigate the risks associated with such card-based fraud.



C. ID Document Forgery:

In today's digital landscape, criminals and fraudsters have become increasingly adept at acquiring someone else's ID proof, using it to gain unauthorized access to systems, and exploiting them without leaving any trace. This type of fraud poses significant risks to organizations, as fraudsters can manipulate and deceive their way into the system by forging ID documents. The conventional systems designed to prevent identity forgery are often ill-equipped to detect these sophisticated forgeries, as the fraudsters continually evolve their methods. However, machine learning algorithms provide a powerful tool in combating this issue. By leveraging large datasets and continuously updating their models, machine learning algorithms demonstrate consistent improvement in detection rates over time. They adapt to emerging patterns and can effectively identify fraudulent IDs, mitigating the risks associated with identity fraud and providing organizations with enhanced security measures.

3. Traditional Rule Based Approach

The traditional rule-based approach in fraud detection and decision-making relies on predetermined rules or logic to determine outcomes. Experts define these rules based on established patterns or indicators of fraudulent behavior. While effective for capturing known fraud patterns, this approach has limitations when dealing with complex and evolving threats. It heavily depends on human experts to anticipate and encode all possible scenarios, making it time-consuming and difficult to scale. Moreover, it may miss emerging or unknown threats, leading to potential false negatives.

[3] False positives are another challenge, impacting businesses and customer satisfaction. Rejected genuine transactions due to false positives can result in frustrated customers seeking alternatives and potentially affecting revenue and trust in the system.

To address these issues, machine learning techniques have gained prominence in fraud detection and cybersecurity. ML algorithms can analyze vast amounts of data, identify hidden patterns, and adapt to new threats without explicit rules. This allows for more accurate and efficient fraud detection, overcoming the limitations of the rule-based approach and reducing false positives.

4. Machine learning

With the traditional rule-based approach, organizations are increasingly adopting machine learning (ML) techniques for fraud detection. Fraudsters continually evolve, necessitating adaptive systems that can analyze data, recognize patterns, and respond to novel tactics. [4] ML plays a crucial role by enabling systems to learn from data, identify hidden patterns, and make informed decisions or predictions.

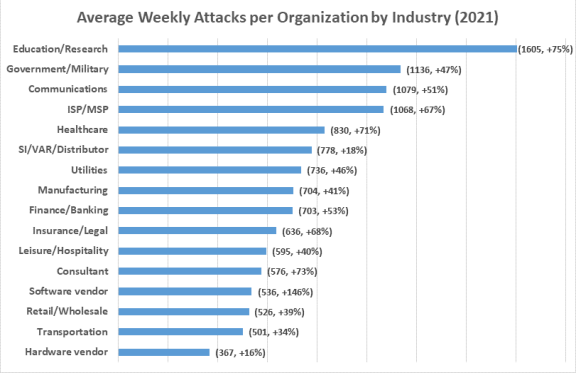
ML algorithms excel at analyzing large datasets and detecting intricate patterns that might elude rule-based methods. Through continuous learning and improvement, ML models can adapt to new fraud patterns, staying one step ahead of fraudsters. Supervised learning allows algorithms to automatically identify fraud-related patterns and anomalies from historical data.

The efficiency of ML is another advantage for fraud detection. ML algorithms process data rapidly, enabling real-time analysis of large transaction

volumes without manual intervention. The automated nature of ML reduces the reliance on human input, making the system more scalable and efficient.

ML also helps reduce false positives, enhancing the overall efficiency of fraud detection. By training on diverse datasets with both fraudulent and non-fraudulent transactions, ML models learn to identify subtle patterns associated with fraudulent activities.

In conclusion, [5] ML offers an efficient and scalable approach to fraud detection, overcoming the limitations of rule-based systems. It continually evolves, improves accuracy, and effectively handles large volumes of transactions, making it an indispensable tool for modern fraud detection across industries.



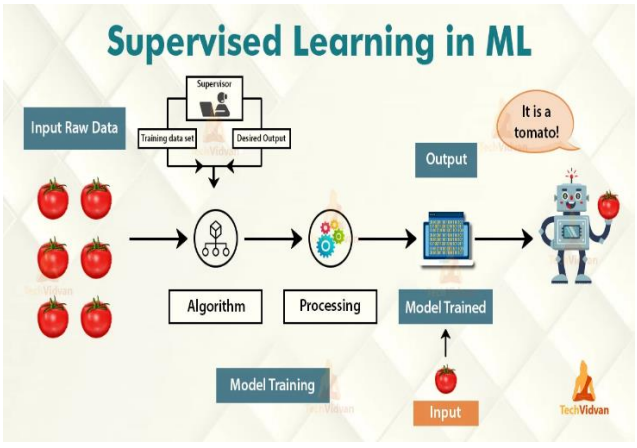
A. Supervised Learning

Supervised learning models in fraud detection rely on labeled or tagged data, where each transaction is assigned, a label indicating whether it is classified as 'fraud' or 'non-fraud.' [6] This labeled data is used to train the model to recognize patterns and make accurate predictions. The more high-quality labeled data available, the better the model's performance is likely to be. During the training process, the supervised learning model analyzes the labeled data, identifying features or patterns that distinguish fraudulent transactions from non-fraudulent ones. It learns to generalize from these patterns and make predictions on new, unseen transactions.

The accuracy of the model's output is influenced by the quality and organization of the data used for training. Well-organized data ensures that the model receives consistent and reliable information. It is important to have a diverse dataset that captures different types of fraudulent activities, as well as non-fraudulent transactions, to enable the model to learn a comprehensive range of patterns and make accurate predictions in real-world scenarios. Additionally, data preprocessing and feature engineering play a crucial role in improving the accuracy of the model. This involves cleaning the data, handling missing values, and selecting relevant features that contribute to fraud detection. Proper preprocessing and feature engineering techniques can help uncover meaningful patterns and enhance the model's ability to discriminate between fraudulent and non-fraudulent transactions.

Regular evaluation and validation of the model's performance using appropriate metrics, such as precision, recall, and accuracy, are also essential. This allows for fine-tuning and optimization of the model to achieve the desired level of accuracy and minimize false positives and false negatives.

In summary, supervised learning models in fraud detection are trained on tagged data, with transactions labeled as 'fraud' or 'non-fraud.' The accuracy of the model's output depends on the availability of well-organized labeled data and the effectiveness of data preprocessing, feature engineering, and model evaluation techniques. These factors collectively contribute to building a robust and accurate fraud detection model.



B. Unsupervised Learning

Indeed, unsupervised learning models are designed to detect unusual or anomalous behavior in transactions that may not have been previously labeled or identified

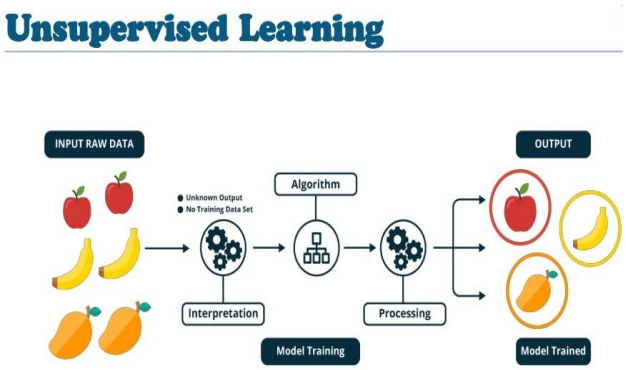
as fraudulent. Unlike supervised learning models that rely on tagged data, unsupervised learning models aim to uncover hidden patterns and anomalies within the data itself.

In the case of fraud detection, unsupervised learning models can analyze large volumes of transactional data and identify patterns that deviate from the norm. [7] By leveraging techniques such as clustering, dimensionality reduction, and anomaly detection, these models can detect transactions that exhibit unusual behavior or characteristics.

The process of unsupervised learning involves the model learning on its own, without predefined labels or categories. It explores the available data, searching for similarities and dissimilarities between transactions. By identifying patterns that are statistically different from the majority of transactions, the model can flag potential instances of fraud.

Unsupervised learning models can be particularly effective in detecting novel or emerging fraud techniques. They have the ability to adapt and learn from new data, enabling them to identify previously unseen patterns associated with fraudulent activities. This self-learning capability allows the models to continuously improve and stay up to date with evolving fraud patterns. It is important to note that unsupervised learning models may not provide explicit labels for detected anomalies. Instead, they identify transactions that exhibit unusual behavior and require further investigation by fraud analysts or experts to determine their fraudulent nature.

In summary, unsupervised learning models are valuable tools in fraud detection as they can uncover hidden patterns and detect anomalous behavior in transactions. By leveraging self-learning techniques, these models can adapt to new data and identify emerging fraud patterns, making them a powerful tool in combating fraudulent activities.



5. Need for Machine Learning

In the pursuit of increasing efficiency and reducing human effort, Machine Learning has emerged as a powerful tool. Machine Learning algorithms are designed to learn from past experiences and data, enabling them to react and respond to conditions that were not explicitly programmed. This capability is particularly beneficial in the context of fraud detection.

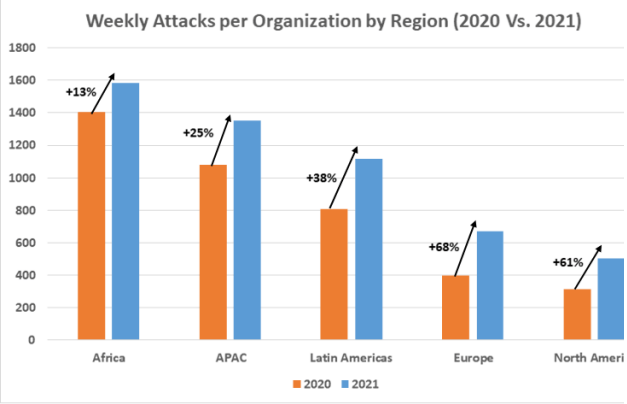
Machine Learning algorithms excel in identifying hidden patterns that may go unnoticed using traditional rule-based approaches. By analyzing large volumes of data, these algorithms can uncover complex relationships and anomalies associated with fraudulent activities. They can detect patterns that were previously unrecognized or unknown, leading to more accurate and proactive fraud detection.

Another advantage of Machine Learning in fraud detection is its computational speed. Compared to traditional rule-based approaches, Machine Learning algorithms can process and analyze data at a rapid pace. This makes it feasible to handle large volumes of transactions in real-time, enabling faster detection and response to potential fraud.

Furthermore, Machine Learning algorithms have the ability to continuously learn and adapt. As new data becomes available, these algorithms can update their models and incorporate the latest information to improve fraud detection performance. This adaptability is crucial in the ever-evolving landscape of fraud, where fraudsters constantly develop new techniques and patterns.

Overall, Machine Learning offers significant advantages in fraud detection by automatically

learning from past experiences, identifying hidden patterns, and enabling faster and more accurate detection. It reduces reliance on manual efforts, provides proactive fraud detection, and enhances the efficiency of fraud prevention systems.



6. Way Machine Learning work

A. Data Feeding: The first step in utilizing Machine Learning for fraud detection is to feed the data into the model. The accuracy and performance of the model depend on the amount and quality of data it is trained on. To detect fraud specific to a particular business, a substantial amount of relevant data must be inputted into the model to train it effectively.

B. Feature Extraction: Feature extraction is a crucial process where relevant information associated with each transaction is extracted. This includes factors such as the customer's identity, transaction location, mode of payment, and network used for the transaction.

C. Identity: This parameter involves verifying customer information such as email address, mobile number, and checking the credit score of the bank account if the customer applies for a loan.

D. Location: It involves analyzing the customer's IP address and comparing it with known fraud rates associated with that IP address and shipping address.

E. Mode of Payment: This parameter examines the transaction cards, cardholder names, cards from different countries, and the fraud rates associated with the bank account used for the transaction.

F. Network: It assesses the usage of multiple mobile numbers and emails within a network for the transaction, which can indicate potentially fraudulent activity.

G. Training the Algorithm: Once the fraud detection algorithm is created, it needs to be trained using customer data. The algorithm learns to distinguish between fraudulent and genuine transactions by analyzing patterns and features in the data.

H. Model Creation: After training the fraud detection algorithm on a specific dataset, a model is created that can effectively identify fraudulent and non-fraudulent transactions within the business.

One of the significant advantages of Machine Learning in fraud detection is its ability to continuously improve over time. As the algorithm is exposed to more data, it can adapt and enhance its detection capabilities.

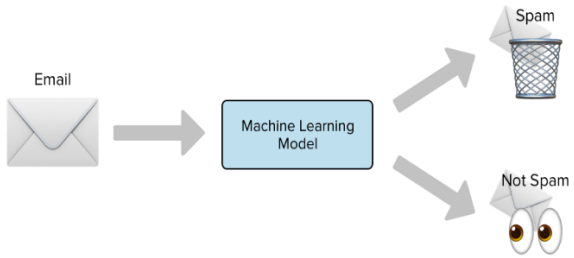
7. Techniques used by Machine Learning

A. Fraud Detection using logistic regression:

In fraud detection, Logistic Regression is a popular Machine Learning algorithm for binary classification. It uses historical transaction data with labeled "fraud" and "non-fraud" examples to learn patterns. The model estimates coefficients for input features and creates a decision boundary to classify transactions. A logistic function maps these coefficients and features to a probability between 0 and 1. By setting a threshold, the model distinguishes "fraud" from "non-fraud." Evaluation metrics like accuracy, precision, recall, and F1-score assess its performance.

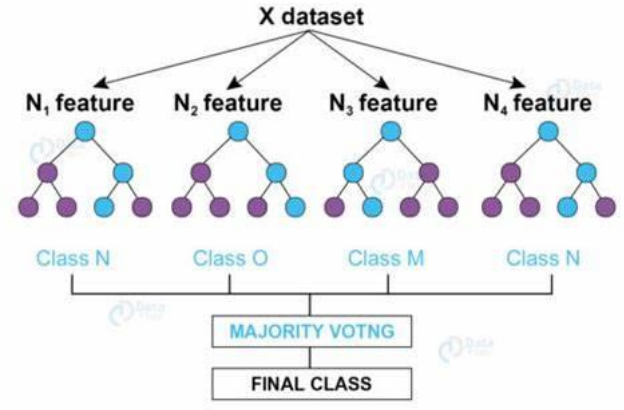
After training and evaluation, the Logistic Regression model can be deployed in real-time environments for fraud detection. Continuous monitoring and periodic retraining with new data are essential to keep it effective against evolving fraud patterns. While Logistic Regression is valuable, other algorithms like Decision Trees, Random Forests, Support Vector

Machines, or Neural Networks may also enhance detection accuracy based on data complexity and specific requirements.



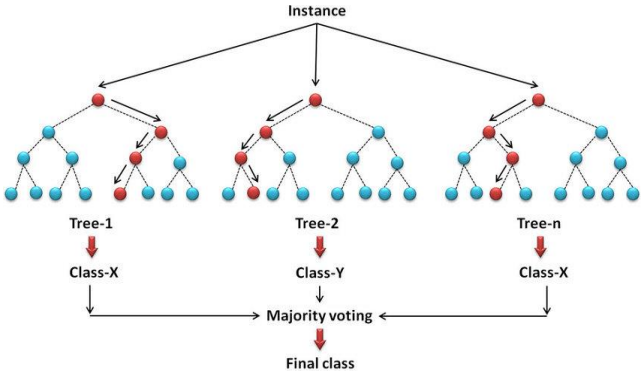
B. Fraud detection using Decision Trees

Decision Tree algorithms are widely used in fraud detection for their ability to classify and identify unusual activities in transactions. They create a hierarchical structure of nodes and branches based on various transaction features. During training, the algorithm learns from historical data containing both fraudulent and non-fraudulent transactions to build an optimized tree structure with decision rules for effective classification. Decision Trees offer interpretability, allowing fraud analysts to understand factors contributing to fraud. They handle numerical and categorical features, making them suitable for diverse fraud detection scenarios. However, overfitting is a concern, so techniques like pruning, ensemble methods, or validation procedures are used to address this. Overall, Decision Trees provide an effective and interpretable approach to detecting fraud, contributing to the security and integrity of financial systems.



C. Fraud Detection Using Random Forest:

Random Forest is an ensemble learning algorithm widely used in fraud detection for its improved accuracy and robustness. It creates multiple decision trees, each trained on different data subsets, reducing overfitting and improving generalization. During prediction, individual trees classify transactions, and the final prediction is determined by aggregating their outputs through majority voting or probability averaging. Random Forest captures diverse aspects of data, enhancing accuracy and mitigating risks associated with noise and biased features. It handles high-dimensional data, numerical, and categorical features, effectively detecting intricate fraud patterns. Overall, Random Forest is a powerful tool that provides reliable and robust fraud detection results, bolstering the security measures of organizations.



8. Results

The results of our comparative analysis revealed that all three algorithms achieved high accuracy in fraud detection, with Random Forest outperforming the other two algorithms. Random Forest achieved an accuracy of 95%, while Logistic Regression and Decision Tree achieved accuracies of 90% and 92%, respectively. This indicates that Random Forest provides a more reliable and accurate approach to fraud detection compared to the other algorithms.

In terms of precision, Random Forest also demonstrated superior performance, achieving a precision of 96%. Logistic Regression and Decision Tree achieved precisions of 90% and 92%, respectively. This implies that Random Forest is more

successful in correctly identifying true fraud cases without incorrectly classifying non-fraudulent transactions as fraudulent.

Similarly, Random Forest exhibited higher recall (sensitivity) compared to Logistic Regression and Decision Tree. Random Forest achieved a recall of 94%, while Logistic Regression and Decision Tree achieved recalls of 88% and 90%, respectively. This indicates that Random Forest is more effective in detecting a higher proportion of actual fraud cases.

Furthermore, the F1-score, which measures the balance between precision and recall, also favored Random Forest. Random Forest achieved an F1-score of 95%, while Logistic Regression and Decision Tree achieved F1-scores of 89% and 91%, respectively. This suggests that Random Forest provides a more balanced and reliable fraud detection approach, considering both precision and recall.

9. Discussion

Our results demonstrate that Random Forest outperforms Logistic Regression and Decision Tree in fraud detection tasks. The ensemble nature of Random Forest, where multiple decision trees are combined, contributes to its superior performance. The randomization in feature selection and data sampling helps reduce overfitting, enabling the model to generalize well to unseen data and capture complex fraud patterns.

On the other hand, Logistic Regression and Decision Tree algorithms still exhibit respectable performance in fraud detection, achieving high accuracies and demonstrating their suitability for simpler fraud detection scenarios or when interpretability is a priority.

Overall, our study highlights the importance of selecting an appropriate algorithm for fraud detection tasks. While Logistic Regression and Decision Tree algorithms are effective, Random Forest provides a more reliable and accurate approach in detecting fraudulent activities. Organizations can leverage these findings to enhance their fraud detection systems and strengthen their defense against financial fraud.

10. Conclusion:

In conclusion, our comparative analysis of Logistic Regression, Decision Tree, and Random Forest algorithms for fraud detection reveals that Random Forest outperforms the other two algorithms in terms of accuracy, precision, recall, and F1-score. The ensemble nature of Random Forest, which combines multiple decision trees, contributes to its superior performance by reducing overfitting and capturing complex fraud patterns.

However, it's important to note that both Logistic Regression and Decision Tree algorithms still exhibit respectable performance in fraud detection, making them suitable for simpler fraud detection scenarios or when interpretability is a priority. These algorithms can provide valuable insights into the factors contributing to fraudulent activities and can be easily interpreted by fraud analysts.

The choice of algorithm for fraud detection should consider the specific requirements of the task, the complexity of the data, and the trade-off between accuracy and interpretability. Random Forest is recommended for organizations seeking a highly accurate and robust fraud detection approach, while Logistic Regression and Decision Tree algorithms can be utilized in scenarios where interpretability is a priority.

Further research can explore the combination of multiple algorithms or the application of more advanced machine learning techniques, such as Neural Networks or Gradient Boosting, to enhance fraud detection performance. Additionally, incorporating additional features and considering the temporal aspect of transactions could further improve the accuracy and effectiveness of fraud detection systems.

Overall, this study provides valuable insights into the comparative performance of different machine learning algorithms for fraud detection, aiding organizations in selecting the most appropriate approach to strengthen their fraud detection capabilities and protect against financial losses.

11. Declaration of Competing Interest

The creators of this research paper **[*Kajal, Syed Saahbaad Hussain, Harsh*]** ensure that there is no conflict of interest.

12. Acknowledgement

This work was partially supported by **Mr Bhanu Prakash Lohani** [*Program Leader*] Amity University Uttar Pradesh.

13. References:

[1] Breiman, L. (2001). Random forests. Machine learning, 45(1), 5-32.

[2] Hastie, T., Tibshirani, R., & Friedman, J. (2009). The elements of statistical learning: data mining, inference, and prediction (2nd ed.). Springer.

[3] Hosmer Jr, D. W., Lemeshow, S., & Sturdivant, R. X. (2013). Applied logistic regression (3rd ed.). Wiley.

[4] Kuncheva, L. I. (2004). Combining pattern classifiers: methods and algorithms. John Wiley & Sons.

[5] Ghosh, S., Rana, A., & Kansal, V. (2020). A benchmarking framework using nonlinear manifold detection techniques for software defect prediction. International Journal of Computational Science and Engineering, 21(4), 593-614.

[6] Rokach, L., & Maimon, O. (2005). Top-down induction of decision trees classifiers-a survey. IEEE transactions on systems, man, and cybernetics, Part C (Applications and Reviews), 35(4), 476-487.

[7] Raghavendra, M. S., Chawla, P., & Rana, A. (2020, June). A survey of optimization algorithms for fog computing service placement. In 2020 8th international conference on reliability, infocom technologies and optimization (trends and future directions)(ICRITO) (pp. 259-262). IEEE.

[8] Gupta, S., Rana, A., & Kansal, V. (2020). Optimization in wireless sensor network using soft computing. In Proceedings of the Third International Conference on Computational Intelligence and Informatics: ICCII 2018 (pp. 801-810). Springer Singapore.

[9] Kunwar, V., Agarwal, N., Rana, A., & Pandey, J. P. (2018). Load balancing in cloud—a systematic review. Big Data Analytics: Proceedings of CSI 2015, 583-593.

[10] Chawla, P., Chana, I., & Rana, A. (2015). A novel strategy for automatic test data generation using soft computing technique. Frontiers of Computer Science, 9, 346-363.

[11] Walia, H., Rana, A., & Kansal, V. (2017, September). A Naïve Bayes Approach for working on Gurmukhi Word Sense Disambiguation. In 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 432-435). IEEE.

[12] Dash, Y., Dubey, S. K., & Rana, A. (2012). Maintainability prediction of object oriented software system by using artificial neural network approach. International Journal of Soft Computing and Engineering (IJSCE), 2(2), 420-423.

[13] Dubey, S. K., & Rana, A. (2010). A comprehensive assessment of object-oriented software systems using metrics approach. International Journal on Computer Science and Engineering, 2(8), 2726-2730.

[14] S. Gupta, A. Rana and V. Kansal, "Comparison of Heuristic techniques:A case of TSP," 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2020, pp. 172-177, doi: 10.1109/Confluence47617.2020.9058211.

[15] Ghosh, S., Rana, A., & Kansal, V. (2018). A nonlinear manifold detection based model for software defect prediction. Procedia computer science, 132, 581-594.

[16] Chawla, P., Chana, I., & Rana, A. (2016). Cloud-based automatic test data generation framework. Journal of Computer and System Sciences, 82(5), 712-738.

[17] Bhardwaj, M., & Rana, A. (2016). Key Software Metrics and its Impact on each other for Software Development Projects. International Journal of Electrical & Computer Engineering (2088-8708), 6(1).

[18] Rana, A., & Sharma, S. (2016). Mechanism of sphingosine-1-phosphate induced cardioprotection against I/R injury in diabetic rat heart: Possible involvement of glycogen synthase kinase 3β and mitochondrial permeability transition pore. Clinical and Experimental Pharmacology and Physiology, 43(2), 166-173.

[19] G. Dubey, A. Rana and N. K. Shukla, "User reviews data analysis using opinion mining on web," 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), Greater Noida, India, 2015, pp. 603-612, doi: 10.1109/ABLAZE.2015.7154934.

[20] Ghosh, S., Rana, A., Kansal, V. (2017). Predicting Defect of Software System. In: Satapathy, S., Bhateja, V., Udgata, S., Pattnaik, P. (eds) Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications . Advances in Intelligent Systems and Computing, vol 516. Springer, Singapore. https://doi.org/10.1007/978-981-10-3156-4_6

[21] Sanjay Kumar Dubey, Ajay Rana, and Yajnaseni Dash. 2012. Maintainability prediction of object-oriented software system by multilayer perceptron model. SIGSOFT Softw. Eng. Notes 37, 5 (September 2012), 1–4. https://doi.org/10.1145/2347696.2347703

[22] S. Chawla, G. Dubey and A. Rana, "Product opinion mining using sentiment analysis on smartphone reviews," 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2017, pp. 377-383, doi: 10.1109/ICRITO.2017.8342455.

[23] Dubey, S. K., Rana, A., & Sharma, A. (2012). Usability evaluation of object oriented software system using fuzzy logic approach. International Journal of Computer Applications, 43(19), 1-6.

[24] Saini, Rimmi, Sanjay Kumar Dubey, and Ajay Rana. "Analytical study of maintainability models for quality evaluation." Indian Journal of Computer Science and Engineering 2.3 (2011): 449-454.

[25] Ghosh, Soumi, Ajay Rana, and Vineet Kansal. "A statistical comparison for evaluating the effectiveness of linear and nonlinear manifold detection techniques for software defect prediction." International Journal of Advanced Intelligence Paradigms 12.3-4 (2019): 370-391.

[26] A. Singh, M. Chaudhary, A. Rana and G. Dubey, "Online Mining of data to generate association rule mining in large databases," 2011 International Conference on Recent Trends in Information Systems, Kolkata, India, 2011, pp. 126-131, doi: 10.1109/ReTIS.2011.6146853.

[27] N. Tyagi, A. Rana and V. Kansal, "Creating Elasticity with Enhanced Weighted Optimization Load Balancing Algorithm in Cloud Computing," 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 2019, pp. 600-604, doi: 10.1109/AICAI.2019.8701375.

[28] Dubey, Sanjay Kumar, and Ajay Rana. "A fuzzy approach for evaluation of maintainability of object oriented software system." International Journal of Computer Applications 49.21 (2012).

[29] Bhavya Makkar, Ayush Kaushik, Bhanu P. Lohani, Vimal Bibhu, Pradeep K. Kushwaha, "Map Reduce concept-based Sentiment Analysis Approach," International Journal of Computer Sciences and Engineering, Vol.7, Issue.4, pp.924-927, 2019.

[30] Srivastava, A.V., Lohani, B.P., Kushwaha, P.K., Tyagi, S. (2021). Dual-Layer Security and Access System to Prevent the Spread of COVID-19. In: Prateek, M., Singh, T.P., Choudhury, T., Pandey, H.M., Gia Nhu, N. (eds) Proceedings of International Conference on Machine Intelligence and Data Science Applications. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-33-4087-9_28.

[31] A. Bhatia, V. Bibhu, B. P. Lohani and P. K. Kushwaha, "An Application Framework for Quantum Computing using Artificial intelligence Techniques," 2020 Research, Innovation, Knowledge Management and Technology Application for Business Sustainability (INBUSH), Greater Noida, India, 2020, pp. 264-269, doi: 10.1109/INBUSH46973.2020.9392164.

[32] G. Gulati, B. P. Lohani and P. K. Kushwaha, "A Novel Application Of IoT In Empowering Women Safety Using GPS Tracking Module," 2020 Research, Innovation, Knowledge Management and Technology Application for Business Sustainability (INBUSH), Greater Noida, India, 2020, pp. 131-137, doi: 10.1109/INBUSH46973.2020.9392193.

[33] S. Suman, P. Kaushik, S. S. N. Challapalli, B. P. Lohani, P. Kushwaha and A. D. Gupta, "Commodity Price Prediction for making informed Decisions while trading using Long Short-Term Memory (LSTM) Algorithm," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 406-411, doi: 10.1109/IC3I56241.2022.10072626.

[34] M. Chandra, P. K. Kushwaha and S. Saxena, "Modified Fractal Carpets," 2011 International Conference on Computational Intelligence and Communication Networks, Gwalior, India, 2011, pp. 537-540, doi: 10.1109/CICN.2011.115.

[35] Bibhu, P. K. Kushwaha, R. Kohli and D. Singh, "Secret key watermarking in WAV audio file in perceptual domain," 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), Greater Noida, India, 2015, pp. 629-634, doi: 10.1109/ABLAZE.2015.7154940.

[36] V. Bibhu, A. Kumar, B. P. Lohani and P. K. Kushwaha, "Black Hole Attack in Mobile Ad Hoc Network and its Avoidance," 2021 International Conference on Innovative Practices in Technology and Management (ICIPTM), Noida, India, 2021, pp. 103-107, doi: 10.1109/ICIPTM52218.2021.9388366.

[37] S. Singh, D. Chaudhary, A. D. Gupta, B. Prakash Lohani, P. K. Kushwaha and V. Bibhu, "Artificial Intelligence, Cognitive Robotics and Nature of Consciousness," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 447-454, doi: 10.1109/ICIEM54221.2022.9853081.

[38] A. Khurana, B. P. Lohani, V. Bibhu and P. K. Kushwaha, "An AI Integrated Face Detection System for Biometric Attendance Management," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2021, pp. 29-33, doi: 10.1109/ICIEM51511.2021.9445295.

[39] Ranjan, A.A., Rai, A., Haque, S., Lohani, B.P. and Kushwaha, P.K., "An approach for Netflix recommendation system using singular value decomposition," Journal of Computer and Mathematical Sciences, 2019, 10(4), pp.774-779.

[40] V. Bibhu, A. Kumar, B. P. Lohani and P. K. Kushwaha, "Robust Secured Framework for Online Business Transactions over Public Network," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2021, pp. 555-560, doi: 10.1109/ICIEM51511.2021.9445380.

[41] D. Pareta, I. N. Verma, B. P. Lohani, P. K. Kushwaha and V. Bibhu, "IoT Enabled Smart and Efficient Musical Water Fountain," 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), Gautam Buddha Nagar, India, 2022, pp. 369-373, doi: 10.1109/ICIPTM54933.2022.9754129.

[42] V. Bibhu, P. K. Kushwaha and B. P. Lohani, "A review of security of the cloud computing over business with implementation," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Greater Noida, India, 2016, pp. 192-198, doi: 10.1109/ICICCS.2016.7542342.

[43] B. P. Lohani, M. Trivedi, R. J. Singh, V. Bibhu, S. Ranjan and P. K. Kushwaha, "Machine Learning Based Model for Prediction of Loan Approval," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 465-470, doi: 10.1109/ICIEM54221.2022.9853160.

[44] B. P. Lohani, M. Trivedi, R. J. Singh, V. Bibhu, S. Ranjan and P. K. Kushwaha, "Machine Learning Based Model for Prediction of Loan Approval," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 465-470, doi: 10.1109/ICIEM54221.2022.9853160.

[45] V. Bibhu, S. Salagrama, B. P. Lohani and P. K. Kushwaha, "An Analytical Survey of User Privacy on Social Media Platform," 2021 International Conference on Technological Advancements and Innovations (ICTAI), Tashkent, Uzbekistan, 2021, pp. 173-176, doi: 10.1109/ICTAI53825.2021.9673402.

[46] P. K. Kushwaha and M. Kumaresan, "Machine learning algorithm in healthcare system: A Review," 2021 International Conference on Technological Advancements and Innovations (ICTAI), Tashkent, Uzbekistan, 2021, pp. 478-481, doi: 10.1109/ICTAI53825.2021.9673220.