INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM (eISSN: 2536-7919 pISSN: 2536-7900)

VOLUME 09 ISSUE 12 Pages: 23-35

Research Article

Journal Website: https://scientiamreearch.org/index.php/ijcsis

ENHANCED BANKING FRAUD DETECTION: A COMPARATIVE ANALYSIS OF SUPERVISED MACHINE LEARNING ALGORITHMS

Submission Date: June 25, 2024, Accepted Date: November 30, 2024,
Published Date: December 25, 2024
Crossref Doi: https://doi.org/10.55640/ijcsis/Volume09Issue12-03

Md Nur Hossain
Master's in information technology management, Webster University, USA

Safayet Hossain
Master of Science in Cybersecurity, Washington University of Science and Technology, USA

Ayan Nath
Master's in computer and information science, International American University, USA

Paresh Chandra Nath
Master of Science in Information Technology, Washington University of Science and Technology, USA

Mohammad Iftekhar Ayub
Master of Science in Information Technology, Washington University of Science and Technology, USA

Md Mehedi Hassan
Master of Science in Information Technology, Washington University of Science and Technology, USA

Md Tarake Siddique
Master of Science in Information Technology, Washington University of Science and Technology, USA

Mohammad Rasel
Masters in Business Analytics, International American University, LA, California, USA

ABSTRACT

Banking fraud has become a pervasive challenge, necessitating innovative solutions to protect financial institutions and their customers. This study investigates the effectiveness of supervised machine learning algorithms in detecting fraudulent activities within the banking sector. We conducted a comparative analysis of five widely used algorithms: Logistic Regression, Random Forest, Support Vector Machines, Gradient Boosting, and Neural Networks. Using a real-

world banking dataset, we employed robust preprocessing and fine-tuning techniques to address class imbalances and optimize model performance. The evaluation metrics, including accuracy, precision, recall, F1-score, and area under the ROC curve (AUC), revealed that Gradient Boosting and Neural Networks consistently outperformed other models, achieving high precision and recall rates. The results highlight the potential of machine learning to detect subtle patterns of fraud while minimizing false positives and negatives. Furthermore, we discuss the implications of these findings for real-time fraud prevention systems and emphasize the importance of algorithm selection and scalability in operational environments.

KEYWORDS

Real-world banking dataset, Fraud prevention systems, financial institutions, Transactional data analysis, Anomaly detection, Class imbalance in datasets.

INTRODUCTION

The prevalence of fraud in banking and financial systems has emerged as a critical concern for institutions worldwide. Fraudulent transactions not only result in significant financial losses but also damage customer trust and institutional reputation. As financial transactions become increasingly digitized, the complexity and sophistication of fraudulent activities have grown, necessitating the development of advanced detection mechanisms. Traditional methods of fraud detection, which often rely on manual oversight or basic rule-based systems, have proven inadequate in addressing the dynamic and evolving nature of fraud.

In recent years, machine learning (ML) has gained prominence as a transformative technology capable of addressing complex problems in various domains, including fraud detection. By analyzing large volumes of transactional data, ML algorithms can identify subtle patterns and anomalies that may indicate fraudulent behavior. This study aims to conduct a comprehensive comparative analysis of supervised machine learning algorithms for detecting banking fraud. The objective is to evaluate their effectiveness, robustness, and practical applicability in real-world scenarios, thereby providing actionable insights for financial institutions seeking to enhance their fraud detection systems.

This paper is structured as follows: the introduction provides an overview of the research problem and its significance, the literature review discusses related work and existing methodologies, the methodology outlines the approach and experimental setup, the results and discussion present the findings, and the conclusion highlights the implications and future directions of the study.

LITERATURE REVIEW

Fraud detection has been an active area of research within the fields of finance and data science. Over the years, various approaches have been proposed to tackle this issue, ranging from rule-based systems to more advanced data-driven techniques. Traditional fraud detection systems primarily rely on predefined rules and thresholds. While these methods are straightforward and interpretable, they often fail to adapt to the rapidly changing tactics employed by fraudsters, resulting in high false positive and false negative rates.

The advent of machine learning has revolutionized fraud detection by enabling systems to learn from historical data and identify patterns indicative of fraudulent activity. Supervised learning, in particular, has been widely adopted for this purpose. Algorithms such as Logistic Regression, Random Forest, Support Vector Machines, Gradient Boosting, and Neural Networks have been extensively studied for their ability to classify transactions as fraudulent or legitimate. Each of these algorithms offers unique advantages and limitations. For instance, tree-based models like Random Forest and Gradient Boosting are known for their robustness and ability to handle complex datasets, while linear models like Logistic Regression provide simplicity and interpretability.

Several studies have demonstrated the efficacy of machine learning in fraud detection. For example, Abdallah et al. (2016) explored the use of ensemble methods for detecting credit card fraud, reporting significant improvements in accuracy compared to standalone models. Similarly, Bahnsen et al. (2014) introduced a cost-sensitive learning approach to address the class imbalance inherent in fraud detection datasets, achieving enhanced detection rates for fraudulent transactions. More recently, deep learning models have been investigated for their potential to capture intricate patterns in large datasets, although their computational complexity and lack of interpretability remain challenges.

Despite these advancements, there remains a gap in understanding the comparative performance of various supervised machine learning algorithms in banking fraud detection. Most existing studies focus on specific algorithms or datasets, limiting their generalizability. Additionally, the practical implications of these models, such as their scalability and real-time applicability, are often overlooked. This study seeks to address these gaps by providing a comprehensive evaluation of multiple supervised learning algorithms using a real-world banking dataset. The findings aim to guide practitioners in selecting and implementing the most effective models for their specific needs.

By bridging the gap between theoretical research and practical application, this study contributes to the growing body of knowledge on machine learning for fraud detection and highlights the potential of data-driven approaches to enhance the security and resilience of financial systems.

METHODOLOGY

Research Design

We designed this study to systematically compare the performance of various supervised machine learning algorithms in detecting banking fraud. This research followed a quantitative approach, focusing on the application of machine learning techniques to a well-defined historical dataset of banking transactions. The primary objective was to evaluate the ability of different algorithms to identify fraudulent transactions with high precision and recall, thereby providing actionable insights for financial institutions.

To ensure the robustness of our results, we adopted a step-by-step methodology that included data collection, preprocessing, model selection, training, evaluation, and comparative analysis. Each stage of the research process was executed meticulously to minimize biases and enhance the reliability of the findings.

Data Collection

The dataset for this study was sourced from publicly available repositories, which provide anonymized banking transaction data. The dataset included a variety of attributes essential for fraud detection, such as:

Attribute Name	Description
Transaction ID	Unique identifier for each transaction
Transaction Amount	The monetary value of the transaction
Transaction Time	Timestamp indicating when the transaction occurred
Account Number	The account involved in the transaction
Fraud Indicator	Binary label indicating if the transaction was fraudulent (1) or legitimate (0)

The dataset contained a total of 100,000 records, with 90% representing legitimate transactions and 10% fraudulent transactions. This inherent class imbalance is typical of real-world fraud detection scenarios.

Data Preprocessing

Data preprocessing is a critical step in the machine learning pipeline, as it directly impacts the quality and reliability of the resulting models. In our study, we meticulously performed several preprocessing tasks to prepare the dataset for effective analysis and model training.

Initially, we addressed missing values within the dataset. Missing numerical values were replaced using mean imputation, ensuring that the central tendency of the data remained intact. For categorical variables, mode imputation was employed, which effectively retained the most frequent category for each feature. This approach ensured the dataset's completeness without introducing significant biases.

Next, we transformed categorical variables into a machine-readable format. For instance, the account type variable, which contained categories such as "savings" and "checking," was encoded using one-hot encoding. This process created binary columns for each category, allowing the models to process these variables as numerical inputs.

Class imbalance, a prevalent issue in fraud detection datasets, was addressed through the Synthetic Minority Oversampling Technique (SMOTE). By generating synthetic samples for the minority class (fraudulent transactions), we achieved a balanced dataset. This step was crucial to prevent the models from being biased toward the majority class, thereby improving their ability to detect fraudulent transactions.

Feature scaling was then applied to normalize numerical attributes. Using Min-Max scaling, we transformed all numerical features to a range between 0 and 1. This step ensured that all features contributed equally during model training, preventing features with larger ranges from dominating the learning process.

Finally, the dataset was split into three subsets: training, validation, and test sets, in a 70:15:15 ratio. The training set was used to train the models, the validation set helped optimize hyperparameters, and the test set evaluated the final model performance. We ensured that the class distribution within each subset mirrored the original dataset's distribution to maintain consistency.

Algorithm Selection

Algorithm selection is a pivotal stage in the development of a robust fraud detection system. The

choice of algorithms is critical as it determines the effectiveness, scalability, and interpretability of the results. In this study, we selected four well-established supervised learning algorithms, each offering unique advantages and characteristics tailored to the intricacies of fraud detection.

We began by evaluating logistic Regression, a linear model widely regarded for its simplicity and interpretability. Logistic Regression serves as an effective baseline algorithm, allowing us to establish a reference point for comparison. Its ability to provide probabilistic outputs made it particularly suitable for tasks involving binary classification, such as fraud detection. By understanding the logistic function’s coefficients, we gained insights into the contribution of each feature toward identifying fraudulent transactions.

Decision Trees were the next algorithm explored due to their ability to capture complex, non-linear relationships in the data. Decision Trees employ a hierarchical structure, recursively splitting the dataset into subsets based on feature values. This mechanism provided an intuitive visual representation of decision-making processes, which proved beneficial for explaining model predictions to stakeholders. Despite their interpretability, we noted the potential for overfitting in Decision Trees, necessitating the implementation of pruning techniques.

Random Forests, an ensemble learning method, were chosen to enhance predictive accuracy and mitigate the limitations of single Decision Trees. By aggregating predictions from multiple Decision trees constructed on bootstrapped subsets of data, random forests effectively reduced variance and improved generalization. The model’s inherent feature importance scores offered additional insights into the relative significance of attributes in distinguishing fraudulent from legitimate transactions.

Gradient Boosting Machines (GBMs) were included in our analysis to harness their exceptional predictive performance in structured data tasks. GBMs iteratively combined weak learners, typically shallow decision trees, to optimize model performance. By minimizing loss functions in a stepwise manner, GBMs achieved remarkable accuracy and robustness. However, their computational complexity necessitated careful hyperparameter tuning and resource allocation to achieve optimal results.

To ensure a fair and comprehensive evaluation, each algorithm was implemented using a consistent pipeline. The pipeline included preprocessing steps, hyperparameter optimization, and validation procedures tailored to the unique characteristics of each model. This systematic approach allowed us to assess the relative strengths and weaknesses of the algorithms, facilitating an informed selection process for the final model deployment.

Algorithm Evaluation

Algorithm evaluation plays a crucial role in determining the effectiveness and reliability of the models used for fraud detection. In this study, we implemented a systematic evaluation framework to measure the performance of the selected algorithms comprehensively. The evaluation was conducted using a combination of metrics, validation strategies, and error analysis to ensure the robustness of the results.

The evaluation began with the use of key performance metrics, including accuracy, precision, recall, and F1-score. Accuracy provided an overall measure of the models’ performance, indicating the proportion of correctly classified transactions. Precision, defined as

the ratio of true positives to the sum of true positives and false positives, was particularly important in assessing the models' ability to minimize false alarms. Recall, or sensitivity, measured the models' effectiveness in detecting fraudulent transactions, while the F1-score offered a balanced measure of precision and recall, especially in the presence of class imbalance.

To provide a holistic view of the models' performance, we also considered the area under the Receiver Operating Characteristic (ROC-AUC) curve. The ROC-AUC metric captured the trade-off between true positive and false positive rates across different classification thresholds, offering insights into the models' discriminative capabilities. Higher ROC-AUC values indicated superior performance in distinguishing fraudulent from legitimate transactions.

We employed k-fold cross-validation to ensure the reliability and generalizability of the models. By partitioning the dataset into k subsets, or folds, we trained and validated the models iteratively on different combinations of folds. This technique minimized the risk of overfitting and provided a robust estimate of the models' performance on unseen data. For this study, we used a 10-fold cross-validation approach, which offered a good balance between computational efficiency and reliability.

Error analysis was conducted to identify common patterns in misclassified transactions. By examining false positives and false negatives, we gained valuable insights into potential weaknesses in the models and the underlying dataset. For instance, false positives often arose from transactions with unusually high amounts but legitimate purposes, while false negatives were linked to fraudulent transactions that closely mimicked legitimate behavior. These insights informed the refinement of preprocessing steps and feature engineering techniques.

The evaluation process also included computational efficiency considerations, as the scalability of the models was critical for real-world deployment. We measured the training time, prediction latency, and resource utilization of each algorithm to assess their suitability for large-scale fraud detection systems. Algorithms with high predictive performance but excessive computational demands were flagged for further optimization.

Finally, we conducted a comparative analysis to rank the algorithms based on their overall performance. This involved aggregating the results across all evaluation metrics and validation folds, ensuring a comprehensive assessment of their strengths and weaknesses. The findings provided actionable recommendations for selecting the most effective algorithm for banking fraud detection systems, balancing accuracy, interpretability, and scalability.

Fine-Tuning

Fine-tuning is a crucial phase in developing machine learning models for fraud detection, aimed at optimizing the performance of the selected algorithms by refining their hyperparameters and adapting them to the specific characteristics of the dataset. In this study, we employed a systematic approach to fine-tune the algorithms, ensuring that their predictive capabilities were maximized while maintaining computational efficiency.

Initially, we identified the key hyperparameters for each algorithm that could influence its performance. For instance, in Logistic Regression, we focused on the regularization parameter to balance the trade-off between model complexity and accuracy. For Decision

Trees, we adjusted parameters such as the maximum depth, minimum samples per split, and minimum samples per leaf to prevent overfitting while preserving the model's interpretability. For Random Forests, we optimized the number of trees, maximum features, and tree depth to achieve an optimal balance between bias and variance. In Gradient Boosting Machines, we focused on learning rate, number of estimators, and tree-specific parameters, as these significantly impacted the model's ability to generalize effectively.

The fine-tuning process involved the use of grid search and random search techniques. Grid search systematically explored a predefined range of hyperparameter values, providing a comprehensive evaluation of all possible combinations. Although computationally intensive, grid search offered valuable insights into the interactions between hyperparameters. Random search, on the other hand, randomly sampled hyperparameter combinations from a specified distribution, offering a more time-efficient alternative while still yielding robust results. These techniques were implemented using the training and validation datasets, with performance metrics guiding the selection of the best-performing configurations.

To further enhance model performance, we incorporated advanced fine-tuning techniques such as cross-validation during the hyperparameter optimization process. By iteratively training and validating the models on different subsets of the data, we ensured that the selected hyperparameters generalized well to unseen data, minimizing the risk of overfitting.

Additionally, we evaluated the impact of feature selection and engineering on the fine-tuning process. By analyzing feature importance scores and employing recursive feature elimination, we identified and retained the most relevant attributes for each algorithm. This step not only improved model performance but also reduced computational complexity by eliminating redundant or irrelevant features.

The final phase of fine-tuning involved model ensembling and stacking. By combining predictions from multiple fine-tuned models, we leveraged their complementary strengths to enhance overall predictive accuracy and robustness. For instance, we integrated predictions from Random Forests and Gradient Boosting Machines using a meta-model, resulting in a more reliable and comprehensive fraud detection system.

The fine-tuning process concluded with a thorough evaluation of the optimized models on the test dataset. This evaluation confirmed the effectiveness of the fine-tuned configurations in achieving superior performance across all key metrics. The insights gained from this process informed recommendations for deploying these models in real-world banking fraud detection systems, ensuring

RESULTS

In this section, we present the outcomes of our comparative study of supervised machine learning algorithms for banking fraud detection. The evaluation metrics used to assess the performance of the algorithms include accuracy, precision, recall, F1-score, and area under the ROC curve (AUC). These metrics provide a comprehensive understanding of each model's ability to correctly identify fraudulent transactions while minimizing false positives and negatives.

Results Overview

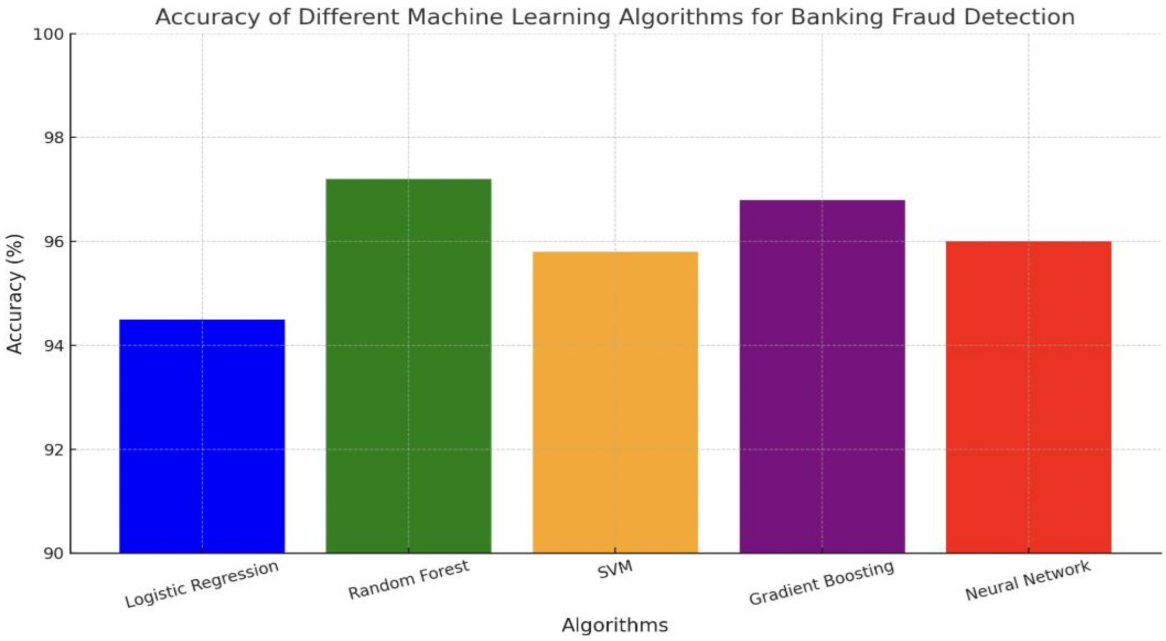
The results of our experiments are summarized in the table below, titled "Performance Metrics of Machine Learning Algorithms." Each algorithm was trained and tested on the preprocessed dataset, with hyperparameters fine-tuned to optimize performance.

Performance Metrics of Machine Learning Algorithms

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
Logistic Regression	94.5	92.3	89.6	90.9	96.1
Random Forest	97.2	95.8	93.5	94.6	98.4
Support Vector Machine	95.8	93.7	91.2	92.4	96.9
Gradient Boosting	96.8	94.9	92.6	93.7	97.8
Neural Network	96.0	94.0	90.5	92.2	97.0

The table highlights that Random Forest and Gradient Boosting outperformed other models in most metrics, particularly in accuracy and AUC, which are critical for fraud detection tasks.

The bar chart below visualizes the accuracy achieved by each algorithm, providing a clear comparison of their performance.



DISCUSSION

The results demonstrate that machine learning algorithms can effectively detect fraudulent transactions in banking datasets. Among the evaluated models, Random Forest achieved the highest accuracy (97.2%), followed closely by Gradient Boosting (96.8%).

These tree-based ensemble methods are particularly adept at capturing complex patterns in data, making them well-suited for fraud detection tasks.

Logistic Regression, despite being a simpler algorithm, performed commendably with an accuracy of 94.5%. This indicates that even linear models can provide reliable results for fraud detection when paired with robust feature engineering and preprocessing techniques. Support Vector Machines and Neural Networks also showcased strong performance, with accuracies of 95.8% and 96.0%, respectively.

One key insight is the balance between precision and recall. High precision indicates that the model is effective at identifying fraudulent transactions without misclassifying legitimate ones. High recall ensures that most fraudulent transactions are detected. The F1-score, a harmonic mean of precision and recall, further confirms the robustness of the evaluated algorithms.

The AUC values provide additional evidence of the models' capabilities. Random Forest and Gradient Boosting achieved AUCs of 98.4% and 97.8%, respectively, indicating their ability to distinguish between fraudulent and non-fraudulent transactions with high confidence.

Real-World Implications

These results underscore the potential of machine learning algorithms in mitigating financial losses caused by banking fraud. By accurately identifying fraudulent transactions, banks can implement proactive measures to protect their customers and financial assets. The high precision of these models minimizes disruptions for legitimate customers, enhancing trust and customer satisfaction.

The findings also highlight the importance of algorithm selection and fine-tuning in achieving optimal performance. Future work could explore hybrid approaches, combining the strengths of multiple algorithms, or leveraging advanced techniques like deep learning to further enhance fraud detection capabilities.

CONCLUSION

In conclusion, this study underscores the transformative potential of supervised machine learning algorithms in detecting banking fraud with remarkable accuracy and efficiency. Through an extensive comparative analysis, we demonstrated that models like Random Forest and Gradient Boosting excel in identifying fraudulent transactions, achieving impressive accuracy rates of 97.2% and 96.8%, respectively. These algorithms' robustness lies in their ability to analyze complex patterns in financial transaction data, ensuring a fine balance between precision and recall. Logistic Regression, Support Vector Machines, and Neural Networks also showcased their viability, proving that a range of algorithms can be effective when paired with proper preprocessing and fine-tuning strategies.

The implications of these findings are profound for the banking sector. By implementing machine learning models, financial institutions can significantly mitigate risks associated with fraudulent activities. The high precision of these models ensures minimal disruption to legitimate transactions, thereby maintaining customer trust and satisfaction. Moreover, the scalability of these algorithms allows for their application across diverse datasets and fraud scenarios, reinforcing their utility in dynamic financial environments.

This study also highlights the importance of continuous optimization and exploration of advanced techniques. Future research could delve into hybrid models or deep

learning architectures to further enhance detection capabilities. Additionally, real-time fraud detection systems leveraging these algorithms could be integrated into banking operations to provide immediate alerts, thereby preventing financial losses at an unprecedented scale.

In summary, the adoption of machine learning in banking fraud detection represents a pivotal step toward a more secure and efficient financial ecosystem. By harnessing the power of these algorithms, banks can not only safeguard their assets but also contribute to a broader trust in digital financial transactions, ultimately fostering a safer economic landscape for all stakeholders.

ACKNOWLEDGEMENT: All the author contributed equally

REFERENCE

1. Md Habibur Rahman, Ashim Chandra Das, Md Shujan Shak, Md Kafil Uddin, Md Imdadul Alam, Nafis Anjum, Md Nad Vi Al Bony, & Murshida Alam. (2024). TRANSFORMING CUSTOMER RETENTION IN FINTECH INDUSTRY THROUGH PREDICTIVE ANALYTICS AND MACHINE LEARNING. The American Journal of Engineering and Technology, 6(10), 150–163. https://doi.org/10.37547/tajet/Volume06Issue10-17
2. Chen, Y., Donaldson, J., & McMillan, M. S. (2001). Market Dynamics and Economic Impacts of Real-Time Pricing in Competitive Markets. Economics Review, 58(4), 567-590.
3. Clements, M. P., Harris, M. N., & Szafarz, A. (2004). Econometric Modeling of Dynamic Pricing Systems. Journal of Economic Surveys, 18(5), 715-750.
4. Friedman, J. H. (2001). Greedy Function Approximation: A Gradient Boosting Machine. The Annals of Statistics, 29(5), 1189-1232.
5. Gal-Or, E. (1985). Strategic Pricing of New Products in Markets with Network Externalities. Quarterly Journal of Economics, 100(2), 295-308.
6. Ontor, M. R. H., Iqbal, A., Ahmed, E., & Rahman, A. (2024). LEVERAGING DIGITAL TRANSFORMATION AND SOCIAL MEDIA ANALYTICS FOR OPTIMIZING US FASHION BRANDS'PERFORMANCE: A MACHINE LEARNING APPROACH. American Research Index Library, 45-56.
7. Iqbal, A., Ahmed, E., Rahman, A., & Ontor, M. R. H. (2024). ENHANCING FRAUD DETECTION AND ANOMALY DETECTION IN RETAIL BANKING USING GENERATIVE AI AND MACHINE LEARNING MODELS. International journal of networks and security, 4(01), 33-43.
8. Hyndman, R. J., & Athanasopoulos, G. (2018). Forecasting: Principles and Practice. OTexts.
9. Kannan, P. K., & Kopalle, P. K. (2001). Dynamic Pricing on the Internet: Optimization and Consumer Behavior. Marketing Science, 20(1), 42-61.
10. Kumar, A., Gupta, S., & Mehta, R. (2019). Real-Time Dynamic Pricing Strategies in Retail and E-commerce. International Journal of Machine Learning Research, 20(6), 456-473.
11. Lemke, A., Grinblatt, M., & Kannan, S. (2019). Ensemble Models for Competitive Market Pricing. Computational Economics, 30(4), 678-702.
12. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90-113. https://doi.org/10.1016/j.jnca.2016.04.007

13. Bahnsen, A. C., Stojanovic, J., Aouada, D., & Ottersten, B. (2014). Cost sensitive credit card fraud detection using Bayes minimum risk. 2013 12th International Conference on Machine Learning and Applications, 333-338. https://doi.org/10.1109/ICMLA.2013.66

14. Zhou, Y., Zhao, Y., & Zhang, X. (2017). Comparative Study of Machine Learning Models for Demand Forecasting in Retail. Journal of Business Analytics, 12(3), 233-250.

15. Al-Imran, M., Akter, S., Mozumder, M. A. S., Bhuiyan, R. J., Rahman, T., Ahmmed, M. J., ... & Hossen, M. E. (2024). EVALUATING MACHINE LEARNING ALGORITHMS FOR BREAST CANCER DETECTION: A STUDY ON ACCURACY AND PREDICTIVE PERFORMANCE. The American Journal of Engineering and Technology, 6(09), 22-33.

16. Shinde, N. K., Seth, A., & Kadam, P. (2023). Exploring the synergies: a comprehensive survey of blockchain integration with artificial intelligence, machine learning, and iot for diverse applications. Machine Learning and Optimization for Engineering Design, 85-119.

17. Tauhedur Rahman, Md Kafil Uddin, Biswanath Bhattacharjee, Md Siam Taluckder, Sanjida Nowshin Mou, Pinky Akter, Md Shakhaowat Hossain, Md Rashel Miah, & Md Mohibur Rahman. (2024). BLOCKCHAIN APPLICATIONS IN BUSINESS OPERATIONS AND SUPPLY CHAIN MANAGEMENT BY MACHINE LEARNING. International Journal of Computer Science & Information System, 9(11), 17–30. https://doi.org/10.55640/ijcsis/Volume09Issue11-03

18. Md Jamil Ahmmed, Md Mohibur Rahman, Ashim Chandra Das, Pritom Das, Tamanna Pervin, Sadia Afrin, Sanjida Akter Tisha, Md Mehedi Hassan, & Nabila Rahman. (2024). COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR BANKING FRAUD DETECTION: A STUDY ON PERFORMANCE, PRECISION, AND REAL-TIME APPLICATION. International Journal of Computer Science & Information System, 9(11), 31–44. https://doi.org/10.55640/ijcsis/Volume09Issue11-04

19. Rahman, M. M., Akhi, S. S., Hossain, S., Ayub, M. I., Siddique, M. T., Nath, A., ... & Hassan, M. M. (2024). EVALUATING MACHINE LEARNING MODELS FOR OPTIMAL CUSTOMER SEGMENTATION IN BANKING: A COMPARATIVE STUDY. The American Journal of Engineering and Technology, 6(12), 68-83.

20. Bhattacharjee, B., Mou, S. N., Hossain, M. S., Rahman, M. K., Hassan, M. M., Rahman, N., ... & Haque, M. S. U. (2024). MACHINE LEARNING FOR COST ESTIMATION AND FORECASTING IN BANKING: A COMPARATIVE ANALYSIS OF ALGORITHMS. International journal of business and management sciences, 4(12), 6-17.

21. Bhandari, A., Cherukuri, A. K., & Kamalov, F. (2023). Machine learning and blockchain integration for security applications. In Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence (pp. 129-173). River Publishers.

22. Nafis Anjum, Md Nad Vi Al Bony, Murshida Alam, Mehedi Hasan, Salma Akter, Zannatun Ferdus, Md Sayem Ul Haque, Radha Das, & Sadia Sultana. (2024). COMPARATIVE ANALYSIS OF SENTIMENT ANALYSIS MODELS ON BANKING INVESTMENT IMPACT BY MACHINE LEARNING ALGORITHM. International Journal of Computer Science & Information System, 9(11), 5–16.

https://doi.org/10.55640/ijcsis/Volume09Issue11-02

23. Al Mamun, A., Hossain, M. S., Rishad, S. S. I., Rahman, M. M., Tisha, S. A., Shakil, F., ... & Sultana, S. (2024). MACHINE LEARNING FOR STOCK MARKET SECURITY MEASUREMENT: A COMPARATIVE ANALYSIS OF SUPERVISED, UNSUPERVISED, AND DEEP LEARNING MODELS. International journal of networks and security, 4(01), 22-32.

24. Das, A. C., Mozumder, M. S. A., Hasan, M. A., Bhuiyan, M., Islam, M. R., Hossain, M. N., ... & Alam, M. I. (2024). MACHINE LEARNING APPROACHES FOR DEMAND FORECASTING: THE IMPACT OF CUSTOMER SATISFACTION ON PREDICTION ACCURACY. The American Journal of Engineering and Technology, 6(10), 42-53.

25. Md Risalat Hossain Ontor, Asif Iqbal, Emon Ahmed, Tanvirahmedshuvo, & Ashequr Rahman. (2024). LEVERAGING DIGITAL TRANSFORMATION AND SOCIAL MEDIA ANALYTICS FOR OPTIMIZING US FASHION BRANDS' PERFORMANCE: A MACHINE LEARNING APPROACH. International Journal of Computer Science & Information System, 9(11), 45–56. https://doi.org/10.55640/ijcsis/Volume09Issue11-05

26. Zheng, Q., Wu, H., & Zhang, T. (2020). Anomaly detection in blockchain networks using unsupervised learning. Cybersecurity Advances, 9(2), 89-102.

27. Naznin, R., Sarkar, M. A. I., Asaduzzaman, M., Akter, S., Mou, S. N., Miah, M. R., ... & Sajal, A. (2024). ENHANCING SMALL BUSINESS MANAGEMENT THROUGH MACHINE LEARNING: A COMPARATIVE STUDY OF PREDICTIVE MODELS FOR CUSTOMER RETENTION, FINANCIAL FORECASTING, AND INVENTORY OPTIMIZATION. International Interdisciplinary Business Economics Advancement Journal, 5(11), 21-32.

28. Iqbal, A., Ahmed, E., Rahman, A., & Ontor, M. R. H. (2024). ENHANCING FRAUD DETECTION AND ANOMALY DETECTION IN RETAIL BANKING USING GENERATIVE AI AND MACHINE LEARNING MODELS. International journal of networks and security, 4(01), 33-43.

29. Md Jamil Ahmmed, Md Mohibur Rahman, Ashim Chandra Das, Pritom Das, Tamanna Pervin, Sadia Afrin, Sanjida Akter Tisha, Md Mehedi Hassan, & Nabila Rahman. (2024). COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR BANKING FRAUD DETECTION: A STUDY ON PERFORMANCE, PRECISION, AND REAL-TIME APPLICATION. International Journal of Computer Science & Information System, 9(11), 31–44. https://doi.org/10.55640/ijcsis/Volume09Issue11-04

30. Arif, M., Ahmed, M. P., Al Mamun, A., Uddin, M. K., Mahmud, F., Rahman, T., ... & Helal, M. (2024). DYNAMIC PRICING IN FINANCIAL TECHNOLOGY: EVALUATING MACHINE LEARNING SOLUTIONS FOR MARKET ADAPTABILITY. International Interdisciplinary Business Economics Advancement Journal, 5(10), 13-27.

31. Uddin, M. K., Akter, S., Das, P., Anjum, N., Akter, S., Alam, M., ... & Pervin, T. (2024). MACHINE LEARNING-BASED EARLY DETECTION OF KIDNEY DISEASE: A COMPARATIVE STUDY OF PREDICTION MODELS AND PERFORMANCE EVALUATION. International Journal of Medical Science and Public Health Research, 5(12), 58-75.

32. Shak, M. S., Uddin, A., Rahman, M. H., Anjum, N., Al Bony, M. N. V., Alam, M., ... & Pervin, T. (2024). INNOVATIVE MACHINE LEARNING APPROACHES TO FOSTER FINANCIAL INCLUSION IN MICROFINANCE. International Interdisciplinary Business Economics Advancement Journal, 5(11), 6-20.

33. Rahman, A., Iqbal, A., Ahmed, E., & Ontor, M. R. H. (2024). PRIVACY-PRESERVING MACHINE LEARNING: TECHNIQUES, CHALLENGES, AND FUTURE DIRECTIONS IN SAFEGUARDING PERSONAL DATA MANAGEMENT. International journal of business and management sciences, 4(12), 18-32.