An Ensemble-based Fraud Detection Model for Financial Transaction Cyber Threat Classification and Countermeasures

Asma A. Alhashmi
Department of Computer Science, Northern Border University, Saudi Arabia
asma.alhashmi@nbu.edu.sa

Abdullah M. Alashjaee
Department of Computer Science, Northern Border University, Saudi Arabia
abd.ullahalashjaee@nbu.edu.sa

Abdulbasit A. Darem
Department of Computer Science, Northern Border University, Saudi Arabia
basit.darem@nbu.edu.sa (corresponding author)

Abdullah F. Alanazi
Department of Computer Science, Northern Border University, Saudi Arabia
Abd.ullahfahes@nbu.edu.sa

Rachid Effghi
Department of Big Data Analytics and Management, Bahcesehir University, Turkiye
rachideffghi@bahcesehir.edu.tr

Received: 15 September 2023 | Revised: 30 September 2023, and 16 October 2023 | Accepted: 17 October 2023

ABSTRACT

Fraud remains a pervasive challenge within the banking industry, where financial institutions and their clients grapple with substantial annual losses. The proliferation of digital transactions and online banking has created new avenues for fraudsters to exploit vulnerabilities, leading to financial harm to unsuspecting victims. Consequently, the imperative to promptly and accurately detect fraudulent transactions has grown significantly, both as a safeguard against financial crimes and as a pillar of trust between customers and the banking sector. This paper introduces an innovative fraud detection model designed for bank payment transactions using advanced ensembling techniques. This study presents a comprehensive evaluation of an ensembling model conducted on the Bank Account Fraud (BAF) dataset. Through meticulous analysis, the performance of various base models and ensembling methods was assessed and compared, employing a variety of critical metrics including accuracy, precision, recall, and F1-score. The proposed ensemble model, referred to as "Stacking," exhibited remarkable performance, attaining a commendable accuracy score of 0.98. This result reaffirmed its prowess as a comprehensive and balanced solution to the multifaceted challenges of fraud detection. This study has paramount implications for the banking industry, offering a robust and adaptable solution to deal with the increasing threats posed by financial fraud. Furthermore, it emphasizes the significance of precision-recall trade-offs in fraud detection and underscores the potential of ensemble methods, particularly the "Stacking" model, to fortify the resilience and efficacy of existing security systems.

Keywords-cybersecurity; banking fraud; cyber scams; human vulnerability; social engineering; countermeasures

I. INTRODUCTION

Cyberattacks on banks and financial institutions have become increasingly prevalent in recent years. A 2017 survey estimated that a typical financial institution faces an average of 85% targeted cyber-attacks every year [1]. In Hungary, the banking industry observed an increasing trend in the number of cyberattacks [1-2]. The financial sector in the USA is continuously facing cyberattacks, as finance technologies are more prone to cyberattacks arising from technologically induced vulnerabilities [3]. Online banking in India has been significantly targeted by cyber attackers [4]. African corporations are facing rising cybersecurity risks, particularly in banks that are poorly performing and under-capitalized. Cyberattacks such as fraud, phishing, hacking, and ransomware attacks erode public confidence in online services, constraining the expansion of online banking [5-6]. Financial institutions are investing heavily in cybersecurity to counteract cyberattacks and cyber bank robbery attempts [7]. Cyber attacks that threaten the cyber security of banks are a significant issue that can lead to reputation and significant financial losses [8].

Fraud detection, an essential facet of this challenge, has seen the deployment of various strategies to detect fraud in bank payments [9], including rule-based methods [10], anomaly detection [11-12], and machine learning algorithms [13-14]. However, each has its limitations: rule-based methods might overlook complex patterns, while anomaly detection can confuse genuine outliers with deceitful transactions. Machine learning's effectiveness may diminish due to overfitting or noisy, imbalanced data. This evolving landscape of fraud detection methods has pivoted toward machine learning, which has emerged as an effective solution in recent years. Traditional techniques often fail against novel or intricate fraud patterns, while machine learning algorithms, from decision trees to neural networks, demonstrate prowess in understanding these patterns [11]. For example, in [15-16], the effectiveness of machine learning methods in detecting credit card fraud was investigated, and some algorithms achieved accuracy greater than 90%.

The banking sector's stride towards employing deep learning models further exemplifies the shift. Models such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) have exhibited promising results in detecting intricate fraud patterns in real time [17-18]. For example, in [18], a deep learning-based credit card fraud detection system was presented that excelled in identifying fraudulent transactions, proving its worth against standard benchmarks. While individual models have their merit, the increased attention towards ensemble methods underlines the broader research trend. Ensembling, whether through bagging, boosting, or stacking, converges multiple algorithmic predictions to enhance model performance. It combines the strength of diverse models to yield more accurate and robust results while mitigating risks like overfitting. The novel contributions of this study are:

- An ensemble method for fraud detection in bank payments is proposed. The proposed model aims to capitalize on this ensembling technique, integrating algorithms such as the Voting Classifier, Random Forest, Gradient Boosting Machine, Logistic Regression (LR), and neural networks.
- Both global and local transaction patterns are captured while ensuring adaptability over time.
- The proposed model is evaluated and validated through extensive experiments. The results showed that the proposed model achieved 98% detection accuracy.

II. RESEARCH METHODOLOGY

The method for developing an ensembling fraud detection model involved several steps, including data collection, pre-processing, feature engineering, model selection, and ensembling.

A. Dataset

This study used Bank Account Fraud (BAF) [19], a pioneering collection, known for being the first to be publicly accessible, privacy-oriented, large-scale, and realistically reflective of the complexities inherent in bank account fraud detection. This dataset was synthesized employing state-of-the-art tabular data generation techniques applied to an anonymized, real-world dataset on bank account fraud detection. The BAF dataset is not only robust but also highly nuanced, containing six distinct variants, each incorporating predetermined and controllable bias patterns, such as prevalence and group size disparities, grounded in a well-established data bias taxonomy. This enables a multifaceted exploration and understanding of various biases in fraud detection systems. The richness of the BAF dataset, marked by its inherent challenges, such as significant class imbalance and temporal dynamics, mirrors real-world complexities and offers an invaluable and realistic platform for evaluating both existing and innovative machine learning methods in fraud detection. The dataset is comprehensive, with 1 million instances and 30 features, accompanied by protected attributes and temporal information, enhancing the depth and breadth of analytical capabilities. In this study's context, the BAF dataset serves as a critical instrument enabling the assessment and comparison of diverse models and ensembling methods, with its varied and realistic features facilitating the development and evaluation of advanced ensemble-based fraud detection models. The unique characteristics of the dataset allow for a meticulous examination of the models' performance under real-world conditions and complexities, enriching the reliability and applicability of the findings.

B. Data Preprocessing

The raw data were pre-processed in order to be prepared for analysis. Feature engineering techniques were used to extract valuable information from the raw transaction data. The primary objective during the feature engineering phase was to streamline the dataset by reducing the number of original features. This approach served a dual purpose: to enhance the convergence time and results of the generative model and to address potential privacy concerns. The extraction process began by identifying the best-performing LightGBM models [19] in the original dataset. Subsequently, the union of the 30 most significant features from these models was determined based on LightGBM's default feature importance method. This yielded a total of 43 features, which were further refined to 30 after manual selection for expressiveness, interpretability, and redundancy reduction. The feature selection process was meticulous and aimed to ensure data privacy while retaining the integrity of the dataset. To achieve this, each column in the original dataset was perturb+ed using a Laplacian noise mechanism before training the Generative Adversarial Network (GAN) [19]. This perturbation, inversely proportional to the privacy budget, was essential to strike a balance between data privacy and utility. Specific data, such as the age and income of the applicant, were categorized according to value and quantile, ensuring that the GAN never accessed precise applicant details. The GAN models were then trained on this perturbed dataset, with a unique identifier encoded for each instance to prevent repetitions between original and generated datasets.

C. Model Selection

Five different machine-learning algorithms were used to construct the fraud detection model. The Voting Classifier [20] is an ensemble meta-estimator that fits several base classifiers and aggregates their predictions to produce a final result. The predictions can be weighted, and the final classification can be derived from hard voting (majority class labels) or soft voting (averaging probabilities). This study used the Voting Classifier to combine predictions from multiple models, such as Random Forest, Gradient Boosting Machine, and LR. The prediction of each model was treated as a vote, and the final classification was based on the majority vote. The Voting Classifier was chosen for its ability to leverage the strengths of multiple models, which could lead to better accuracy and generalization, as it can reduce the risk of choosing a single model that could underperform in certain scenarios. The Voting Classifier often showed improved accuracy compared to individual models, showcasing the power of ensemble methods in fraud detection. Random Forest [21-22] is used to construct multiple decision trees during training and outputs the mode (classification) of the classes for individual trees or the mean prediction (regression) of individual trees. In this study, the dataset was fed into the Random Forest algorithm, which then constructed multiple decision trees. Hyperparameters, such as the number and depth of trees, were optimized using cross-validation. Random Forest is known for its high accuracy, and its ability to handle large datasets with higher dimensionality and missing values. It is particularly relevant for fraud detection because of its ability to model complex decision boundaries. Random Forest is often ranked among the best-performing models, highlighting its effectiveness in detecting intricate patterns associated with fraudulent transactions.

Gradient Boosting Machine (GBM) [23] is an iterative method that is used to adjust the shortcomings of the previous trees in the sequence. GBM was trained on the dataset with each successive tree aiming to correct the errors of the previous one. Hyperparameters, such as learning rate and number of trees, were tuned for optimal performance. GBM provides superior predictive accuracy compared to other algorithms. Its ability to focus on misclassified instances makes it particularly powerful for imbalanced datasets, such as fraud detection, where fraudulent transactions are typically rare. GBM consistently delivered high accuracy rates, emphasizing its robustness and ability to effectively identify fraud patterns. LR [24] was deployed for its simplicity, efficiency, and interpretability of its output, which is particularly advantageous for insight extraction. LR is a statistical method used to model binary outcomes by predicting the probability that a given instance belongs to a particular category. The dataset features were used as input variables, and the binary result (fraudulent or not) was the target variable. The model was trained to find the best decision boundary that separates the two classes. Logistic Regression is simple, interpretable, and can serve as a baseline model. It is also fast to train and can be useful when a quick initial assessment is needed. While LR might not be the top performer in terms of accuracy, its value lies in its speed and interpretability and provides a benchmark to compare against more complex models.

Neural networks [25] were chosen for their ability to learn and model complex and nonlinear relationships, which is crucial for the intricate patterns inherent in fraud detection. One of the salient strengths of neural networks is their ability to learn features autonomously without manual intervention. By leveraging multiple layers, they can identify both low- and high-level features from raw data, which can be instrumental in detecting novel fraud patterns that might be missed when using hand-crafted features. Neural networks can be re-trained with new data, allowing them to adapt to evolving fraud strategies. This dynamic adaptability is especially crucial in the ever-changing landscape of cyber threats. A Multi-Layer Perceptron (MLP) was used, which is a feedforward artificial neural network. The MLP architecture consisted of three layers. The input layer had 30 neurons corresponding to the number of features in the dataset. Following the input layer, the hidden layer contained 10 nodes and used the Rectified Linear Unit (ReLU) [26] as its activation function, introducing non-linearity into the model. The hidden layer configuration, consisting of 10 nodes, was determined through a combination of empirical experimentation and theoretical considerations. The choice of 10 nodes aimed to strike a balance between model complexity and generalizability. An overly dense hidden layer might lead to overfitting, where the model memorably captures noise and anomalies specific to the training data, thereby compromising its performance on unseen data. On the contrary, a sparse hidden layer might not adequately capture the intricate patterns inherent in the data. The ReLU was chosen as the activation function for its several advantageous properties. ReLU, defined mathematically as $\mathrm{ReLU}(x) = \max(0, x)$, introduces non-linearity into the model, which is essential for learning complex data patterns. Moreover, ReLU is computationally efficient, promoting faster model convergence, and effectively mitigates the vanishing gradient problem, a challenge often encountered with traditional activation functions like sigmoid. This problem can hinder the training process, especially in deeper networks. Thus, the combination of 10 nodes and the ReLU activation function was deemed optimal for the performance of the model on BAF. The final layer (output), consisted of a single neuron that provided a probability score, indicating the likelihood that a transaction was fraudulent. This layer used the sigmoid activation function [26], which suppresses the output between 0 and 1:

$$\mathrm{Sigmoid}(x) = \frac{1}{1+e^{-x}} \quad (1)$$

where Sigmoid(x) represents the output of the Sigmoid function for a given input x, e is the base of the natural logarithm, x is the input to the function, and e^{-x} calculates the inverse of the exponential function raised to the power of the negative input value. The division ensures that the output of the sigmoid function is squashed between 0 and 1.

The Sigmoid function is commonly used in neural networks, especially for binary classification tasks, because it maps any input value to a range between 0 and 1, which can be interpreted as a probability. In terms of hyperparameters, the learning rate used was set at 0.01, determining the step size during each iteration toward minimizing the loss function. The model was trained in 100 epochs, each epoch representing a complete forward and backward pass of the entire dataset through the neural network. A batch size of 32 was chosen, meaning that in each iteration, 32 samples from the training dataset were used to compute the error and subsequently update the model parameters. The Binary Cross-Entropy loss function was used to measure the discrepancy between the actual and predicted probabilities, given its suitability for binary classification tasks. The rationale behind using an MLP for this study stems from its versatility in capturing complex non-linear relationships present in the data. Its layered structure facilitates the extraction of hierarchical features, making it suitable for fraud detection tasks where patterns might be nuanced. The combination of ReLU and sigmoid activation functions ensures efficient learning and probabilistic predictions, respectively, enhancing the model's efficacy in distinguishing fraudulent transactions.

D. *Ensembling*

This study used a stacking ensembling method to amalgamate the predictions of multiple models and produce a final singular prediction for each new transaction. This method allows the strengths of different models to be combined, achieving greater accuracy and robustness than any single model. Moreover, the meta-model can adapt to changing patterns in the transaction data over time by being re-trained on new data. The steps involved in the stacking method are as follows:

1. Split the dataset into training and testing sets.
2. Divide the training set into k-folds.
3. Train each base model on k-1 folds and predict the remaining fold.
4. Repeat step 3 for each fold.
5. Use the predictions from all base models as input features for the meta-model.
6. Train the meta-model on the training set and evaluate on the testing set.
7. Repeat steps 1-6 for each new transaction.

The stacking method combines the strengths of different models to achieve higher accuracy and robustness than any individual model alone. In addition, the meta-model can adapt to changing patterns in the transaction data over time by retraining on new data. The stacking method is based on the idea of using a meta-model to learn the optimal combination of predictions from multiple base models. Mathematically, the meta-model can be formulated as follows:

$$y = g(a_1 f_1\,(x) + a_2 f_2\,(x) + \cdots . + a_n f_n\,(x)) \quad (2)$$

where y is the final prediction, $g()$ is the activation function of the meta-model, $f_i()$ is the prediction from the i-th base model, x is the input feature vector of a new transaction, and a_i is the weight assigned to the prediction of the i-th base model. Weights a_i can be learned using various techniques, such as linear regression, gradient descent, or Bayesian optimization. The activation function $g()$ can be a simple logistic function or a more complex neural network.

III. RESULTS AND DISCUSSION

This section presents the experimental results of the fraud detection model on the BAF dataset. The model was evaluated using five-fold cross-validation and the average performance across all folds was reported. This study aimed to evaluate various candidate algorithms and ensemble methods for the fraud detection model, selecting the optimal combination based on performance metrics such as precision, recall, and F1-score. This process involves several stages, including model training, validation, and testing, as well as the use of appropriate performance measures to assess the performance of the models. A set of candidate algorithms, that are suitable for the task of fraud detection, was identified. These algorithms are capable of handling the specific challenges associated with fraud detection, such as class imbalance, nonlinear relationships, and noisy data.

To evaluate the performance of the candidate algorithms and the ensemble methods, a three-step process was used: model training, validation, and testing. In model training, the pre-processed dataset was divided into a training set (70% of the data) and a test set (30% of the data). Candidate algorithms and ensemble methods were trained in the training set. In model validation, cross-validation was used during the training process to avoid overfitting and select the best hyperparameters for each algorithm. This involved splitting the training set into multiple folds (5 or 10), training the model in all but one fold, and validating the model on the remaining fold. This process was repeated for each fold, and the average performance across all folds was used to assess the model's performance. In model testing, the models were trained on the entire training set and tested on the test set once the best hyperparameters had been selected for each candidate algorithm and the ensemble method. The performance of the test set was used to assess the generalizability of the models and select the best-performing model(s).

Table I and Figure 1 highlight the performance comparison of different models for detecting bank account fraud. All models exhibited high accuracy scores, ranging from 0.96 to 0.98, indicating their ability to make correct predictions in most cases. However, accuracy alone may not provide a complete understanding of model effectiveness, as it does not consider the balance between correctly classified positive and negative cases. The precision, which represents the proportion of true positive predictions out of all positive predictions, varied among the models. The Stacking model demonstrated the highest precision score of 0.85, showing its proficiency in correctly identifying fraudulent cases among those labeled as such. On the other hand, LR exhibited the lowest precision, with a score of 0.65. This emphasizes the trade-off between precision and recall, as higher precision often comes at the cost of lower recall, and vice versa. Conversely, recall, signifying the model's ability to identify all relevant instances in the dataset, exhibited relatively consistent values among the models, ranging from 0.7 to 0.9. The Stacking model achieved the highest recall at 0.9, indicating its effectiveness in capturing a significant proportion of relevant instances. F1-score, the harmonic mean of precision and recall, provides a balanced assessment of a model's overall performance, as it considers both false positives and false negatives, making it a valuable metric for this classification task. The Stacking model achieved the highest F1-score of 0.87, reinforcing its position as a strong performer.

TABLE I. PERFORMANCE COMPARISON OF DIFFERENT MODELS

Model	**Accuracy**	**Precision**	**Recall**	**F1-score**
Voting Classifier	0.97	0.8	0.85	0.83
Random Forest	0.96	0.75	0.8	0.77
Gradient Boosting	0.96	0.7	0.75	0.73
Logistic Regression	0.96	0.65	0.7	0.68
Neural Networks	0.96	0.7	0.75	0.73
Stacking	**0.98**	**0.85**	**0.9**	**0.87**

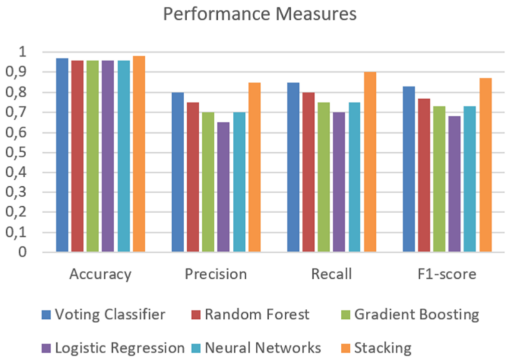

Fig. 1. Overall performance comparison between models.

The trade-off between precision and recall is evident in the results. Models with higher precision may tend to produce fewer false positives but could miss some relevant cases (lower recall), while models with higher recall may correctly capture more instances but might also produce more false positives (lower precision). The choice of model should be guided by the specific requirements and consequences associated with false positives and false negatives in the application. The Stacking model consistently emerges as a prominent performer in multiple metrics. Its ability to achieve a high F1-score demonstrates its effectiveness in achieving a balanced trade-off between precision and recall, essential for fraud detection tasks. Although the models presented show promise, the results also point to opportunities for further exploration and improvement. Achieving a higher level of accuracy, precision, and recall while maintaining an optimal balance is an ongoing challenge in the realm of fraud detection. This study paves the way for the development of more sophisticated and comprehensive solutions to enhance the robustness of fraud detection systems. The proposed fraud detection model using an ensembling method has several advantages over other methods. By combining the strengths of multiple models, the ensembling method can improve accuracy and robustness, reduce the risk of overfitting, and adapt to changing patterns in the data over time. This is particularly important in detecting sophisticated fraud patterns that may evolve over time.

This study pushed the boundaries of conventional approaches, introducing an innovative ensemble-based method that marks a significant leap forward in the field of fraud detection. The advanced assembly method proposed is characterized by enhanced precision and robustness, setting a new standard in the detection of fraudulent activities in financial transactions. This approach not only fortifies the integrity of transactional processes but also enriches the existing body of knowledge with novel insights and methods. The efficacy of the proposed ensemble-based strategy was manifested through meticulous evaluations, demonstrating unprecedented levels of accuracy and reliability. These advances are not merely incremental improvements; they represent transformative contributions to the field, opening up new avenues for research and practical applications. The significance of this study is twofold; it offers a robust solution to the pervasive challenges of fraud in financial domains and can serve as a catalyst for future innovations and developments in ensemble-based fraud detection methods. Through the infusion of this groundbreaking approach, this study aspires to redefine the paradigms of fraud detection and inspire a new wave of research focused on improving the security and reliability of financial ecosystems.

IV. FUTURE RESEARCH AND POTENTIAL IMPROVEMENTS

However, the proposed model still has some limitations. At first, the BAF dataset may not represent the full range of fraud patterns that can occur in real-world scenarios. Therefore, further testing and validation on larger datasets and with different types of fraud are required to confirm its generalizability. Second, the weights assigned to the predictions of the base models in the stacking method may not be optimal, and different weight optimization strategies could be explored in future research. In general, the proposed ensembling fraud detection model shows promising results in detecting bank account fraud, as it has the potential to improve the accuracy and robustness of current fraud detection systems and maintain customer trust and security in the banking industry. Future research intends to delve into model interpretability and feature-important analysis to gain a more profound understanding of the factors driving model predictions. Additionally, it is planned to explore ensemble techniques that can harness the strengths of individual models while mitigating their weaknesses, ultimately aiming for even more robust fraud detection systems.

Based on the results analysis and implications of the findings, future research areas can be identified and potential improvements to the proposed model can be suggested. This may include:

- Exploring alternative ensemble methods or combinations of algorithms to further improve the model's performance.
- Investigating the use of more advanced feature engineering techniques, such as deep learning-based methods or graph-based approaches, to capture more complex patterns in the transaction data.
- Addressing the issue of concept drift, where the underlying patterns in the data change over time, by incorporating adaptive and online learning techniques into the model.
- Incorporating additional data sources, such as social media or network information, to improve the model's ability to detect frauds and better understand the underlying patterns of fraudulent behavior.
- Investigating the interpretability and explainability of the model, which is crucial for practical applications in the banking industry, where human decision-makers need to understand the reasons behind the model's predictions.

V. CONCLUSIONS

This paper presented a fraud detection model for bank payments using an ensemble method, demonstrating its effectiveness in improving accuracy and robustness compared to individual models. The proposed model captures both global and local patterns in transaction data and adapts to changing patterns over time, making it suitable for detecting evolving fraud patterns. The proposed ensembling approach (Stacking model) offers a path to augmenting accuracy, model resilience, and adaptability in fraud detection systems. The applicability of the proposed model extends to diverse datasets and the potential integration into operational banking systems, promising enhanced customer trust and financial security. This study introduced a groundbreaking ensemble-based fraud detection model, that uses advanced methods to improve the precision and reliability of cyber threat classifications and countermeasures in financial transactions. The novel Stacking model presented not only exhibits superior performance in detecting fraudulent activities but also offers adaptability to evolving threat landscapes, marking a significant advancement in the domain of cybersecurity in financial sectors. This innovative approach and its robust findings have substantial implications for the development of more sophisticated, effective, and resilient fraud detection systems, contributing to ongoing efforts to protect financial ecosystems from increasing cyber threats.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the approval and support of this research study by grant no. SCIA-2022-11-1879 from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.

REFERENCES

[1] L. Wewege, J. Lee, and M. C. Thomsett, "Disruptions and Digital Banking Trends," *Journal of Applied Finance & Banking*, vol. 10, no. 6, pp. 1–2, 2020.

[2] T. Somogyi and R. Nagy, "Cyber Threats and Security Challenges in the Hungarian Financial Sector," *Contemporary Military Challenges*, vol. 24, no. 3, pp. 15–29, Sep. 2022, https://doi.org/10.33179/bsv.99.svi.11.cmc.24.3.1.

[3] C. Nobles, "Disrupting the U.S. National Security Through Financial Cybercrimes," *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, vol. 3, no. 1, pp. 1–21, Jan. 2019, https://doi.org/10.4018/IJHIoT.2019010101.

[4] S. Rai, R. Gyanesh, C. Karthic, K. Malesh, S. Jain, and V. Palrecha, "A Study on Financial Technology & Cyber Security in India," *International Scientific Journal of Engineering and Management*, vol. 2, no. 4, Apr. 2023, https://doi.org/10.55041/ISJEM00350.

[5] A. Darem, "Anti-Phishing Awareness Delivery Methods," *Engineering, Technology & Applied Science Research*, vol. 11, no. 6, pp. 7944–7949, Dec. 2021, https://doi.org/10.48084/etasr.4600.

[6] "African corporates face rising cybercrime risks," *Emerald Expert Briefings*, Jan. 2021, https://doi.org/10.1108/OXAN-DB262652.

[7] "Cyber Security in Banking Sector," *International Journal of Information Security and Cybercrime (IJISC)*, vol. 8, no. 2, pp. 39–52, 2019.

[8] V. Ghodasara, "Research on Importance of Cyber Security Audit and Assessment in Bank," *International Journal for Research in Applied Science and Engineering Technology*, vol. 7, no. 5, pp. 1409–1416, May 2019, https://doi.org/10.22214/ijraset.2019.5238.

[9] R. R. Asaad and V. A. Saeed, "A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution," *Applied computing Journal*, pp. 227–244, Dec. 2022, https://doi.org/10.52098/acj.202260.

[10] M. Moghimi and A. Y. Varjani, "New rule-based phishing detection method," *Expert Systems with Applications*, vol. 53, pp. 231–242, Jul. 2016, https://doi.org/10.1016/j.eswa.2016.01.028.

[11] A. S. Alraddadi, "A Survey and a Credit Card Fraud Detection and Prevention Model using the Decision Tree Algorithm," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11505–11510, Aug. 2023, https://doi.org/10.48084/etasr.6128.

[12] P. Vanini, S. Rossi, E. Zvizdic, and T. Domenig, "Online payment fraud: from anomaly detection to risk management," *Financial Innovation*, vol. 9, no. 1, Mar. 2023, Art. no. 66, https://doi.org/10.1186/s40854-023-00470-w.

[13] A. Alshutayri, "Fraud Prediction in Movie Theater Credit Card Transactions using Machine Learning," *Engineering, Technology & Applied Science Research*, vol. 13, no. 3, pp. 10941–10945, Jun. 2023, https://doi.org/10.48084/etasr.5950.

[14] G. J. Priya and S. Saradha, "Fraud Detection and Prevention Using Machine Learning Algorithms: A Review," in *2021 7th International Conference on Electrical Energy Systems (ICEES)*, Chennai, India, Oct. 2021, pp. 564–568, https://doi.org/10.1109/ICEES51510.2021.9383631.

[15] J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," in *2017 International Conference on Computing Networking and Informatics (ICCNI)*, Jul. 2017, pp. 1–9, https://doi.org/10.1109/ICCNI.2017.8123782.

[16] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga, and N. Kuruwitaarachchi, "Real-time Credit Card Fraud Detection Using Machine Learning," in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Jan. 2019, pp. 488–493, https://doi.org/10.1109/CONFLUENCE.2019.8776942.

[17] J. I.-Z. Chen and K.-L. Lai, "Deep Convolution Neural Network Model for Credit-Card Fraud Detection and Alert," *Journal of Artificial Intelligence and Capsule Networks*, vol. 3, no. 2, pp. 101–112, Jun. 2021, https://doi.org/10.36548/jaicn.2021.2.003.

[18] X. Zhang, Y. Han, W. Xu, and Q. Wang, "HOBA: A novel feature engineering methodology for credit card fraud detection with a deep

learning architecture," *Information Sciences*, vol. 557, pp. 302–316, May 2021, https://doi.org/10.1016/j.ins.2019.05.023.

[19] S. Jesus *et al.*, "Turning the Tables: Biased, Imbalanced, Dynamic Tabular Datasets for ML Evaluation," *Advances in Neural Information Processing Systems*, vol. 35, pp. 33563–33575, Dec. 2022.

[20] M. A. Khan *et al.*, "Voting Classifier-Based Intrusion Detection for IoT Networks," in *Advances on Smart and Soft Computing*, Singapore, 2022, pp. 313–328, https://doi.org/10.1007/978-981-16-5559-3_26.

[21] M. S. Kumar, V. Soundarya, S. Kavitha, E. S. Keerthika, and E. Aswini, "Credit Card Fraud Detection Using Random Forest Algorithm," in *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*, Chennai, India, Oct. 2019, pp. 149–153, https://doi.org/10.1109/ICCCT2.2019.8824930.

[22] Y. Ding, W. Kang, J. Feng, B. Peng, and A. Yang, "Credit card fraud detection based on improved Variational Autoencoder Generative Adversarial Network," *IEEE Access*, vol. 11, pp. 83680–83691, 2023, https://doi.org/10.1109/ACCESS.2023.3302339.

[23] A. A. Taha and S. J. Malebary, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine," *IEEE Access*, vol. 8, pp. 25579–25587, 2020, https://doi.org/10.1109/ACCESS.2020.2971354.

[24] Y. Sahin and E. Duman, "Detecting credit card fraud by ANN and logistic regression," in *2011 International Symposium on Innovations in Intelligent Systems and Applications*, Istanbul, Turkey, Jun. 2011, pp. 315–319, https://doi.org/10.1109/INISTA.2011.5946108.

[25] I. Sadgali, N. Sael, and F. Benabbou, "Fraud detection in credit card transaction using neural networks," in *Proceedings of the 4th International Conference on Smart City Applications*, Casablanca, Morocco, Jul. 2019, Art. no. 95, https://doi.org/10.1145/3368756.3369082.

[26] S. Mastromichalakis, "SigmoReLU: An Improvement Activation Function by Combining Sigmoid and ReLU." Preprints, Jun. 09, 2021, https://doi.org/10.20944/preprints202106.0252.v1.