

CLocMLGuard: A Novel Risk Scoring Framework for Transaction Card Fraud Mitigation and Detection with Machine Learning

Abdullah Md Raihan Chy

Dept. of CSE , SUB

Chittagong, Bangladesh

raihanchowdhuryengineer@gmail.com

Mohammad Jahangir Alam

Dept. of CSE , SUB

Chittagong, Bangladesh

Jahangir@southern.ac.bd

Md Farhan Shahriyar

Dept. of CSE , HSTU

Dinajpur, Bangladesh

farhanshahriyar.cse1@gmail.com

Abstract—Card fraud has become an increasing concern evolving through various tactics over the years. To combat these growing threats a multi-layered security strategy is essential. This research proposes CLocMLGuard, a framework for detecting transaction of credit card fraud by utilizing a two-layer risk scoring with machine learning model. The framework focuses on identifying unusual location-time patterns in transactions such as abnormal travel distances for ATM or online activities to predict fraud risks. It incorporates a two-layer risk scoring system: the first layer assesses the location-time distance while the second uses a machine learning model with specific features for further risk prediction. This approach enhances early detection particularly for cross border fraud reducing the time and cost associated with traditional models. The framework employs traditional machine learning models with Random Forest achieving the highest F1-Score of 94% outperforming other models.

Index Terms—Card Fraud Detection, Transaction Fraud, Risk Scoring, Machine Learning, ATM Fraud, Online Transaction Fraud, Risk Scoring Framework

I. INTRODUCTION

Credit card theft is a widespread and growing threat that affects various sectors including financial institutions, corporate enterprises, and government agencies. Strong systems for prompt detection and prevention are required. [1] As on line transactions and the sophistication of fraudulent activity even in atm transaction. In addition to increasing trade in goods and services like credit cards and telecommunications, the widespread use of electronic commerce in corporations, organizations, and government institutions has maximized productivity. However, these systems are more vulnerable to widespread fraud due to fraudsters and legitimate clients' simultaneous use of e-commerce networks. [2] Organizations utilize fraud control systems designed to secure new technology and prevent fraudulent activities to reduce the widespread danger of credit card theft. But depending only on preventive measures is insufficient, so fraud detection is being used as a process which necessitates accurate detection and identification skills which requires highly trained systems with pertinent data. With the quickening pace of technical development in society resulting in decreased cash payments and increased internet transactions, people are more susceptible to credit card fraud committed by unseen parties. [3]

Numerous online payment methods that simply require the card number, expiration date, and CVV present

potential for data breaches that may occur without the cardholder's awareness. The environment is made more complex by the anonymity of online transactions and scammers' employment of phishing tactics. Sometimes, people don't realize their data has been compromised until they see strange transactions. The rise of phishing websites presents a significant risk to user data, potentially leading to the unauthorized disclosure of sensitive information. Additionally, the loss or theft of physical credit cards further exposes users to financial vulnerability. [4] To mitigate these risks, understanding client spending patterns is crucial for verifying the legitimacy of transactions. By leveraging machine learning algorithms to analyze transaction trends, it is possible to differentiate between legitimate purchases and potential fraud.

Fraud can happen in many ways, such as phishing, fake applications, phone scams, stolen cards, and data breaches. Because of this, it is important to have a strong and flexible system to detect fraud. Data mining tools have helped in finding fraud, but credit card fraud detection still needs to be more accurate. While data mining tools have made strides in identifying fraudulent activity, the accuracy of credit card fraud detection still requires improvement. To effectively reduce the financial losses caused by fraud, advanced algorithms and more refined detection techniques are necessary. As the reliance on digital transactions grows, a secure and efficient credit card issuing and management system is vital. Fraudulent use of credit cards, whether through stolen physical cards, PINs, or account details, poses a serious threat. Therefore, detecting and preventing fraudulent transactions is critical not only to protect users but also to minimize potential financial losses. [5]

In machine learning if the dataset increases, the complexity increases. So, if we use more effective techniques before processing transactions through these models, it will be more time saving and cost minimizing. The risk scoring technique with traditional machine learning is a potent paradigm that provides advanced remarkable fraud detection skills. Machine learning

protects against dishonest tactics by detecting fraud with unmatched accuracy. Second, it performs exceptionally well in real-time streaming, making it possible to spot fraudulent transactions as soon as they happen. Thirdly, machine learning algorithms speed up fraud detection procedures by cutting down on the time needed for authentication procedures. Ultimately, machine learning with risk scoring techniques can reveal latent relationships in data, allowing for a deeper comprehension of trends and anomalies. This study enhances transaction card fraud detection with the following key contributions:

- Assessed a range of machine learning models find best for fraud detection for proposed CLocMLGuard system
- Introduced a unique two layer risk scoring framework, CLocMLGuard, which combines machine learning with location-time anomaly detection to enhance real time fraud detection.

This paper reviews existing literature in Section II and outlines its methodology in Section III. Experiments and their outcomes are covered in Section IV, and Section V provides concluding remarks and proposes future research directions.

II. LITERATURE REVIEW

A model of LR that can detect fraud achieving impressive results in terms of accuracy, sensitivity, and error rate. In comparison, their model outperformed KNN and the 5-Voting Classifier. KNN, tested with values of k ranging from 1 to 10, had a lower accuracy of 93% and a higher error rate of 7%, while the Voting Classifier performed somewhat lower overall. [6] Mani raj's team developed a model that achieved an exceptional detection rate, identifying 99.7% of fraudulent transactions. This approach drastically reduced the number of fraudulent transactions misclassified. Meanwhile, Dheepa and Dhanapal used a behavior-based classification method, which focused on customer transaction patterns such as time, location, and frequency. Their approach had a solid accuracy above 80 though it was slightly lower than some other methods. [7] Mailini and Pushpa tested KNN and outlier detection, finding that KNN was particularly effective in fraud detection, especially when memory limitations were a concern. However, outlier detection was faster and more memory efficient when processing large datasets, even though KNN achieved higher accuracy. [8]

Maes and colleagues found that Bayesian methods outperformed ANN by about 8% in fraud detection efficiency. While ANN required significantly more time to train, Bayesian methods were much faster taking just 20 minutes compared to several hours for ANN. [9] In an explored study, researchers tested KNN, NB, and LR on skewed credit card datasets. For one distribution (10:90), NB showed the highest accuracy at 97.5%, closely followed by KNN at 97.1%. LR, however, performed poorly in this scenario, achieving only 36.4% accuracy. In a different distribution (34:66), KNN again proved to be the best performer at

97.9%, with NB achieving a strong 97.6%. [10] Jain's team evaluated SVM, ANN, and KNN, reporting nearly 100% accuracy with ANN, while SVM had an accuracy of 94.65% and KNN achieved 97.15%. ANN also outperformed the others in terms of precision and false alarm rates.

A study assessed at different machine learning methods for finding fraud. It found that NB was the best technique. NB was very good at spotting fraudulent transactions. It had an accuracy of about 80% and a high AUC score. [11] Adepoju and colleagues tested SVM, Naïve Bayes, and KNN on skewed datasets. They found that SVM had the highest accuracy at around 97.5%, while KNN and Naïve Bayes had slightly lower, but still very good, performance. [12] Safa and Ganga also evaluated KNN, Logistic Regression, and Naïve Bayes. Their findings showed that Logistic Regression outperformed the others with an accuracy of 97.69%, while KNN scored significantly lower at 54.86%. [13] A related study looked at several models: RF, MLP, NB, and LR. They used SMOTE to balance the data. RF had the best accuracy at 99.96%. MLP was close behind at 99.93%. NB achieved 99.23%, and LR came in at 97.46%. [14] Sailusha's team compared Adaboost and Random Forest, finding that Random Forest performed slightly better achieving a high accuracy. [15]

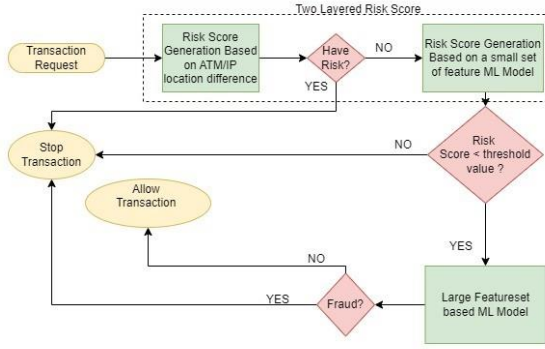
Another study also proved Random Forest's supremacy in their task. [16] Kiran's hybrid approach, combining Naïve Bayes with KNN, achieved 95% accuracy, outperforming KNN. Najdat's team used advanced models like BiLSTM-

BiGRU along with classifiers such as KNN and Logistic Regression. KNN achieved good accuracy while Logistic Regression performed slightly lower. [17] Genetic Algorithms were used for feature selection. This was tested with NB, RF, and SVM models. RF showed the highest accuracy. SVM's accuracy increased by 5%, placing it closely behind RF. NB, however, had lower accuracy. [18] [19]

III. METHODOLOGY

A. The Proposed Method

The proposed framework in fig 1 integrates anomaly detection based on location-time factors such as ATM or online transaction patterns and uses machine learning models for decision-making based on predicted risk scores. The approach involves two main stages: first, identifying potential location time anomalies (e.g., unusual travel distances for ATM or online transactions) and lastly various transaction features are used in ML models to predict risk based on . Finally the machine learning models are evaluated based on their ability to predict fraud. Security laws and privacy concerns make it hard to use PII (Personally Identifiable Information). PII is important for



exact location-time analysis, but it's just not available. Even without this data, the CLocMLGuard system still evaluates its ML-based fraud detection model using the datasets it has.

B. Risk Score Generation Based on ATM/IP Location-TimeEvaluation

Algorithm 1 outlines a step-by-step process for detecting potential fraud based on location-time anomalies in both ATM and online transactions. The algorithm starts by initializing

Fig. 1. Risk Scoring Based Credit Card Fraud Detection System CLocMLGuard.

the risk score r to 0, which will be updated based on the outcome of various checks. For ATM transactions, the system figures out two things: how much time passed since the last transaction and how far apart the two transaction locations are. Using a speed threshold, the algorithm determines the maximum possible travel distance. If the actual distance exceeds this threshold, the transaction is flagged as suspicious, and the algorithm stops ("Stop"). If the transaction passes the location-time checks, it moves to Algorithm 2 for further analysis using machine learning. For online transactions, the algorithm compares the IP locations of the current and previous transactions, calculating the distance between them. It then checks if the distance is feasible based on the time difference and the speed threshold. If the distance exceeds the maximum allowable travel distance, it indicates a potential fraud (e.g., a user making a transaction from an unlikely location), and the risk score is incremented accordingly. If no anomalies are detected, the algorithm moves to Algorithm 2 for further decision-making. In both cases, the algorithm helps flag suspicious transactions based on location-time inconsistencies, contributing to fraud detection and prevention.

C. Risk Score Generation Based on Machine Learning Algorithms

Algorithm 2 outlines a machine learning-based process for predicting and making decisions about transaction risk. The algorithm begins by combining key features (F, user id, device id, and txn type) into an input vector (ml input). It goes into a pre-trained ML model. The model then predicts the transaction's risk.

Algorithm 1 Risk Scoring and Anomaly Detection Based on ATM/IP Location-Time

```

1: Step 1: Initialize Risk Scoring
2:  $r \leftarrow 0$ 
3: Step 2: Location-Time Anomaly Check for ATM Transactions
4: if txn type = ATM then
5:    $time\_diff \leftarrow txn\_time - last\_txn\_time$ 
6:    $distance \leftarrow CalculateDistance(last\_loc, current\_loc)$ 
7:    $max\_travel\_distance \leftarrow speed\_threshold \times time\_diff$ 
8:   if  $distance > maxpossible\_travel\_distance$  then
9:     If this predicted risk hits or goes over a set risk threshold, the transaction is flagged as suspicious right away. The system then outputs "Stop." If the predicted risk is below the threshold, the algorithm moves to a deeper analysis by combining a larger set of features (F large, user id, device id, txn type) into a new input vector (large ml input). This input is then processed by a more complex model (large model) to make a final prediction. If the final prediction classifies the transaction as "fraud," the algorithm returns "Stop," flagging it as fraudulent. If the transaction is not predicted to be fraudulent, the algorithm allows the transaction and returns
10:   else
11:     Call: Algorithm 2 (Machine Learning Prediction and Decision Making)
12:   end if
13: end if
14: Step 3: Location-Time Anomaly Check for Online Transactions
15: if txn type = Online then
16:    $current\_ip\_loc \leftarrow GetIPLocation(current\_loc)$ 
17:    $last\_ip\_loc \leftarrow GetIPLocation(last\_loc)$ 
18:    $distance \leftarrow CalculateDistance(last\_ip\_loc, current\_ip\_loc)$ 
19:    $max\_travel\_distance \leftarrow speed\_threshold \times (txn\_time - last\_txn\_time)$ 
20:   if  $distance > maxpossible\_travel\_distance$  then
21:     return "Stop"
22:   else
23:     Call: Algorithm 2 (Machine Learning Prediction and Decision Making)
24:   end if
25: end if
  
```

Algorithm 2 Machine Learning Prediction and Decision Making Based on Risk

```

1: Step 4: Predict Risk Using Machine Learning Model
2:  $ml\_input \leftarrow \text{Combine}(F, [user\_id, device\_id, txn\_type])$ 
3:  $predicted\_risk \leftarrow model.predict(ml\_input)$ 
4: Step 5: Decision Making Based on Predicted Risk
5: if  $predicted\_risk \geq risk\_threshold$  then
6:     return "Stop"
7: else
8:      $large\_ml\_input \leftarrow \text{Combine}(F_{large}, [user\_id, device\_id, txn\_type])$ 
9:      $final\_prediction \leftarrow large\_model.predict(large\_ml\_input)$ 
10:    if  $final\_prediction = fraud$  then
11:        return "Stop"
12:    else
13:        return "Allow"
14:    end if
15: end if

```

"Allow." Overall, Algorithm 2 enhances the fraud detection process by using machine learning to evaluate transaction risk, making it capable of handling both high-risk and borderline transactions with higher accuracy.

D. The Machine Learning Based Detection with Large Feature set

A overview of Large Featureset Based Detection with Machine Learning proppes is shown in fig2.

1) *The Card Fraud Dataset*: The dataset [20] is used here which includes information on credit card transactions conducted by cardholders in Europe covering all transactions over a two-day period. The dataset was organized through a self-classification and data mining task, and for detailed information on its contents and relationships, reference to [30] is suggested. Access to the dataset is direct, allowing storage on a network disk or local hard drive. Privacy concerns under laws like GDPR and CCPA likely led to the use of PCA in the dataset, ensuring data anonymity and compliance while allowing for fraud detection.

2) *Data Preprocessing*: It is an essential pre processing step and ensures the dataset's quality and reliability. It is used in this study to identify and rectify flaws, inconsistencies, and inaccuracies, preparing the data for analysis. Missing values are handled by imputation algorithms or by removing affected rows or columns. Dupli cates are eliminated to avoid skewed analysis that could affect model accuracy. A problem in fraud detection is class imbalance. This means there are many more normal transactions than fraudulent ones. To fix this, methods like SMOTE are used. SMOTE helps balance the dataset and makes models work better by creating fake data points. 3) *The models included in this evaluation are*:

- Random Forest: This learning method uses many decision trees. It then combines all their predictions. This is to improve accuracy as well as tackle the overfitting. It is widely used for

classification tasks and friendly to handle multi dimensional data.

- MLP (Multi-Layer Perceptron): It works on a number of layered nodes with neural networks to capture complex relationships in the data. MLP is a powerful model for non-linear decision boundaries and is often used in situations where feature interactions are not easily captured by traditional models.
- Gradient Boosting: This technique reduces the errors in the current model learning from the previous one by utilizing ensemble mechanism. It is highly competent in improving predictive performance on structured data and is often used when a model requires fine tuning to achieve optimal results.
- Decision Tree: A simple but interpretable model that divides the data into subsets. The subsets are formed on the basis of feature values. Decision Trees are fast to train and easy to interpret but may suffer from overfitting if not effectively regularized.
- ANN (Artificial Neural Network): A well-known deep learning model is designed like the human brain. It uses

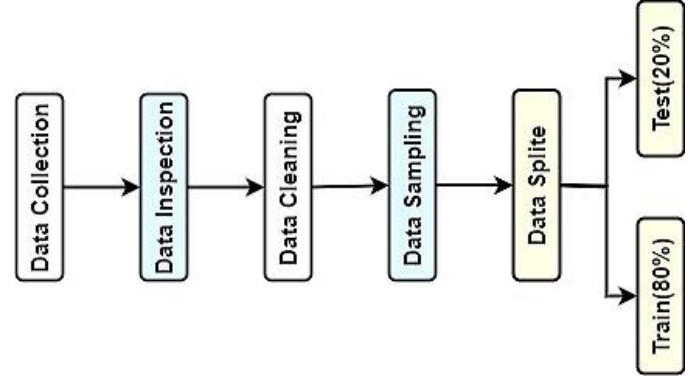


Fig. 2. Large Feature set based Machine Learning Detection Approach.

layers of interconnected nodes to learn complex patterns within data. ANNs can capture intricate relationships in data but they require a handful of data as well as computational power for effective training.

- Logistic Regression: It is used as a simple linear task for binary classification. A set of features as a input data provides a probability of a task. Despite its simplicity logistic regression is often a baseline model that most of the time ensures efficiency and interpretability for binary classification.

IV. EXPERIMENTS AND RESULTS

Table I evaluates different ML model performances using their F1 scores. This is important because the dataset is imbalanced, meaning fraud transactions are much fewer.

RF had the highest F1 score at 0.94, almost twice that of LR (0.55). The MLP model also performed well, scoring 0.89 F1. This was about 1.6 times better than GB, which got 0.60. ANN also showed strong results with an F1 score of 0.90, slightly beating MLP. Finally, the DT model had an F1 score of 0.76, around 1.4 times higher than LR. Random Forest outperformed all other models by a significant margin in terms of F1 score with its effectiveness in handling the imbalanced dataset with fraud transactions.

TABLE I

PERFORMANCE OF VARIOUS MODELS ON FRAUD DETECTION (F1 SCORE)

Model	F1-Score
Random Forest	0.94
MLP (Neural Network)	0.89
Gradient Boosting	0.60
Decision Tree	0.76
ANN (Artificial Neural Net)	0.90
Logistic Regression	0.55

In fig 3 the normal transactions are highly misclassified as fraud by LR and GB. The lowest misclassification of normal transactions is observed in RF. Fraud cases are mostly misclassified as normal by DT and ANN. The RF model consistently maintains superior performance in all metrics.

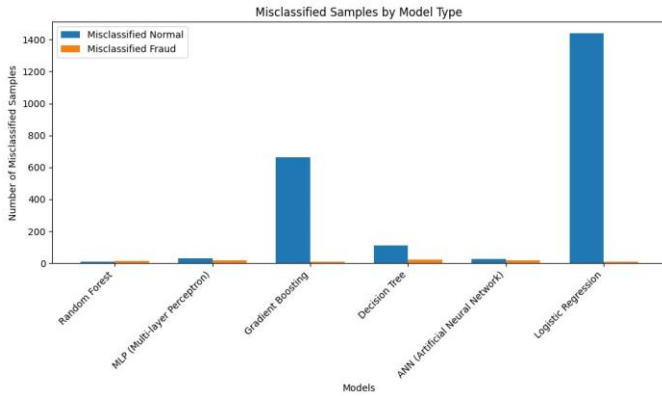


Fig. 3. Misclassification of different ML models.

V. CONCLUSION AND FUTURE WORK

This study presents a new two-layered risk scoring system called CLocMLGuard. It uses heavy and light ML models to improve fraud detection in card transactions. The primary goal of this system is to assign a risk score to each transaction in real-time enabling early detection of fraudulent activity. In this study, RF performed best. It got an F1 score of 0.94, making it excellent at finding fraudulent transactions. This was true even though the dataset was imbalanced, with far fewer fraud cases than normal ones. Gradient Boosting is still successful in classifying fraud cases, albeit with a lower F1 score.

To improve fraud detection future work could combine different models such as Random Forest with Gradient Boosting or MLP to take advantage of their strengths. Deep learning models like CNNs and RNNs could also help find more complex patterns in transaction data with risk scoring method. Improving feature engineering by adding user behavior and device data could also boost performance. Additionally, tech niques like SMOTE could help balance the data. Methods like transfer learning and unsupervised learning could be helpful when there is little labeled data.

Since fraud detection needs to work in real time, it is important to optimize how quickly models process transactions. Using efficient hardware like edge devices or cloud computing will help deploy these models effectively. Future research can improve fraud detection systems and reduce financial fraud risks. Finally, combining intrusion detection techniques (IDTs) with deep machine learning models or BERT[21] could further strengthen fraud detection and reduce financial loss.

REFERENCES

- [1] Australian Bureau of Statistics, "Card fraud rises amid increasing use of digital payments," 2023. Accessed: 2024-11-17.
- [2] R. Rajendran, "Data breach fraudulence and preventive measures in ecommerce platforms," in **Advancements in Cybercrime Investigation and Digital Forensics**, pp. 161–184, Apple Academic Press, 2024.
- [3] Security.org, "Credit card fraud statistics and prevention tips," July 2023. Accessed: 2024-11-24.
- [4] I. D. Mienye and N. Jere, "Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions," **IEEE Access**, 2024.
- [5] N. Wilson, "The aftermath of transunion: An empirical analysis of standing in federal data breach cases 2021–2023," 2024.
- [6] H. Z. Alenzi and N. O. Aljehane, "Fraud detection in credit cards using logistic regression," **International Journal of Advanced Computer Science and Applications**, vol. 11, no. 12, 2020.
- [7] S. Maniraj, A. Saini, S. Ahmed, and S. Sarkar, "Credit card fraud detection using machine learning and data science," **International Journal of Engineering Research**, vol. 8, no. 9, pp. 110–115, 2019.
- [8] N. Malini and M. Pushpa, "Analysis on credit card fraud identification techniques based on KNN and outlier detection," in **2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)**, pp. 255–258, IEEE, 2017.
- [9] S. Maes, K. Tuyls, B. Vanschoenwinkel, and B. Manderick, "Credit card fraud detection using Bayesian and neural networks," in **Proceedings of the 1st International NAISO Congress on Neuro Fuzzy Technologies**, vol. 261, p. 270, 2002.
- [10] 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)**, pp. 1–9, IEEE, 2017.
- [11] A. Gupta, M. Lohani, and M. Manchanda, "Financial fraud detection using naive Bayes algorithm in highly imbalance data set," **Journal of Discrete Mathematical Sciences and Cryptography**, vol. 24, no. 5, pp. 1559–1572, 2021.
- [12] O. Adepoju, J. Wosowei, H. Jaiman, et al., "Comparative evaluation of credit card fraud detection using machine learning techniques," in **2019 Global Conference for Advancement in Technology (GCAT)**, pp. 1–6, IEEE, 2019.

- [13] S. Marabad, "Credit card fraud detection using machine learning," **Asian Journal For Convergence In Technology (AJCT)**, vol. 7, no. 2, pp. 121–127, 2021.
- [14] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "Credit card fraud detection-machine learning methods," in **2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)**, pp. 1–5, IEEE, 2019.
- [15] R. Sailusha, V. Gnaneswar, R. Ramesh, and G. R. Rao, "Credit card fraud detection using machine learning," in **2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)**, pp. 1264–1270, IEEE, 2020.
- [16] M. F. Shahriyar, Z. S. Seyam, A. Ullah, and M. N. Sakib, "Phishing detection in browser-in-the-middle: A novel empirical approach incorporating machine learning algorithms," in **International Conference on Advanced Network Technologies and Intelligent Computing**, pp. 123–134, Springer, 2023.
- [17] H. Najadat, O. Altiti, A. A. Aqouleh, and M. Younes, "Credit card fraud detection based on machine and deep learning," in **2020 11th International Conference on Information and Communication Systems (ICICS)**, pp. 204–208, IEEE, 2020.
- [18] Y. K. Saheed, M. A. Hambali, M. O. Arowolo, and Y. A. Olasupo, "Application of GA feature selection on naive Bayes, random forest and SVM for credit card fraud detection," in **2020 International Conference on Decision Aid Sciences and Application (DASA)**, pp. 1091–1097, IEEE, 2020.
- [19] F. Itoo, Meenakshi, and S. Singh, "Comparison and analysis of logistic regression, naïve Bayes and KNN machine learning algorithms for credit card fraud detection," **International Journal of Information Technology**, vol. 13, no. 4, pp. 1503–1511, 2021.
- [20] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," in **2015 IEEE Symposium Series on Computational Intelligence**, pp. 159–166, IEEE, 2015.
- [21] G. Tanbhir, M. F. Shahriyar, K. Shahed, A. M. R. Chy, and M. A. Adnan, "Hybrid machine learning model for detecting bangla smishing text using bert and character-level cnn," *arXiv preprint arXiv:2502.01518*, 2025.