THE USA JOURNALS
THE AMERICAN JOURNAL OF MANAGEMENT AND ECONOMICS INNOVATIONS (ISSN- 2693-0811)
VOLUME 06 ISSUE06

PUBLISHED DATE: - 15-06-2024
DOI: - https://doi.org/10.37547/tajmei/Volume06Issue06-02 **PAGE NO.: - 8-22**

RESEARCH ARTICLE **Open Access**

AI-POWERED FRAUD DETECTION IN BANKING: SAFEGUARDING FINANCIAL TRANSACTIONS

Fatema Tuz Johora
Department of Business Administration, Westcliff University, California 90020, USA
Orchid Id: - https://orcid.org/0009-0004-9862-5355

Rakibul Hasan
Department of Business Administration, Westcliff University, California 90020, USA
Orchid Id: - https://orcid.org/0009-0001-7268-390X

Jahanara Akter
Department of Business Administration, Westcliff University, California 90020, USA
Orchid Id: - https://orcid.org/0009-0006-1143-1668

Sayeda Farjana Farabi
Department of Business Administration, Westcliff University, California 90020, USA
Orchid Id: - https://orcid.org/0009-0006-2440-495X

Md Abdullah Al Mahmud
Department of Business Administration, International American University, California 90004, USA
Orchid Id: - https://orcid.org/0009-0006-1501-1003

Abstract

The banking industry's metamorphosis through digitalization has unquestionably revolutionized accessibility and convenience for customers worldwide. However, this paradigm shift has ushered in a new era of challenges, most notably in the realm of cybersecurity. Conventional rule-based fraud detection strategies have struggled to keep pace with the rapid evolution of cyber threats, prompting a surge of interest in more adaptive approaches like unsupervised learning. Furthermore, the COVID-19 pandemic has exacerbated the issue of bank fraud due to the widespread transition to online platforms and the proliferation of charitable funds, which present ripe opportunities for exploitation by cybercriminals. In response to these pressing concerns, this study delves into the realm of machine learning algorithms for the analysis and identification of fraudulent banking transactions. Notably, it contributes scientific novelty by developing models specifically tailored to this purpose and implementing innovative preprocessing techniques to enhance detection accuracy. Utilizing a diverse array of algorithms, including Random Forest, K-Nearest Neighbor (KNN), Naïve Bayes, Decision Trees, and Logistic Regression, the study showcases promising results. In particular, logistic regression and decision tree models exhibit impressive accuracy and Area Under the Curve (AUC) values of approximately 0.98, 0.97 and 0.95, 0.94, respectively. Given the pervasive nature of banking fraud in our digital society, the utilization of artificial intelligence algorithms for fraud detection stands as a critical and timely endeavor, promising enhanced security and trust in the financial ecosystem.

Keywords Banking, Cybersecurity, Fraud detection, Machine learning, Digital transaction.

INTRODUCTION

In the digital age, the banking industry is leading the charge in technological advancement, providing unparalleled convenience and efficiency through online and mobile banking services (Ameme & Wireko, 2016). This transformation has empowered customers globally with unprecedented accessibility, allowing them to manage their finances with ease from anywhere, anytime. Through seamless integration of technology, banking operations have become streamlined, offering personalized services and responsive customer support. As banks continue to embrace emerging technologies like AI and blockchain, the future holds promise for further evolution, ensuring banking services not only remain digital but also transformative in enhancing financial well-being worldwide (Arslanian & Fischer, 2019).

However, in an era marked by heightened digital connectivity, the banking sector finds itself at the forefront of a relentless battle against escalating cybersecurity threats. With an ever-increasing reliance on digital platforms, financial institutions confront a complex array of challenges in safeguarding sensitive customer data, fortifying transactions, and thwarting fraudulent activities (Patel et al., 2024). The evolving sophistication of cybercriminal tactics necessitates the adoption of innovative defensive strategies to effectively counter these threats. From phishing attacks and ransomware to malware infestations and data breaches, banks encounter a diverse range of risks that not only imperil their financial stability but also erode the trust of their clientele. Consequently, the imperative for the banking industry lies in comprehensively understanding these threats and proactively devising robust mitigation strategies to ensure its continued resilience and growth in an increasingly digital landscape.

Conventional fraud detection methods, reliant on established rules and signatures, have shown effectiveness but struggle to adapt to evolving fraudulent tactics. As fraudulent practices become more sophisticated, the limitations of rule-based techniques become increasingly apparent, necessitating more adaptable and efficient approaches. Machine learning, a subset of artificial intelligence, offers a promising alternative by leveraging both labeled and unlabeled data to identify patterns and anomalies

(Himeur et al., 2021; Jabin et al., 2024). By continuously learning from data without explicit programming, machine learning algorithms can dynamically adjust to new fraudulent behaviors, potentially enhancing detection accuracy and efficiency in combating financial crimes.

The study presented focuses on leveraging machine learning models to detect fraudulent banking transactions, aiming to enhance accuracy in identifying such activities. Through the utilization of preprocessing techniques and various machine learning algorithms, the research endeavors to develop algorithms adept at discerning fraudulent transactions from legitimate ones. This work holds considerable significance, particularly in the context of increased online transactions during the pandemic and heightened charitable activities during times of conflict. Recognizing fraudulent transactions involves binary classification, where transactions are categorized as either genuine or fraudulent based on historical data. The proposed approach suggests employing classification algorithms that analyze transaction features alongside preprocessing techniques for optimal performance. Access to a comprehensive historical database of fraudulent activities is imperative for effective detection, albeit maintaining the confidentiality of legitimate transactions through encryption. At the same time, AI technology offers promising avenues for fraud detection, but challenges such as algorithm transparency, interpretability, and privacy concerns demand careful consideration. Despite these hurdles, the ongoing research and development in AI-based fraud detection present substantial opportunities to enhance efficiency and accuracy in banking operations, contingent upon addressing ethical and practical challenges for its safe and effective implementation.

2. LITERATURE REVIEW

The banking sector has become increasingly vulnerable to cyber threats in recent years, a trend driven by the rapid evolution of technology and the widespread digitization of financial services. This literature review offers a critical examination of current studies and research articles focused on cybersecurity challenges within modern banking, particularly emphasizing the innovative integration of machine learning techniques for fraud detection. The literature underscores the multifaceted nature of these cyber threats, which encompass a spectrum from common phishing attacks and ransomware incidents to highly sophisticated Advanced Persistent Threats (APTs). Such a diverse landscape of threats demands a comprehensive and adaptive approach to cybersecurity within the banking industry, highlighting the necessity for ongoing research and the implementation of cutting-edge technologies to safeguard sensitive financial information and maintain the trust of customers (Rana et al., 2022; Sobuz, Al, et al., 2024).

Scholars (Smith et al., 2021; Sobuz, Joy, et al., 2024) underscore the imperative of adopting a proactive cybersecurity stance, accentuating the significance of employee training, routine security audits, and the deployment of robust encryption protocols. Researchers (Aditto et al., 2023; Chen & Han, 2021) have demonstrated remarkable precision in identifying anomalous patterns within extensive datasets. Moreover, unsupervised learning techniques, such as clustering algorithms and autoencoders, have proven pivotal in uncovering hitherto unknown fraud patterns. Despite the promising prospects that machine learning offers for fraud detection, scholars (Khatri et al., 2020; Lebichot et al., 2021)acknowledge several challenges.

Mytnyk et al. (2023) conducted research on scientific studies within the fraudulent banking field, revealing an increased output and further classified fraudulent banking approaches (see Figure 1 and Table 1).

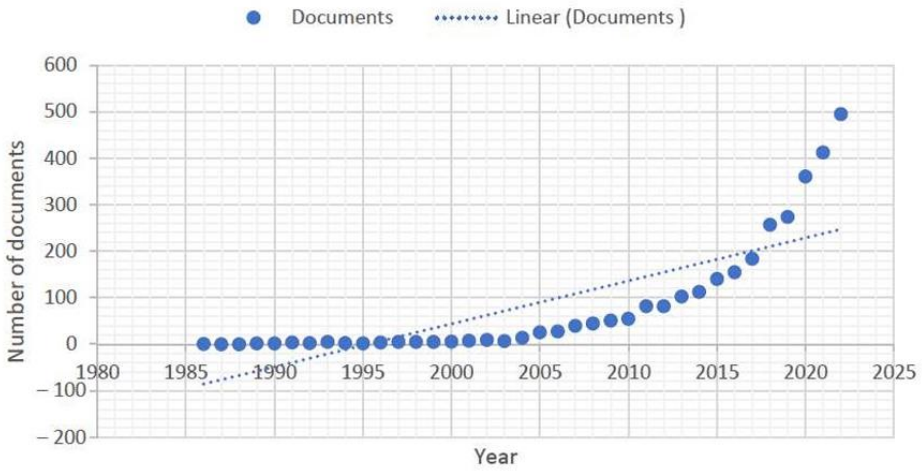

Figure 1. The statistics of scientific studies in fraudulent banking field in Scopus by year (Mytnyk et al., 2023).

Table 1. Fraudulent banking approaches and threats (Mytnyk et al., 2023).

Fraudulent Banking Approach	Threat
Phishing (Abidoye & Kabaso, 2021; Barker, 2020)	The attacker steals login credentials or other personal information by tricking the victim into entering them on a fake banking website or through a fake email or text message.
Malware (Shah et al., 2022)	Malicious software is used to steal login credentials or other personal information and may be used to take control of the victim's computer or manipulate banking transactions.
Social Engineering (Maulana & Fajar, 2021)	Attackers use psychological manipulation to trick victims into disclosing sensitive information or performing transactions they would not normally. This may include pretexting, baiting, or quid pro quo tactics.
Skimming (Al Hattali et al., 2020)	Attackers install devices on ATMs or other card readers to steal card information. This information is then used to create counterfeit cards or make unauthorized transactions.
Account Takeover (Tsai & Su, 2021)	Attackers access a victim's account by stealing login credentials or other means. Once in the account, they make unauthorized transactions, change account details, or otherwise manipulate the account for their gain.
Fake Checks (Hammi et al., 2021)	Attackers send fake checks to victims, asking them to deposit them and send back a portion of the funds. The check eventually bounces, leaving the victim responsible for the funds they sent to the attacker.
Money Mules (Abdul Rani et al., 2024)	Attackers recruit unwitting victims to help launder money by having them receive and send funds on their behalf. The victims say they are performing legitimate work but participating in illegal activities.

In another study, Ileberi et al. (2022) proposed a credit card fraud detection mechanism using a genetic algorithm for feature selection followed by classifiers like random forest, neural network, decision tree, logistic regression, and naïve Bayesian network. It outperforms existing methods for European cardholders and shares similarities with another method emphasizing preprocessing algorithms, utilizing exclusively the genetic algorithm for preprocessing. Similarly, Esenogho et al. (2022) suggested a credit card

fraud detection method using LSTM ensemble and AdaBoost, outperforming other algorithms with 0.996 sensitivity and 0.998 specificity. In a related study [18], artificial neural networks achieved the highest F1 score of 0.91 for fraud detection. Arora and Bhardwaj (2022) emphasized the vital role of secure collaborative information systems in organizations, employing AI, deep learning, and blockchain technologies for safeguarding. The paper introduces a model for fraud detection and user authentication. Logistic regression was utilized to develop a regression model for authenticating participants. Additionally, in the article Navaneethakrishnan and Viswanath (2022), data science and machine learning were used to detect credit card fraud, focusing on handling imbalanced datasets. Feature engineering and dataset modification were highlighted for better detection. Challenges included adapting to real-time situations due to high transaction volumes. The article details evaluation metrics and machine learning techniques for analysis differentiation.

3. Fraud Detection Strategy

In this section, a diverse array of machine learning algorithms were strategically selected to detect any kind of threats, including Random Forest, K-Nearest Neighbor (KNN), Naïve Bayes, Decision Trees, and Logistic Regression.

3.1 Random Forest

Random forest methods have emerged as a prominent tool in machine learning for both classification and regression tasks. This algorithm leverages the flexibility and user-friendly nature of decision trees to construct a robust ensemble model. The strength of the forest grows with the increasing number of constituent trees. Fundamentally, the algorithm operates by generating decision trees from randomly selected subsets of the data, eliciting predictions from each tree, and aggregating these predictions through a voting mechanism. The final prediction is determined by the majority vote across all trees. Moreover, random forest algorithms provide insights into feature importance, aiding in understanding the underlying factors driving predictions. The workflow of the algorithm entails (1) selecting random samples, (2) constructing decision trees, (3) conducting a collective vote, and (4) selecting the prediction result with the highest consensus as the final output (Polimis et al., 2017). This methodology not only yields accurate predictions but also offers interpretability, making it a valuable asset across various domains.

3.2 K-Nearest Neighbor (KNN)

K-nearest neighbors (KNN) stand out as a supervised learning classifier renowned for its nonparametric nature, making minimal assumptions about the underlying data distribution. This versatile algorithm leverages proximity to effectively classify or predict the grouping of individual data points. By examining the k-nearest neighbors to a given data point, KNN determines its classification based on the majority vote among these neighbors. Notably, KNN excels in classification tasks involving multiple classes, where it assigns a class label by considering the group that receives more than 25% of the votes, rather than strictly adhering to a majority rule of over 50% (Isnain et al., 2021). This nuanced approach ensures robustness in diverse datasets, where clear-cut majorities may not always be discernible.

3.3 Naïve Bayes

The Naïve Bayes classifier is a powerful tool in the realm of machine learning, rooted in the principles of Bayes' theorem. It operates under the assumption of feature independence, meaning that each predictor or feature contributes to the classification process autonomously (Zhang & Sakhanenko, 2019). This assumption simplifies the computational complexity of the model, enabling efficient and effective classification even with large datasets. Bayes' theorem, the cornerstone of this classifier, is encapsulated in the equation :

$$P(A/B) = \frac{p(B/A)P(A)}{P(B)}$$

Where P(A) signifies the probability of event A, P(B) denotes the probability of event B, and P(B|

A) represents the probability of event B occurring given the occurrence of event A. In essence, the theorem provides a framework for updating probabilities based on new evidence, making it invaluable in probabilistic reasoning and decision-making processes.

3.4 Decision Trees

In the realm of machine learning, decision trees stand as stalwarts of predictive modeling, bearing a striking resemblance to flowcharts in their structure and functionality. Each node within the tree serves as a checkpoint for a specific attribute, guiding the flow of data along branches that denote outcomes of attribute evaluations. At the culmination of each journey through the tree lies a final node, encapsulating a definitive class label. Through the iterative process of recursive partitioning, the initial dataset undergoes successive divisions based on attribute values, refining the predictive capacity of the tree with each iteration. This recursive partitioning terminates when further splits fail to enhance predictive accuracy. Notably, the beauty of decision tree classification lies in its domain-agnostic nature and the absence of intricate parameter tuning requirements, rendering it a versatile tool for knowledge exploration. Capable of handling vast datasets with aplomb, decision trees consistently yield high accuracy, cementing their status as a cornerstone of classification learning. Instances are effortlessly classified by traversing the tree from root to leaf, where a final classification awaits, epitomizing the simplicity and effectiveness of this enduring methodology (Charbuty & Abdulazeez, 2021).

3.5 Logistic Regression

Logistic regression stands as a cornerstone in statistical modeling, particularly renowned for its prowess in classification and predictive analytics tasks. At its core, this method delves into estimating the likelihood of an event occurrence, drawing insights from a designated set of independent variables. Its efficacy lies in its ability to navigate through complex data landscapes and distill probabilities with remarkable precision. Through the adept utilization of a logit transformation, where the logarithm of odds serves as its guiding principle, logistic regression unveils patterns and relationships that underpin diverse phenomena. By harnessing the natural logarithm of odds, it illuminates the intricate interplay between variables, offering invaluable insights into the probability landscape (Mood, 2010). Thus, logistic regression emerges as an indispensable tool, empowering analysts and researchers to unravel the mysteries embedded within data and make informed decisions across various domains.

4. METHODOLOGY

In the subsequent sections, we delve into the intricacies of data collection through the model evaluation phases. Figure 1 offers a comprehensive portrayal of the overarching workflow of this study, while Figure 2 meticulously delineates the workflow specific to the proposed models.

4.1 Data Collection

Primary Data : Conducting structured interviews and surveys with cybersecurity experts, banking professionals, and data scientists sheds light on the growing challenges of cybersecurity. These firsthand insights revealed the hurdles in implementing machine learning techniques to protect digital assets. The discussions highlighted the dynamic strategies banks use to defend against emerging cyber threats. These collaborative efforts emphasize the need for ongoing innovation and cooperation to stay ahead in the cybersecurity race.

Secondary Data : Gather historical records of cybersecurity breaches, instances of fraud, and the utilization of machine learning in fraud detection from credible sources, ensuring precision and contemporary significance of the data.

4.1 Data Preparation

Handling missing data: In real-world datasets, missing values are expected, arising from incomplete data collection or technical issues. Managing them is crucial for model performance (Liu et al., 2008). Strategies include imputation, replacing missing values with estimates, deletion, removing affected rows or columns; and treating

missing values as a distinct category. Each method has trade-offs but aims to preserve data integrity and model accuracy.

Handling outliers : Outliers, those significantly deviant data points within a dataset, hold particular importance in financial analysis due to their potential indication of irregular transactions or even fraudulent behavior. Recognizing and managing these outliers is paramount to maintaining the integrity of statistical analyses and ensuring robust model performance. Several strategies exist for handling outliers effectively, including trimming, which involves removing extreme values from the dataset, winsorization, which substitutes extreme values with less extreme ones; and data transformation techniques aimed at normalizing the distribution of the data. Employing these methods judiciously helps mitigate the impact of outliers, safeguarding the accuracy and reliability of financial analyses and models.

Noise reduction : In banking data analysis, noise stemming from errors or fluctuations can obscure crucial patterns. Improving the signal-to-noise ratio is essential. Techniques such as smoothing (e.g., moving averages), dimensionality reduction (e.g., principal component analysis), and robust algorithms aid in noise reduction, facilitating more accurate insights.

4.2 Data Standardization and Encoding Categorical Variables

In the realm of machine learning, particularly in methodologies reliant on distance metrics like K-nearest neighbors and support vector networks, the challenge of disparate numerical feature scales poses a significant hurdle. Standardization emerges as a crucial technique to address this issue, harmonizing numerical features by rescaling them to possess a mean of 0 and a standard deviation of 1. This not only mitigates algorithmic sensitivity to feature magnitudes but also enhances convergence rates. Similarly, normalization offers an alternative by compressing numerical features into a uniform range from 0 to 1. Furthermore, the conversion of categorical variables, such as gender and product type, into numerical representations is imperative for many machine learning algorithms that mandate numeric input data. One-hot encoding serves as a prevalent method for this transformation, wherein binary vectors replace categorical variables, ensuring algorithmic interpretability while sidestepping inadvertent ordinal correlations among categories. Through these techniques, the data preprocessing phase lays a solid foundation for robust and accurate machine learning models.

4.3 Feature Extraction

Detecting fraud requires a multifaceted approach that considers various factors. Among these, the transaction amount stands out as a crucial indicator, as unusual amounts, whether unusually large or small, can raise red flags. Additionally, monitoring transaction frequency provides insights into typical user behavior, with sudden variations potentially signaling fraudulent activity. Examining the location of transactions is also vital; transactions occurring in atypical areas compared to a user's usual locations could indicate potential fraud. Moreover, analyzing transaction timing, including the day of the week, month, and time of day, helps uncover patterns and anomalies that fraudsters may exploit. Successful fraud detection involves not only identifying individual features but also understanding their interactions and employing advanced analytical techniques to extract meaningful insights from the data.

4.4 Dimensionality Reduction

Principal Component Analysis (PCA) is a widely adopted technique for reducing the dimensionality of high-dimensional datasets while retaining a significant portion of their variance. It achieves this by transforming the original features into a set of orthogonal principal components, ranked based on the variance they explain. This allows for dimensionality reduction without significant loss of crucial information present in the data. In contrast, t-distributed Stochastic Neighbor Embedding (t-SNE) is a nonlinear method specifically designed for visualizing high-dimensional data in lower-dimensional spaces. Unlike PCA, t-SNE focuses on preserving local structures by modeling pairwise

similarities (Wold et al., 1987). It's often used for exploratory data analysis and visualization rather than as a preprocessing step for machine learning algorithms. Both PCA and t-SNE can help streamline complex datasets, potentially reducing computational costs and improving machine learning model performance by emphasizing informative features or mitigating overfitting (Linderman et al., 2017). However, careful consideration of trade-offs and the impact on model interpretability is essential when employing dimensionality reduction techniques.

4.5 Hypermeter Selection

Isolation Forest is a potent technique for anomaly detection, particularly adept at handling high-dimensional data. To optimize its performance, careful adjustment of hyperparameters is essential. Among these, the Number of Trees parameter stands out, dictating the quantity of trees in the forest. Increasing the number of trees can bolster the model's ability to pinpoint anomalies, yet it comes at the cost of heightened computational complexity (Liu et al., 2008). The ideal number of trees hinges on factors such as the dataset's characteristics and the desired trade-off between processing power and performance. Additionally, the Contamination Level parameter plays a pivotal role in defining the proportion of outliers in the dataset. Typically, fine-tuning this parameter requires either cross-validation techniques or domain expertise. In anomaly detection, striking the right balance between precision and recall necessitates setting an appropriate degree of contamination. Thus, through meticulous adjustment of these hyperparameters, Isolation Forest can be tailored to yield optimal results in anomaly detection tasks.

4.5 Training the Models

The Isolation Forest model is employed on preprocessed banking data subsequent to the selection of appropriate hyperparameters. This model operates by constructing a forest of isolated trees, wherein it discerns underlying patterns within the data during the training phase. In this process, each tree randomly selects a feature and a split value, dividing the feature space iteratively until either every data point is isolated in its own leaf node or the maximum tree depth is reached. Notably, Isolation Forest excels at identifying anomalies by isolating data points that necessitate fewer partitions to separate, indicative of their deviation from the majority of the data (Liu et al., 2008). This methodology leverages the unique characteristics of isolation trees to effectively detect outliers within the dataset.

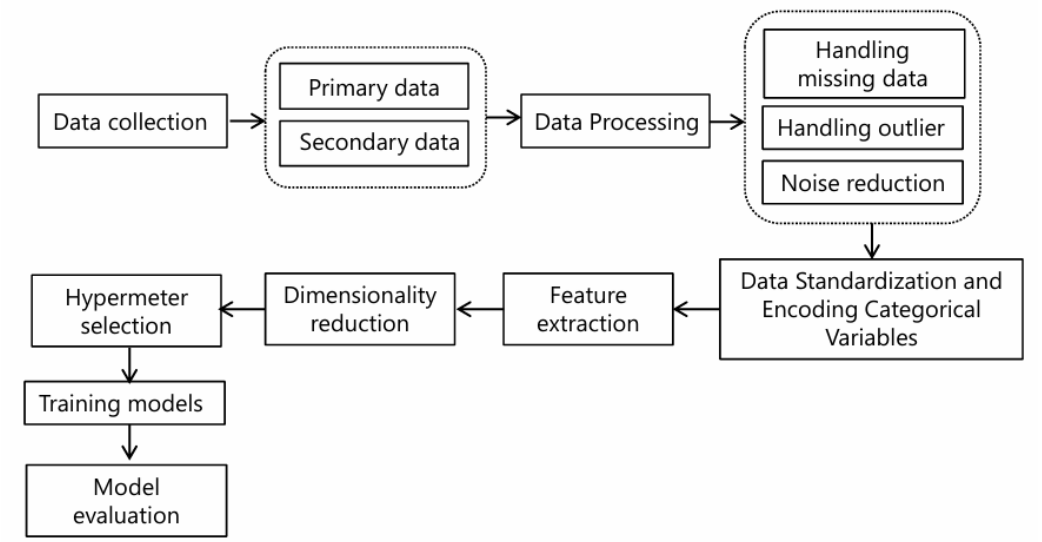

Figure 2. Workflow of the overall process og this study

4.5 Model Evaluation

4.5.1 Precision

Precision in fraud detection refers to the proportion of accurately identified anomalies among all data points flagged as anomalies. This metric serves as a crucial indicator of a system's efficacy in discerning potentially fraudulent transactions while minimizing the misclassification of legitimate ones. Calculated as the ratio of true positives (TP) to the sum of true positives and false positives, precision underscores the system's ability to avoid unnecessary alerts for valid transactions (Gonaygunta, 2023). A higher precision signifies a reduced occurrence of false positives, showcasing the system's capability to maintain a balance between sensitivity to fraud and accuracy in classification, thus enhancing its overall effectiveness in fraud detection and prevention.

$$\Pr ecision = \frac{TP}{TP + FP}$$

4.5.2 Recall

In the realm of fraud detection, recall serves as a beacon, guiding the assessment of a model's capacity to navigate the intricate web of transactions and pinpoint genuine anomalies. Defined as the ratio of true positives to the combined total of true positives and false negatives, recall embodies the system's ability to capture most instances of fraudulent activity while tolerating a degree of oversight. A higher recall signifies a more vigilant system, adept at minimizing the escape of fraudulent transactions without succumbing to the temptation of indiscriminate flagging (Gonaygunta, 2023). It reflects a delicate balance between sensitivity and specificity, ensuring that the net cast by the model is finely tuned to ensnare actual instances of fraud while averting the burden of excessive false positives. Thus, recall stands as a cornerstone in the evaluation of fraud detection mechanisms, offering insights into their efficacy and resilience in the face of evolving threats.

$$\Re call = \frac{TP}{TP + FN}$$

4.5.2 F1-Score

$$F1 - Score = \frac{2 \times \Pr ecision \times \Re call}{\Pr ecision + \Re call}$$

The F1-score serves as a vital measure in classification tasks, harmonizing precision and recall. Particularly useful in imbalanced class distributions, it ranges from 0 (worst) to 1 (best), indicating the balance between precision and recall. Calculated as the harmonic mean of the two, it offers a succinct yet comprehensive evaluation of model performance, facilitating informed decision-making in predictive analytics (Liu et al., 2008).

4.5.2 ROC-AUC (Receiver Operating Characteristic - Area Under Curve)

The Receiver Operating Characteristic Area Under the Curve (ROC-AUC) serves as a pivotal metric in evaluating binary classifiers, particularly in scenarios like anomaly detection systems. ROC-AUC encapsulates the trade-off between the true positive rate (recall) and the false positive rate (FPR) across different threshold levels (Liu et al., 2008). The ROC curve, plotting TPR against FPR, visually illustrates this trade-off. A higher AUC-ROC signifies superior discrimination ability between positive and negative classes, with a perfect score of 1 representing flawless discrimination and 0.5 indicating random guessing. By condensing the model's performance into a single scalar value, ROC-AUC facilitates straightforward comparisons between various algorithms or models, aiding in the comprehensive assessment of their effectiveness in binary classification tasks.

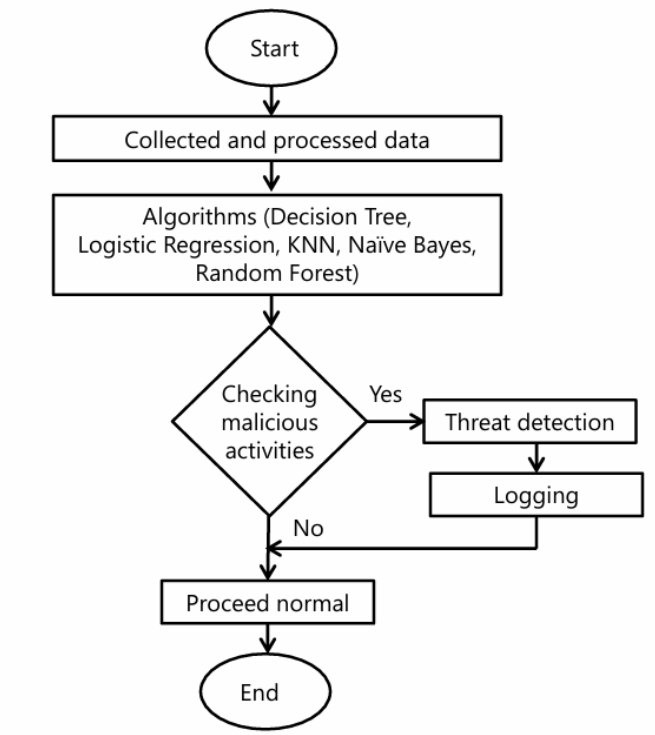

Figure 2. Workflow of the proposed models

5. RESULTS AND DISCUSSION

The dataset underwent a conventional division into training, validation, and testing subsets, with proportions set at 70%, and 30%, respectively, aimed at gauging generalization performance. Diverse classification algorithms, encompassing Decision Trees, Logistic Regression, KNN, Naïve Bayes, and Random Forest, were employed to tackle the classification task. Hyperparameter optimization was conducted through grid search methodology to fine-tune model performance. Subsequent to the initialization and preprocessing stages, models were systematically trained and assessed utilizing the Area Under the Curve (AUC) metric, with the ROC curve being graphically depicted for each algorithm. The outcomes unveiled AUC metrics as detailed in Table 2 and Figure 4 (a-e). Based on these metrics, the logistic regression model emerged as the frontrunner with the highest AUC value, indicative of superior performance. Furthermore, it's noteworthy that all models exhibited satisfactory results.

Table 2. Performance Metrics of AI Algorithms

Algorithm	Accuracy	Precision	Recall	F1-Score	AUC
Decision Trees (DT)	0.97	0.97	0.96	0.92	0.94
Logistic Regression (LR)	0.98	0.99	0.97	0.94	0.95
K-Nearest Neighbor (KNN)	0.95	0.96	0.94	0.88	0.93
Naïve Bayes (NB)	0.91	0.91	0.92	0.86	0.91
Random Forest (RF)	0.91	0.91	0.92	0.86	0.91

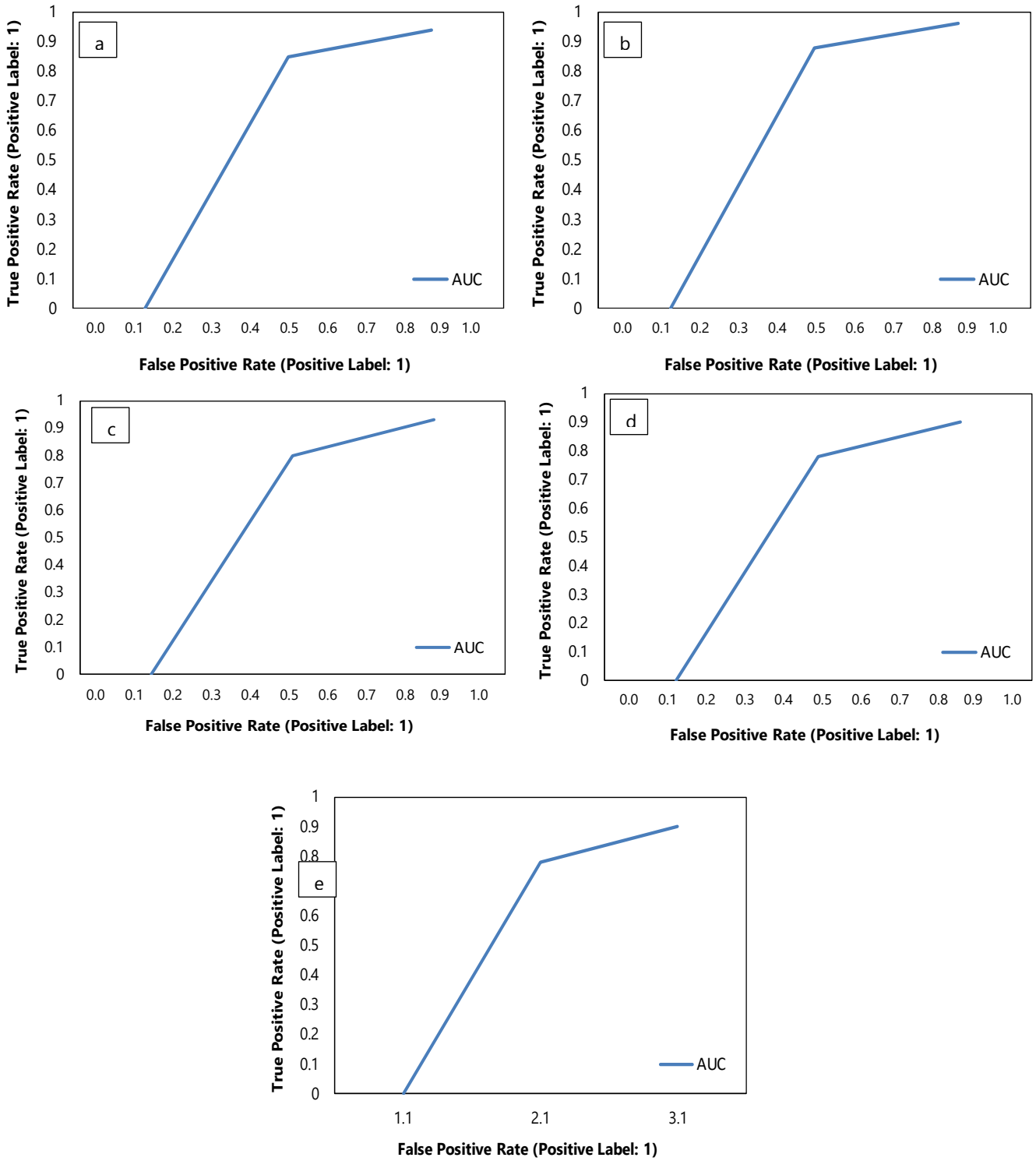

Figure 4. Plots of ROC-AUC curves of the following algorithms: (a) Decision Tree (b) Logistic Regression (c) K-Nearest Neighbor

(d) Naïve Bayes (e) Random Forest

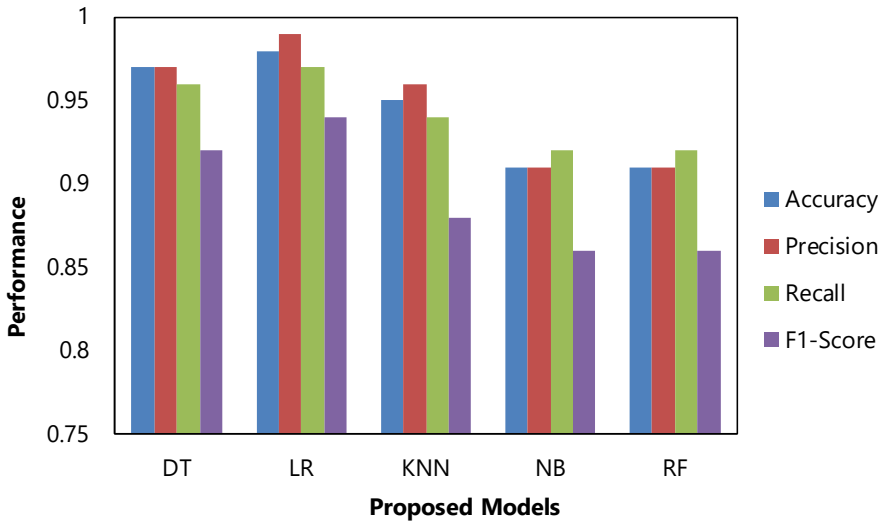

Figure 5. Evaluation of the models performance

However, Logistic Regression outshines the other algorithms with an impressive accuracy score of 0.98, indicating its ability to correctly predict class labels for 98% of instances in the dataset. Its precision of 0.99 signifies its capability to accurately identifying positive instances, while a recall of 0.97 showcases its effectiveness in capturing the true positive rate. With an F1-score of 0.94, Logistic Regression achieves a harmonious balance between precision and recall, further solidifying its position as the top-performing algorithm in this comparison. In contrast, while Decision Trees exhibit commendable accuracy (0.97) and precision (0.97), their slightly lower recall (0.96) and F1-score (0.92) hint at potential challenges in accurately identifying positive instances. KNN follows suit with a respectable accuracy of 0.95 but falls short in precision (0.96), recall (0.94), and F1-score (0.88) compared to Logistic Regression, suggesting limitations in capturing underlying data patterns effectively. Similarly, Naïve Bayes and Random Forest algorithms demonstrate comparable performance with accuracy, precision, recall, and F1-scores hovering around 0.91-0.92, albeit lower than Logistic Regression. This comprehensive dominance across all metrics underscores Logistic Regression's efficacy in modeling the dataset's linear decision boundary, making it the top choice for real-world applications despite competitive performances from other algorithms (see Figure 5).

5. CONCLUSION

This paper underscores the pivotal role of artificial intelligence in identifying fraudulent banking transactions. We propose a range of classification algorithms adept at discerning transaction types based on distinct features. Our model, anchored in an artificial neural network framework, notably enhances the accuracy of fraudulent transaction detection. Moreover, we delve into various methodologies to bolster detection precision, including managing imbalanced datasets, feature transformation, and feature engineering.

Our study showcases the efficacy of artificial intelligence algorithms in recognizing banking fraud. Through rigorous training and testing, each algorithm we selected exhibited exemplary performance, with none yielding an AUC (Area Under the Curve) value lower than 0.9. This consistency is evident in the ROC (Receiver

Operating Characteristic) curves, where discernible visual discrepancies are absent. Notably, our evaluation revealed that all algorithms demonstrated comparable proficiency in identifying fraudulent bank transactions. However, quantitatively, logistic regression emerged as the top performer, boasting an AUC value of approximately 0.946.

Thefindings underscore the robustness of utilizing artificial intelligence in combatting banking fraud, with logistic regression showcasing superior performance in this context.

Funding: The government, a private corporation, or a nonprofit organization provided no funding for this analysis.

Conflicts of Interest: There are no conflicts of interest among the authors or personnel.

REFERENCES

1. Abdul Rani, M. I., Syed Mustapha Nazri, S. N. F., & Zolkaflil, S. (2024). A systematic literature review of money mule: Its roles, recruitment and awareness. Journal of Financial Crime, 31(2), 347-361.
2. Abidoye, A. P., & Kabaso, B. (2021). Hybrid machine learning: A tool to detect phishing attacks in communication networks. ECTI Transactions on Computer and Information Technology (ECTI-CIT), 15(3), 374-389.
3. Aditto, F. S., Sobuz, M. H. R., Saha, A., Jabin, J. A., Kabbo, M. K. I., Hasan, N. M. S., & Islam, S. (2023). Fresh, mechanical and microstructural behaviour of high-strength self-compacting concrete using supplementary cementitious materials. Case Studies in Construction Materials, 19, e02395.
4. Al Hattali, S. S. K., Hussain, S. M., & Frank, A. (2020). Design and development for detection and prevention of ATM skimming frauds. Indonesian Journal of Electrical Engineering and Computer Science, 17(3), 1224.
5. Ameme, B., & Wireko, J. (2016). Impact of technological innovations on customers in the banking industry in developing countries. The Business & Management Review, 7(3), 388.
6. Arora, M., & Bhardwaj, I. (2022). Artificial intelligence in collaborative information system. Int. J. Mod. Educ. Comput. Sci.(IJMECS), 14(1), 44-55.
7. Arslanian, H., & Fischer, F. (2019). The future of finance: The impact of FinTech, AI, and crypto on financial services. Springer.
8. Barker, R. (2020). The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. South African Journal of Business Management, 51(1), 1-10. https://doi.org/https://hdl.handle.net/10520/EJC-20923d99f2
9. Charbuty, B., & Abdulazeez, A. (2021). Classification based on decision tree algorithm for machine learning. Journal of Applied Science and Technology Trends, 2(01), 20-28. https://doi.org/https://doi.org/10.38094/jastt20165
10. Chen, Y., & Han, X. (2021). CatBoost for fraud detection in financial transactions. 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE),
11. Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A neural network ensemble with feature engineering for improved credit card fraud detection. Ieee Access, 10, 16400-16407.
12. Gonaygunta, H. (2023). Machine learning algorithms for detection of cyber threats using logistic regression. Department of Information Technology, University of the Cumberlands. https://doi.org/10.47893/IJSSAN.2023.1229
13. Hammi, B., Zeadally, S., Adja, Y. C. E., Del Giudice, M., & Nebhen, J. (2021). Blockchain-based solution for detecting and preventing fake check scams. IEEE Transactions on Engineering Management, 69(6), 3710-3725.
14. Himeur, Y., Ghanem, K., Alsalemi, A., Bensaali, F., & Amira, A. (2021). Artificial intelligence

based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives. Applied Energy, 287, 116601. https://doi.org/https://doi.org/10.1016/j.apenergy.2021.116601

15. Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. Journal of Big Data, 9(1), 24.

16. Isnain, A. R., Supriyanto, J., & Kharisma, M. P. (2021). Implementation of K-Nearest Neighbor (K-NN) Algorithm For Public Sentiment Analysis of Online Learning. IJCCS (Indonesian Journal of Computing and Cybernetics Systems), 15(2), 121-130.

17. Jabin, J. A., Khondoker, M. T. H., Sobuz, M. H. R., & Aditto, F. S. (2024). High-temperature effect on the mechanical behavior of recycled fiber-reinforced concrete containing volcanic pumice powder: An experimental assessment combined with machine learning (ML)-based prediction. Construction and Building Materials, 418, 135362. https://doi.org/https://doi.org/10.1016/j.conbuildmat.2024.135362

18. Khatri, S., Arora, A., & Agrawal, A. P. (2020). Supervised machine learning algorithms for credit card fraud detection: a comparison. 2020 10th international conference on cloud computing, data science & engineering (confluence),

19. Lebichot, B., Paldino, G. M., Siblini, W., He-Guelton, L., Oblé, F., & Bontempi, G. (2021). Incremental learning strategies for credit cards fraud detection. International Journal of Data Science and Analytics, 12(2), 165-174.

20. Linderman, G. C., Rachh, M., Hoskins, J. G., Steinerberger, S., & Kluger, Y. (2017). Efficient algorithms for t-distributed stochastic neighborhood embedding. arXiv preprint arXiv:1712.09005.

21. Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. 2008 eighth ieee international conference on data mining,

22. Maulana, L. R., & Fajar, A. N. (2021). Extending the Design of Smart Mobile Application to Detect Fraud Theft of E-Banking Access Using Big Data Analytic and SOA. 2021 IEEE 5th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE),

23. Mood, C. (2010). Logistic regression: Why we cannot do what we think we can do, and what we can do about it. European sociological review, 26(1), 67-82. https://doi.org/https://doi.org/10.1093/esr/jcp006

24. Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023). Application of artificial intelligence for fraudulent banking operations recognition. Big Data and Cognitive Computing, 7(2), 93. https://doi.org/10.3390/bdcc7020093

25. Navaneethakrishnan, P., & Viswanath, R. (2022). Fraud Detection On Credit Cards Using Artificial Intelligence Methods. Elementary Education Online, 19(2), 2086-2086.

26. Patel, D., Sahu, C. K., & Rai, R. (2024). Security in modern manufacturing systems: integrating blockchain in artificial intelligence-assisted manufacturing. International Journal of Production Research, 62(3), 1041-1071. https://doi.org/10.1080/00207543.2023.2262050

27. Polimis, K., Rokem, A., & Hazelton, B. (2017). Confidence intervals for random forests in python. Journal of Open Source Software, 2(19), 124. https://doi.org/https://doi.org/10.21105/joss.00124

28. Rana, J., Hasan, R., Sobuz, H. R., & Tam, V. W. (2022). Impact assessment of window to wall ratio on energy consumption of an office building of subtropical monsoon climatic country Bangladesh. International Journal of Construction Management, 22(13), 2528-2553. https://doi.org/https://doi.org/10.1080/15

623599.2020.1808561

29. Shah, S. S. H., Ahmad, A. R., Jamil, N., & Khan, A. u. R. (2022). Memory forensics-based malware detection using computer vision and machine learning. Electronics, 11(16), 2579. https://doi.org/ 10.3390/electronics11162579

30. Smith, K. J., Dhillon, G., & Carter, L. (2021). User values and the development of a cybersecurity public policy for the IoT. International Journal of Information Management, 56, 102123. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2020.102123

31. Sobuz, M. H. R., Al, I., Datta, S. D., Jabin, J. A., Aditto, F. S., Sadiqul Hasan, N. M., Hasan, M., & Zaman, A. A. U. (2024). Assessing the influence of sugarcane bagasse ash for the production of eco-friendly concrete: Experimental and machine learning approaches. Case Studies in Construction Materials, 20, e02839. https://doi.org/https://doi.org/10.1016/j.cscm.2023.e02839

32. Sobuz, M. H. R., Joy, L. P., Akid, A. S. M., Aditto, F. S., Jabin, J. A., Hasan, N. M. S., Meraz, M. M., Kabbo, M. K. I., & Datta, S. D. (2024). Optimization of recycled rubber self-compacting concrete: Experimental findings and machine learning-based evaluation. Heliyon, 10(6). https://doi.org/https://doi.org/10.1016/j.heliyon.2024.e27793

33. Tsai, C.-H., & Su, P.-C. (2021). The application of multi-server authentication scheme in internet banking transaction environments. Information systems and e-business management, 19(1), 77-105.

34. Wold, S., Esbensen, K., & Geladi, P. (1987). Principal component analysis. Chemometrics and Intelligent Laboratory Systems, 2(1), 37-52. https://doi.org/https://doi.org/10.1016/0169-7439(87)80084-9

35. Zhang, Y.-C., & Sakhanenko, L. (2019). The naive Bayes classifier for functional data. Statistics & Probability Letters, 152, 137-146. https://doi.org/https://doi.org/10.1016/j.spl.2019.04.017