International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Analyzing the Impact of Machine Learning Algorithms on Risk Management and Fraud Detection in Financial Institution

Deepak Kumar [a], ***Shoumya Singh*** [b]

[a,] *Department of Information Technology, University of the Cumberlands, KY, USA*
[b] *Department of Computer Science, San Francisco Bay University, CA, USA*

DOI: https://doi.org/10.55248/gengpi.5.0524.1135

ABSTRACT

This study examines the impact of machine learning algorithms on risk management and fraud detection in financial institutions. Machine learning has the potential to be integrated into various decision-making systems. In recent years, the ability of machine learning algorithms to analyze large datasets and provide precise predictions has attracted significant attention across multiple sectors. Accurate risk assessment and fraud prevention are crucial for financial institutions to avoid potential financial losses and damage to their reputation. Machine learning algorithms have enabled financial institutions to adopt more efficient and effective strategies to mitigate these risks. Financial institutions increasingly utilize machine learning algorithms to improve risk management and fraud detection. These algorithms employ advanced statistical techniques to analyze massive datasets and identify patterns and anomalies that may indicate potential risks or fraudulent activities. The most widely used machine learning algorithms in risk management and fraud detection are supervised learning algorithms like logistic regression and decision trees and unsupervised learning algorithms like clustering and anomaly detection. These algorithms can process and analyze vast amounts of data in real time, allowing financial institutions to detect and respond more effectively to potential risks and fraudulent activities.

Keywords: *Finance, Banking, Information Technology, Internet of Things, Machine Learning, Artificial Intelligence*

1. Introduction:

Various machine learning techniques can aid in managing risks in financial institutions. Logistic regression and decision trees are two examples of supervised learning algorithms that can be used to predict credit, market, and operational risks by analyzing historical data and learning patterns and relationships between different risk factors(Ashta & Herrmann, 2021). Logistic regression, for instance, can assess the likelihood of a customer defaulting on a loan based on their credit history and other relevant variables. Similarly, decision trees can be used to evaluate market risks by analyzing past market data and identifying key variables contributing to the risk(Jain et al., 2020). Moreover, unsupervised learning algorithms, such as clustering and anomaly detection, are also valuable for risk management in financial institutions. Clustering algorithms can group similar customer profiles or financial transactions, enabling institutions to identify higher-risk segments and develop targeted risk mitigation strategies. For instance, k-means clustering can be used to group customers based on their purchasing behavior and identify segments with a higher likelihood of default or fraud(Singla & Jangir, 2020). Successful case studies indicate that machine learning can improve accuracy and efficiency in risk management, including credit risk assessment, where a major financial institution reported a significant reduction in default rates and an improved loan approval process. Machine learning algorithms are also effective in fraud detection within financial institutions(Uchhana et al., 2021). For example, a study analyzed the performance of various machine learning models, including logistic regression, random forest, and decision trees, in detecting fraudulent credit card transactions and found that these algorithms could accurately detect fraudulent transactions with high precision and recall rates(Nanduri et al., 2020). Additionally, machine learning algorithms can analyze large volumes of data in real time to detect patterns and anomalies that may indicate fraudulent activity. Lin et al. found that combining supervised and unsupervised machine learning algorithms, including logistic regression, support vector machines, and random forests, could effectively identify fraudulent transactions with high accuracy rates(Uchhana et al., 2021). Machine learning algorithms have transformed risk management and fraud detection in financial institutions by providing a more advanced and efficient approach to identifying and mitigating risks and detecting fraud(Sadineni, 2020). As financial transactions become increasingly complex and voluminous, traditional rule-based risk management and fraud detection methods are no longer sufficient(Kousika et al., 2021). Machine learning algorithms offer several advantages in risk management and fraud detection within financial institutions.

2. Machine Learning Techniques for Risk Management:

The progress of telemedicine has been considerable as an outcome of improvements in technology and a growing demand for healthcare that is both accessible and efficient. Machine learning techniques have become increasingly popular in risk management within financial institutions. These techniques leverage advanced algorithms to analyze large datasets and identify patterns or trends that may indicate potential risks(Amarasinghe et al., 2018). One of the key benefits of machine learning is its ability to process and analyze large amounts of data in real time, enabling prompt detection and response to potential risks or fraudulent activities. Moreover, machine learning algorithms can adapt and learn from new data, improving their accuracy and effectiveness. Another advantage of machine learning is its ability to identify complex patterns and correlations in data that may take time to be apparent to human analysts(Hu et al., 2021). This capability is particularly crucial in detecting fraud, as fraudsters constantly evolve tactics to avoid detection(Uchhana et al., 2021). Machine learning algorithms can be classified into two broad categories: supervised and unsupervised learning techniques. Supervised learning techniques involve training algorithms on labeled data, while unsupervised learning techniques involve identifying patterns in unlabeled data(Nanduri et al., 2020). Overall, machine learning techniques are an invaluable tool for financial institutions seeking to mitigate risks and protect themselves from potentially fraudulent activity(Nanduri et al., 2020). By leveraging these techniques, organizations can analyze vast amounts of data more effectively, identify key patterns and correlations, and respond more promptly to potential risks.

2.1 Supervised learning:

Supervised and unsupervised learning algorithms have become increasingly popular in the domains of risk management and fraud detection. Supervised learning algorithms require labeled training data, which involves providing the algorithm with inputs and their corresponding correct outputs(Singla & Jangir, 2020). This enables the algorithm to learn from the labeled data and make predictions or classifications based on new, unseen data. Logistic regression, decision trees, random forests, and support vector machines are some of the commonly used supervised learning algorithms in risk management and fraud detection(Hu et al., 2021).On the other hand, unsupervised learning algorithms do not require labeled data. Instead, they rely on clustering and anomaly detection techniques to identify patterns and anomalies within the data(Abinayaa et al., 2020). K-means clustering, DBSCAN, and Isolation Forest are some of the popular unsupervised learning algorithms used in risk management and fraud detection(Robisco & Martínez, 2022). Figure 1 describes the different steps in Supervised Learning process which includes data gathering, model evaluation, and testing of model. Regression algorithms are widely employed in risk management to predict and assess credit risk, market risk, and operational risk (Gonaygunta, H,2023). These algorithms use historical data to create models that can predict the likelihood and severity of different risks. Author has highlighted the importance of such algorithms in enabling businesses to make informed decisions about risk management and fraud detection (Amarasinghe et al., 2018).

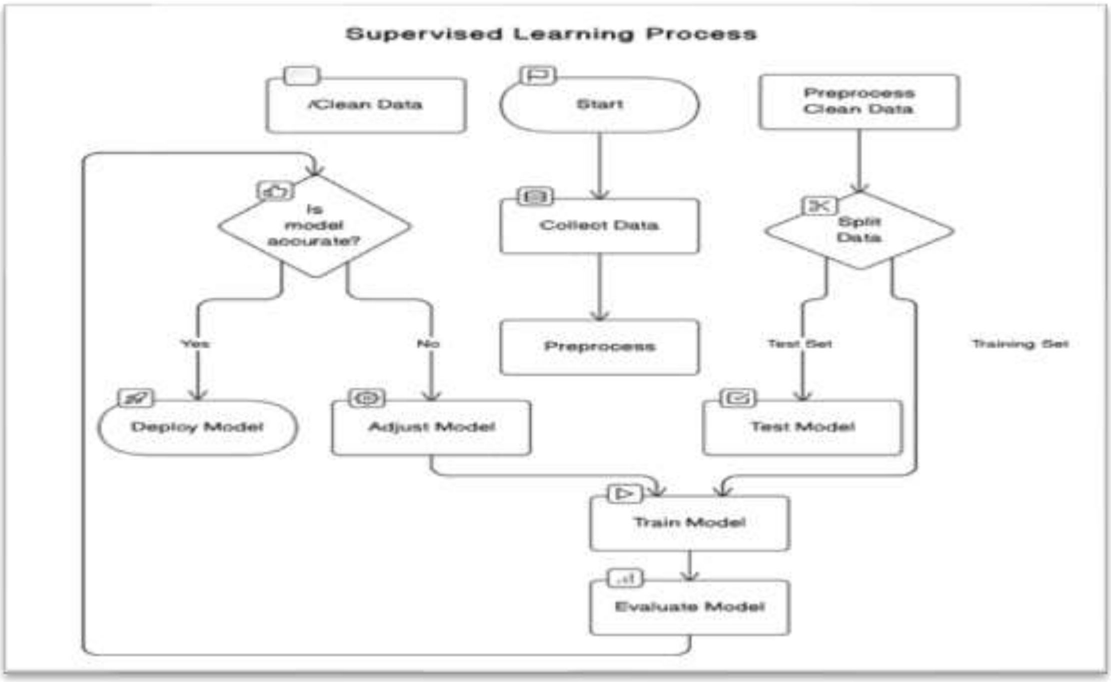

Figure1. *Supervised learning process for fraud detection*

2.2 Unsupervised Learning:

Unsupervised learning algorithms are used to identify patterns and anomalies in data without the need for labeled training data. This type of machine learning allows for discovering hidden patterns and relationships within the data, which can be highly beneficial for risk management and fraud detection(Nanduri et al., 2020).

These algorithms use clustering techniques to group similar data points and identify outliers or anomalies. Some case studies have showcased successful implementations of machine learning in risk management, such as using clustering algorithms to identify patterns of fraudulent behavior in credit card transactions(Jain et al., 2020). For instance, a study found that using unsupervised learning algorithms such as K-means clustering and DBSCAN helped identify clusters of fraudulent transactions based on common characteristics such as transaction amount, location, and frequency(Talavera et al., 2019). Another study utilized unsupervised learning algorithms like Isolation Forest to detect anomalies in financial data, helping identify potential fraud cases.

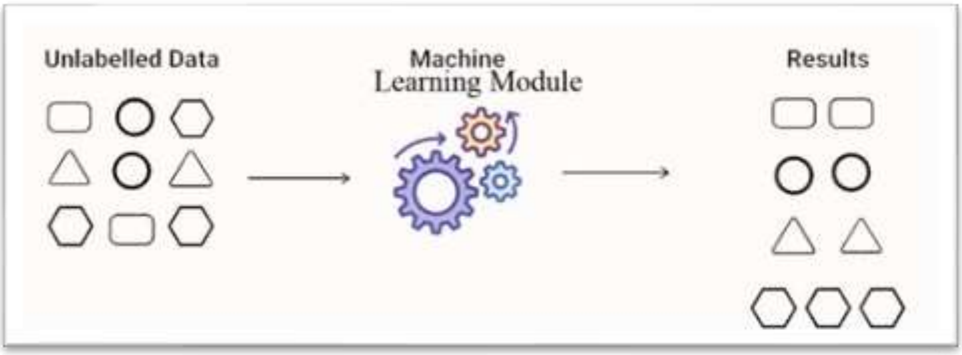

***Figure 2**: Unsupervised Learning*

2.3 Application of regression, classification, and clustering algorithms to predict credit, market, and operational risks:

The application of machine learning algorithms has proven to be an effective solution for predicting and mitigating various types of risks in financial institutions. These algorithms offer a wide range of capabilities, such as regression algorithms like linear regression and logistic regression, which can be utilized to assess credit risk by analyzing factors such as credit scores, income levels, and past repayment history(Senatobia et al., 2018). Moreover, classification algorithms, such as decision trees and random forests, can be employed to identify different levels of market risk by analyzing market data and indicators(Uchhana et al., 2021). Additionally, clustering algorithms like K-means clustering can be used to group customers or transactions with similar characteristics and identify potential patterns of fraudulent behavior(Aziz & Dowling, 2018).Case studies have demonstrated successful implementations of machine learning in risk management and fraud detection in financial institutions. One such study used machine learning algorithms to detect credit card fraud (Karthik Meduri, 2024). The study utilized a supervised learning algorithm, such as a support vector machine or a random forest classifier, to train a model on historical credit card transaction data and predict whether future transactions are fraudulent(Ashta & Herrmann, 2021). Another case study focused on the application of machine learning in market risk management. The study used regression and classification algorithms to analyze market data and identify potential risks(Uchhana et al., 2021). In conclusion, adopting machine learning algorithms has significantly impacted risk management and fraud detection in financial institutions(Duan, 2020). These algorithms provide more accurate and efficient methods for assessing and predicting risks, enabling financial institutions to protect themselves against fraud better and make more informed decisions(Sun, 2021). In today's rapidly changing world, accurate risk assessment and fraud prevention in financial institutions cannot be overstated.

2.4 Machine Learning for Fraud Detection:

The financial industry is plagued with the threat of fraudulent activities, posing significant risks to banking systems and the corporate financial sector. However, with the advent of technology, machine-learning techniques have emerged as practical tools for detecting and preventing financial fraud(Ashta & Herrmann, 2021). Machine learning algorithms analyze large transactional data sets to identify patterns and anomalies that can indicate fraudulent activity. Supervised learning algorithms, such as support vector machines or random forest classifiers, can train models to recognize fraudulent patterns based on historical transaction data and enable predictions about the likelihood of fraud in future transactions (Moreira et al., 2022). Unsupervised learning algorithms can also identify outliers or anomalies in financial data that may indicate fraudulent behavior. Machine learning techniques can be applied to various types of risk management in financial institutions(Liebergen, 2017). Regression algorithms can be utilized for credit risk assessment, predicting the creditworthiness of individuals or businesses based on their financial data and credit history(Amarasinghe et al., 2018). Classification algorithms can categorize individuals or businesses based on their credit risk level. In contrast, regression and classification algorithms can be used for market risk assessment, analyzing market data to identify potential risks and predict future market movements(Moreira et al., 2022). Steps in Figure 3 is about different steps of Machine Learning related to fraud detection.

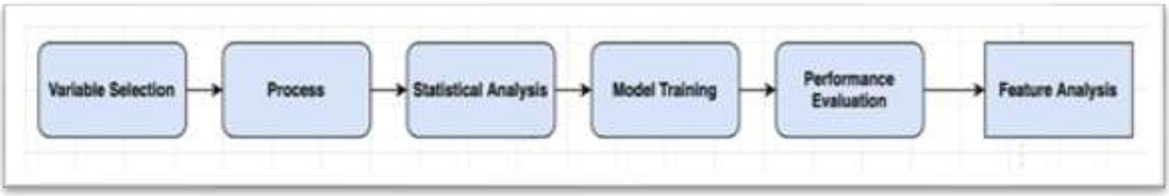

***Figure 3**. Different steps in Machine Learning to find fraud in transactions*

Several case studies have demonstrated the successful implementation of machine learning algorithms in risk management and fraud detection in financial institutions. For instance, a study by Lellis Moreira et al. analyzed the effectiveness of three machine learning algorithms, including Random Forest, Decision Tree, and XGBOOST, in detecting credit card fraud(Moreira et al., 2022). The study found that the Random Forest algorithm had the highest accuracy in detecting fraudulent transactions compared to the other two(Sadineni, 2020). Another case study focused on using machine learning algorithms for fraud classification prediction in a banking network. The study utilized a dataset with over six million records of financial transactions and implemented various machine learning algorithms, including Logistic Regression, Naive Bayes, KNN, and KNN(Jain et al., 2020). The study aimed to balance and train the dataset by employing techniques such as Random Sampling, SMOTE, and ADASYN, which helped enhance the accuracy of fraud classification predictions and overall fraud detection capabilities of the banking network(Addo et al., 2018).

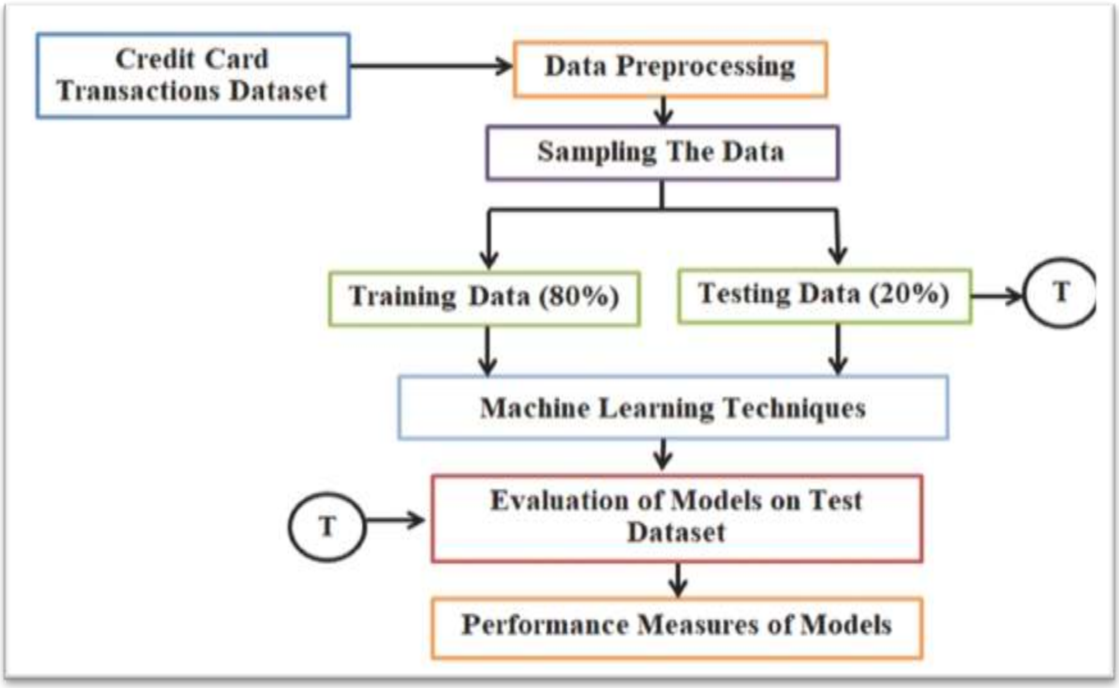
Credit Card Transactions Dataset
Data Preprocessing
Sampling The Data
Training Data (80%)
Testing Data (20%)
T
Machine Learning Techniques
T
Evaluation of Models on Test Dataset
Performance Measures of Models

Figure 4*. Credit card fraud detection using Machine Learning*

Figure 4 describes the different steps of fraud detection based on the Credit card real-time data, which might take in fraction of seconds (Azim et al., 2024). The whole infrastructure is based on the big data and distributed systems, which can process the data in real-time and provides decision based on trained and input data. To conclude, applying machine learning algorithms in risk management and fraud detection in financial institutions has shown promising results. Using supervised and unsupervised learning techniques and regression and classification algorithms can improve the accuracy of credit and market risk assessments and enhance the detection of fraudulent activities in financial institutions(Abinayaa et al., 2020). Therefore, adopting machine learning techniques in the financial industry can provide effective risk management solutions and protect financial institutions from fraud. Examining anomaly detection algorithms is a crucial aspect of machine learning in risk management and fraud detection in financial institutions(Hu et al., 2021). Anomaly detection algorithms are helpful in identifying patterns or behaviors that deviate from everyday activities, indicating potential fraud or unusual risks(Moreira et al., 2022).

Algorithm Description:

The algorithm utilizes a dataset of credit card transactions to predict whether each transaction is legitimate or fraudulent. It begins by splitting the dataset into training and testing data. Then, it applies a sampling technique to the dataset to balance the classes if necessary. Next, it trains several individual machine learning models (e.g., Logistic Regression, Random Forest, XGBoost) on the training data and evaluates their performance on the testing data. Afterward, it selects the top-performing models and creates an ensemble model using soft voting, where the predictions of each model are combined with weights assigned based on their performance. Finally, the ensemble model is used to make predictions on the testing data. Following is the proposed algorithm for fraud detection used in banking industries (Azim et al., 2024).

Algorithm Steps:

1. Split data (dataset):

- Split the dataset into training and testing data.

- Return the training and testing datasets.

2. Data sampling (dataset):

```
  - Apply a sampling technique to balance the classes in the dataset.
  - Return the sampled dataset.
3. Ensemble model (Training_dataset, Testing_data):
  - Create instances of the top-performing individual models (e.g., Random Forest, XGBoost, MLP).
  - Fit each individual model on the training data.
  - Assign weights to the models based on their performance with validation data.
  - Create a soft voting ensemble with the models and weights.
  - Fit the ensemble on the training data.
  - Make predictions using the ensemble model.
  - Return the predictions.
```

Usages:

1. Apply the ‘datasampling’ function to balance the classes in the dataset.

2. Use the ‘Split_data’ function to split the sampled dataset into training and testing data.

3. Call the ‘ensemble_model’ function with the training and testing data as inputs to obtain predictions for the testing data.

Note: Ensure that the necessary machine learning libraries and modules are imported before executing the algorithm.

These algorithms analyze various features and attributes of transactions or activities, such as transaction amount, frequency, time, location, and user behavior, to detect anomalies that may indicate fraudulent behavior(Amarasinghe et al., 2018). Machine learning algorithms can also be applied to clustering analysis to identify groups or clusters of similar transactions or activities (Nadella, 2024). This approach can help identify potentially fraudulent activities and aid in the development of effective risk management strategies.

3. Challenges and Limitations:

Despite the promising results of using machine learning algorithms in risk management and fraud detection, several challenges and limitations must be considered. For example, issues around biased data, model interpretability, and ethical concerns pose significant hurdles that need to be addressed. Additionally, the constant evolution of fraud techniques requires continuous monitoring and updating of machine learning algorithms to stay ahead of fraudulent activities (Moreira et al., 2022).Furthermore, the implementation of machine learning algorithms in risk management and fraud detection may require significant computational resources, data infrastructure, and expertise. Following are the few challenges and limitations in using machine learning algorithms for risk management and fraud detection in financial institutions.

3.1 Challenges associated with implementing machine learning in financial institutions, such as data quality issues and regulatory compliance:

Implementing machine learning algorithms in financial institutions for risk management and fraud detection presents several challenges. Firstly, one of the main challenges is ensuring the quality and accuracy of the data used for training the machine learning algorithms (Jain et al., 2020). Data quality issues can arise due to incomplete or inconsistent data, errors or inaccuracies, and bias(Moreira et al., 2022) . Financial institutions must also ensure compliance with regulatory requirements when implementing machine learning algorithms(Rocha-Salazar et al., 2021). These regulations may impose restrictions on data usage and sharing and require transparency and explainability of the algorithms used. Another challenge is the interpretability of machine learning algorithms. The complexity and black-box nature of some machine learning algorithms can make it difficult for financial institutions to interpret and explain the decisions made by these algorithms(Wu et al., 2023). Moreover, the lack of necessary skillsets and expertise within financial institutions can pose a challenge when implementing machine learning algorithms for risk management and fraud detection.

3.2 Ethical considerations surrounding using machine learning for risk management and fraud detection:

Using machine learning algorithms for risk management and fraud detection raises ethical considerations. These considerations include the potential for algorithmic bias, where the algorithms may unfairly discriminate against specific individuals or groups (Fuster et al., 2021). This bias can occur if the training data used to develop the algorithms is biased or if the algorithms have inherent biases (Liebergen, 2017). Moreover, using machine learning algorithms in risk management and fraud detection may raise concerns about privacy and protecting sensitive financial information. Additionally, there needs to be more clarity about the accountability and transparency of the decisions made by machine learning algorithms(Maple et al., 2023). These algorithms are often complex and difficult to interpret, making it challenging to understand how decisions are being made. Furthermore, using machine learning algorithms in risk management and fraud detection can raise concerns about job displacement and unemployment (Moreira et al., 2022). Machine learning algorithms can potentially automate and streamline financial institutions' risk management and fraud detection processes.

3.3 Limitations of machine learning models and potential biases in algorithmic decision-making:

Machine learning models are important in financial institutions' risk management and fraud detection. However, they have certain limitations and can exhibit biases in algorithmic decision-making(Moreira et al., 2022). These limitations include their reliance on historical data, which may not reflect new types of fraud or emerging trends. Another area for improvement is overfitting, which occurs when the model becomes too specialized to the training data and performs poorly on new, unseen data(Wen et al., 2022). Moreover, machine learning models can also be influenced by biases present in the training data. These biases can arise from various sources, such as data collection methods, sample selection, or societal biases present in the data(Zhang et al., 2023). For instance, if the training data mainly consists of fraudulent transactions from a particular demographic group, the machine learning algorithm may become biased towards classifying all transactions from that group as fraudulent, leading to unfair treatment of individuals from that group(Sawangarreerak & Thanathamathee, 2021). To address these limitations and potential biases, several approaches can be implemented in developing and deploying machine learning algorithms for risk management and fraud detection in financial institutions(Lorenz, 2023). One approach is to ensure that the training data used for machine learning algorithms is diverse and representative of the overall population. This can be achieved through careful data collection strategies that include various demographic groups and transaction types(Lorenz, 2023). Another approach is implementing fairness-aware techniques that explicitly consider fairness criteria during the model training process (Meduri, K., Gonaygunta, H., & Nadella, G. 2024). These techniques aim to reduce biases and ensure that the machine learning algorithms make fair and unbiased decisions.

4. Future Directions and Opportunities:

The ever-evolving technological landscape and the proliferation of data offer many opportunities for machine learning algorithms to augment risk management and fraud detection in financial institutions (Lokanan & Sharma, 2022). One potential direction is to integrate real-time data streams into machine learning models. This approach would facilitate more accurate and prompt risk assessment and fraud detection, as the models could adapt to changing patterns and identify emerging threats (Rocha-Salazar et al., 2021). Additionally, integrating machine learning algorithms with other advanced technologies, such as natural language processing and image recognition, presents another avenue for enhancing the capabilities of risk management systems. By analyzing unstructured data, such as text or images, this integration can aid in identifying potential risks or fraudulent activities (Liu et al., 2023). Opportunities for integrating machine learning with other technologies, such as blockchain and natural language processing, could also improve the transparency and security of financial transactions, making it more difficult for fraudsters to exploit vulnerabilities in the system (Salazar et al., 2022). Another important direction for future research is the development of explainable and interpretable machine learning models (Nadella, G. S., & Vadakkethil Somanathan Pillai, S. E. 2024). These models would allow users to understand the reasoning behind the decisions made by the algorithms, providing transparency and accountability in risk management and fraud detection processes (Afriyie et al., 2023). Additionally, the development of automated machine-learning techniques holds promise in simplifying the process of building and deploying machine-learning models(Lu et al., 2023). These techniques enable financial institutions to leverage the power of machine learning without requiring extensive expertise in data science or programming.

5. Conclusion:

In summary, machine learning algorithms have made significant strides in improving risk management and fraud detection within financial institutions. These algorithms have the potential to accurately assess risk and identify fraudulent activities, which ultimately leads to increased security and protection for both financial institutions and their customers. Furthermore, integrating machine learning with other advanced technologies and developing transparent and interpretable models presents exciting opportunities for enhancing risk management systems and staying ahead of emerging threats. In today's rapidly evolving landscape, precise risk assessment and fraud prevention in financial institutions cannot be overstated. Therefore, financial institutions must embrace these technological advancements and leverage machine learning algorithms to mitigate risks, detect fraud, and secure their operations. This research paper examines the impact of machine learning algorithms on risk management and fraud detection in financial institutions, providing an overview of the algorithms themselves and how they are applied in risk management and fraud detection. The paper highlights the importance of accurate risk assessment and fraud prevention, exploring various machine learning techniques used for risk management, including supervised and unsupervised learning algorithms. It also investigates how regression, classification, and clustering algorithms are applied to predict credit, market, and operational risks. Case studies are included to showcase successful machine learning implementations in risk management.

References:

Abinayaa, S., Sangeetha, H., Karthikeyan, R A., Kailasam, S., & Piyush, D. (2020, April 30). Credit Card Fraud Detection and Prevention using Machine Learning. International journal of engineering and advanced technology, 9(4), 1199-1201. https://doi.org/10.35940/ijeat.d7327.049420

Addo, P M., Guégan, D., & Hassani, B K. (2018, April 16). Credit Risk Analysis Using Machine and Deep Learning Models. Risks, 6(2), 38-38. https://doi.org/10.3390/risks6020038

Afriyie, J K., Tawiah, K., Pels, W A., Addai-Henne, S., Dwamena, H A., Owiredu, E O., Ayeh, S A., & Eshun, J. (2023, March 1). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. Elsevier BV, 6, 100163-100163. https://doi.org/https://doi.org/10.1016/j.dajour.2023.100163

Amarasinghe, T., Aponso, A., & Krishnarajah, N. (2018, May 19). Critical Analysis of Machine Learning Based Approaches for Fraud Detection in Financial Transactions. https://doi.org/10.1145/3231884.3231894

Ashta, A., & Herrmann, H. (2021, May 1). Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance. Strategic Change, 30(3), 211-222. https://doi.org/10.1002/jsc.2404

Azim Mim, M., Majadi, N., & Mazumder, P. (2024). A soft voting ensemble learning approach for credit card fraud detection. Heliyon, 10(3). https://doi.org/10.1016/j.heliyon.2024.e25466

Aziz, S., & Dowling, M. (2018, December 7). Machine Learning and AI for Risk Management. Palgrave studies in digital business & enabling technologies, 33-50. https://doi.org/10.1007/978-3-030-02330-0_3

Duan, L. (2020, August 1). Performance Evaluation and Practical Use of Supervised Data Mining Algorithms for Credit Card Approval. https://doi.org/10.1109/cds49703.2020.00057

Fuster, A., Goldsmith-Pinkham, P., Ramadorai, T., & Walther, A. (2021, December 16). Predictably Unequal? The Effects of Machine Learning on Credit Markets. The Journal of Finance, 77(1), 5-47. https://doi.org/10.1111/jofi.13090

Gonaygunta, H. (2023). Machine learning algorithms for detection of cyber threats using logistic regression. International Journal of Smart Sensor and Adhoc Network., 36–42. https://doi.org/10.47893/ijssan.2023.1229

Hu, L., Chen, J., Vaughan, J., Aramideh, S., Yang, H., Wang, K., Sudjianto, A., & Nair, V N. (2021, May 4). Supervised Machine Learning Techniques: An Overview with Applications to Banking. International Statistical Review, 89(3), 573-604. https://doi.org/10.1111/insr.12448

Jain, V K., Agrawal, M., & Kumar, A. (2020, June 1). Performance Analysis of Machine Learning Algorithms in Credit Cards Fraud Detection. https://doi.org/10.1109/icrito48877.2020.9197762

Kousika, N., Vishali, G., Sunandhana, S., & Vijay, M. (2021, May 1). Machine Learning based Fraud Analysis and Detection System. Journal of Physics: Conference Series, 1916(1), 012115-012115. https://doi.org/10.1088/1742-6596/1916/1/012115

Karthik Meduri. (2024). Cybersecurity threats in banking: Unsupervised Fraud Detection Analysis. International Journal of Science and Research Archive, 11(2), 915–925. https://doi.org/10.30574/ijsra.2024.11.2.0505

Meduri, K., Gonaygunta, H., & Nadella, G. (2024). Enhancing cybersecurity with Artificial Intelligence: Predictive techniques and challenges in the age of IOT. International Journal of Science and Engineering Applications. https://doi.org/10.7753/ijsea1304.1007

Liebergen, B V. (2017, January 1). Machine learning: A revolution in risk management and compliance. https://econpapers.repec.org/RePEc:ris:jofitr:1592

Liu, Z., Zhang, Z., Yang, T., Wang, G., & Zhou, X. (2023, November 1). An innovative model fusion algorithm to improve the recall rate of peer-to-peer lending default customers. Elsevier BV, 20, 200272-200272. https://doi.org/https://doi.org/10.1016/j.iswa.2023.200272

Lokanan, M., & Sharma, K. (2022, June 1). Fraud prediction using machine learning: The case of investment advisors in Canada. Elsevier BV, 8, 100269-100269. https://doi.org/https://doi.org/10.1016/j.mlwa.2022.100269

Lorenz, K. (2023, January 1). Method of selecting borrowers' features for credit risk assessment. Elsevier BV, 225, 2371-2380. https://doi.org/https://doi.org/10.1016/j.procs.2023.10.228

Lu, Q., Fu, C., Nan, K., Fang, Y., Xu, J., Liu, J., Bellotti, A G., & Lee, B G. (2023, November 1). Chinese corporate fraud risk assessment with machine learning. Elsevier BV, 20, 200294. https://doi.org/https://doi.org/10.1016/j.iswa.2023.200294

Maple, C., Szpruch, Ł., Epiphaniou, G., Staykova, K S., Singh, S B., Penwarden, W., Wen, Y., Wang, Z., Hariharan, J., & Avramović, P. (2023, August 31). The AI Revolution: Opportunities and Challenges for the Finance Sector. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2308.16538

Moreira, M Â L., Rocha, C D S., Silva, D F D L., Castro, M A P D., Costa, I P D A., Gomes, C F S., & Santos, M D. (2022, January 1). Exploratory analysis and implementation of machine learning techniques for predictive assessment of fraud in banking systems. Elsevier BV, 214, 117-124. https://doi.org/https://doi.org/10.1016/j.procs.2022.11.156

Nanduri, J., Jia, Y., Oka, A., Beaver, J., & Liu, Y. (2020, January 1). Microsoft Uses Machine Learning and Optimization to Reduce E-Commerce Fraud. INFORMS journal on applied analytics, 50(1), 64-79. https://doi.org/10.1287/inte.2019.1017

Nadella, G. S., & Vadakkethil Somanathan Pillai, S. E. (2024). Examining the indirect impact of information and system quality on the overall educators' use of E- learning tools: A PLS-SEM analysis. SoutheastCon 2024. https://doi.org/10.1109/southeastcon52093.2024.10500283

Nadella, G. S. (2024). Advancing Edge Computing with Federated Deep Learning: Strategies and challenges. International Journal for Research in Applied Science and Engineering Technology, 12(4), 3422–3434. https://doi.org/10.22214/ijraset.2024.60602

Robisco, A A., & Martínez, J M C. (2022, July 12). Measuring the model risk-adjusted performance of machine learning algorithms in credit default prediction. Financial Innovation, 8(1). https://doi.org/10.1186/s40854-022-00366-1

Rocha-Salazar, J., Vargas, M J S., & Miñano, M D M C. (2021, May 1). Money laundering and terrorism financing detection using neural networks and an abnormality indicator. Elsevier BV, 169, 114470-114470. https://doi.org/https://doi.org/10.1016/j.eswa.2020.114470

Sadineni, P K. (2020, October 7). Detection of Fraudulent Transactions in Credit Card using Machine Learning Algorithms. 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). https://doi.org/10.1109/i-smac49090.2020.9243545

Salazar, J D J R., Vargas, M J S., & Miñano, M D M C. (2022, November 1). Detection of shell companies in financial institutions using dynamic social network. Elsevier BV, 207, 117981-117981. https://doi.org/https://doi.org/10.1016/j.eswa.2022.117981

Sawangarreerak, S., & Thanathamathee, P. (2021, June 1). Detecting and Analyzing Fraudulent Patterns of Financial Statement for Open Innovation Using Discretization and Association Rule Mining. Springer Science+Business Media, 7(2), 128-128. https://doi.org/https://doi.org/10.3390/joitmc7020128

Sinayobye, J O., Kiwanuka, F N., & Kyanda, S. (2018, May 27). A state-of-the-art review of machine learning techniques for fraud detection research. https://doi.org/10.1145/3195528.3195534

Singla, A., & Jangir, H. (2020, February 1). A Comparative Approach to Predictive Analytics with Machine Learning for Fraud Detection of Realtime Financial Data. https://doi.org/10.1109/iconc345789.2020.9117435

Sun, Y. (2021, January 28). Machine Learning Applied in the Financial Industry. Financial forum, 9(4), 239-239. https://doi.org/10.18282/ff.v9i4.1554

Talavera, A., Cano, L., Paredes, D., & Chong, M. (2019, January 1). Data Mining Algorithms for Risk Detection in Bank Loans. Communications in computer and information science, 151-159. https://doi.org/10.1007/978-3-030-11680-4_16

Uchhana, N., Ranjan, R., Sharma, S., Agrawal, D., & Punde, A. (2021, April 30). Literature Review of Different Machine Learning Algorithms for Credit Card Fraud Detection. International journal of innovative technology and exploring engineering, 10(6), 101-108. https://doi.org/10.35940/ijitee.c8400.0410621

Wen, S., Li, J., Zhu, X., & Liu, M. (2022, January 1). Analysis of financial fraud based on manager knowledge graph. Elsevier BV, 199, 773-779. https://doi.org/https://doi.org/10.1016/j.procs.2022.01.096

Wu, B., Lv, X., Al-Ghamdi, A A., Abosaq, H., & Alrizq, M. (2023, March 1). Advancement of management information system for discovering fraud in master card based intelligent supervised machine learning and deep learning during SARS-CoV2. Elsevier BV, 60(2), 103231-103231. https://doi.org/https://doi.org/10.1016/j.ipm.2022.103231

Zhang, W., Chang, W., Yu, J., & Liao, F. (2023, January 1). HY-RISE: Towards Risk Identification Learning from Massive Scientific Economic Activities. Elsevier BV, 221, 609-616. https://doi.org/https://doi.org/10.1016/j.procs.2023.08.029