



ISSN 1989-9572

DOI:10.47750/jett.2024.15.05.31

Artificial Intelligence Based Fake or Fraud Phone Calls Detection

B. Durga Bhavani¹, Uppala Nikitha², Patlolla Nandini², Nethrika Reddy Gogu²

Journal for Educators, Teachers and Trainers, Vol.15(5)

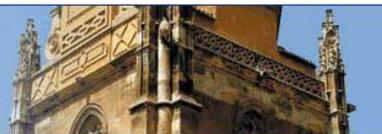
<https://jett.labosfor.com/>

Date of Reception: 24 Oct 2024

Date of Revision: 20 Nov 2024

Date of Publication : 31 Dec 2024

B. Durga Bhavani¹, Uppala Nikitha², Patlolla Nandini², Nethrika Reddy Gogu² (2024). Artificial Intelligence Based Fake or Fraud Phone Calls Detection, Vol.15(5).318-327



Journal for Educators, Teachers and Trainers, Vol. 15(5)

ISSN1989-9572

<https://jett.labosfor.com/>

Artificial Intelligence Based Fake or Fraud Phone Calls Detection

B. Durga Bhavani¹, Uppala Nikitha², Patlolla Nandini², Nethrika Reddy Gogu²

¹Assistant Professor, ²UG Student, ^{1,2}Department of Information Technology

^{1,2}Malla Reddy Engineering College for Women (UGC – Autonomous), Maisammaguda, Hyderabad, 500100, Telangana.

Corresponding Email: bhavanifdp@gmail.com

ABSTRACT

Technology and fraud strategies have made fraudulent phone call detection more complex, from manual monitoring and basic rule-based systems to AI-driven solutions. Rule-based algorithms dominated fraud detection systems before AI. These algorithms identified previously false patterns. A rule may indicate calls from countries with high phone fraud rates or calls made to many recipients quickly. Static Blacklist Dependence Known fake numbers were tracked using static blacklists. These manually updated lists automatically blocked or flagged calls from these numbers. For instance, a phone number that consistently committed fraud would be blacklisted. Automatically block or review future calls from that number. Human Analysts Monitor Manually Because automated systems were limited, human analysts monitored and made decisions about possibly fraudulent calls. These analysts checked flagged calls for fraud. Analysts manually reviewed call records, listened to call recordings, and used their judgment and experience to uncover fraud. Caller ID and Basic Metadata Integration Limited. Current systems typically fail to recognize and prevent sophisticated fake/fraud phone calls, causing users huge financial losses and security breaches. These old methods can't handle modern fraud. By quickly and reliably detecting and mitigating fraudulent phone calls, AI-driven solutions improve user safety and confidence. Security and financial losses can be prevented by better detection. NLP and ML are used to analyze call patterns, voice features, and contextual data in real time in proposed systems. These systems detect and prevent fraudulent calls, reacting swiftly to new fraud strategies to safeguard users.

Keywords: Telecommunications, Fake call detection, Fraud messages, Artificial intelligence.

1. INTRODUCTION

An important aspect for efficiently detecting and suppressing fraud is the detection of fraudulent phone calls [1]. The widespread use of voice over Internet protocol (VoIP) and phone number

modification software, together with the ongoing shift of phone fraud to other nations, has resulted in an increase in the variety and sophistication of fake phone numbers [2]. These modifications render ineffective the conventional black-list based crowd sourcing paradigm. Simultaneously, fraudulent phone call behavior is evolving and improving at a dizzying rate, and the amount of opposition is growing [2]. This detection test is challenging since counterfeit phone numbers are often unpredictable and their call behavior is often opposable. A number of behavioral characteristics, including call frequency, duration, and long-distance call rate, differ between legitimate and fraudulent phone calls, according to the "Scam Call Activity Regularity and Behaviour Features Analysis Report 2016" [3] published by the 360 Internet Security Centre as well as prior studies. However, there is some consistency to phone numbers in general, such as nonstandard numbers, foreign numbers, short numbers, or phony numbers, even if fraudulent phone numbers are unpredictable and unpredictable in nature [5]. Many conventional machine learning methods for detecting fraudulent phone calls have been developed using the aforementioned characteristics.

The government, companies, and individuals are all vulnerable to the ever-changing threat of phone-based spam or frauds [7]. In 2021, the United States' Federal Trade Commission (FTC) received more than 3 million allegations of fraud, leading to a total loss of \$3 billion. In order to get access to sensitive information, steal money, or damage someone's reputation, spammers utilize a number of tactics, such as digital manipulation, impersonation, as well as spoofing. Financial and information losses occurred on a global scale as a consequence. The whole point of fraudulent phone calls is to make you feel anxious and worried. Manually reviewing call information and recordings in search of fraudulent trends is the conventional approach [14] to discovering harmful phone calls. But these ways aren't always helpful in spotting new kinds of frauds, and they may be costly and time-consuming. Consequently, an effective method is required to identify and evaluate fraudulent phone calls with high precision and efficiency.

2. LITERATURE SURVEY

Fawcett and Provost [1] explored adaptive fraud detection methods in their seminal work published in **Data Mining and Knowledge Discovery**. They focus on enhancing fraud detection techniques by adapting to changing patterns in data. The authors discuss various algorithms and models used in fraud detection and emphasize the importance of dynamic adaptation to new fraudulent strategies. Their research provides foundational insights into the development of adaptive systems capable of identifying and mitigating fraud effectively. Weng et al. [2] addressed online e-commerce fraud through a large-scale detection and analysis study presented at the 2018 IEEE 34th International Conference on Data Engineering (ICDE). The paper highlights advanced detection methods for e-commerce fraud, leveraging large datasets and sophisticated analysis techniques. The authors discuss their approach's scalability and effectiveness in identifying fraudulent activities in online transactions, providing a comprehensive overview of current practices and challenges in e-commerce fraud detection.

Gowri et al. [3] investigated telephony spam and scam detection using Recurrent Neural Network (RNN) algorithms. Their study, presented at the 2021 International Conference on Advanced Computing and Communication Systems (ICACCS), demonstrates the application of RNNs for detecting fraudulent and spam calls. The authors evaluate the performance of their proposed model, showcasing its effectiveness in improving the accuracy of telephony fraud detection. Their work highlights the potential of deep learning techniques in addressing issues related to phone-based fraud. Abidogun [4] conducted research on fraud detection in mobile telecommunications through data mining and call pattern analysis. His PhD dissertation, available from the University of the Western Cape, employs unsupervised neural networks to analyze call patterns and detect fraudulent activities.

The study offers an in-depth analysis of various data mining techniques and their applications in telecommunication fraud detection, providing valuable insights into the effectiveness of neural networks in this domain. Sandhya et al. [5] proposed a machine learning method for detecting and analyzing fraud phone calls. Published in the **International Journal of Recent Technology and Engineering**, their paper evaluates different machine learning algorithms for identifying fraudulent calls in telecom datasets. The authors discuss the performance of their proposed methods and highlight their contributions to improving fraud detection in telephony systems. Their research underscores the importance of leveraging machine learning for enhancing fraud prevention strategies.

Akhter and Ahamad [6] explored telecommunication fraud detection using neural networks through data mining techniques. Their paper, published in the **International Journal of Scientific & Engineering Research**, presents various neural network models for detecting fraud in telecom networks. The authors evaluate the effectiveness of these models in identifying fraudulent activities and discuss their potential for improving fraud detection systems. Their work contributes to the ongoing efforts to enhance the accuracy and reliability of fraud detection in telecommunications. Murynets et al. [7] analyzed and detected SIMbox fraud in mobility networks. Their study, presented at IEEE INFOCOM 2014, focuses on identifying SIMbox fraud, a type of fraud involving the use of unauthorized SIM cards to bypass telecom charges. The authors discuss their proposed detection techniques and evaluate their effectiveness in preventing SIMbox fraud. Their research provides valuable insights into combating this specific type of telecom fraud and improving network security. Crawford et al. [8] conducted a survey on review spam detection using machine learning techniques. Published in the **Journal of Big Data**, their study reviews various methods for detecting spam in online reviews. The authors provide a comprehensive overview of machine learning approaches and their applications in identifying fraudulent reviews. Their research highlights the challenges and advancements in review spam detection, offering insights into current practices and future directions in this field.

Marzuoli et al. [9] uncovered the landscape of fraud and spam in the telephony channel through their study presented at the 2016 IEEE International Conference on Machine Learning and Applications (ICMLA). The paper investigates various types of fraud and spam in telephony systems and discusses the methods used for detection and prevention. The authors provide insights into the challenges faced in combating fraud and spam in telecommunication networks, offering a broad perspective on the issue. Teh et al. [10] explored statistical and spending behavior-based fraud detection in card-based payment systems. Their study, presented at the 2018 International Conference on Electrical Engineering and Informatics (ICELTICs), focuses on identifying fraudulent transactions through statistical analysis and spending behavior patterns. The authors discuss their approach's effectiveness in detecting fraudulent activities and highlight its potential for improving payment system security.

Tu et al. [11] conducted a survey on techniques against telephone spam, presented at the 2016 IEEE Symposium on Security and Privacy (SP). Their paper provides a comprehensive review of various methods and technologies used to combat robocalls and other forms of telephone spam. The authors discuss the effectiveness of different approaches and highlight the challenges faced in addressing telephone spam. Their research contributes to the development of strategies for improving telephone communication security. Crawford et al. [12] revisited the survey of review spam detection using machine learning techniques, published in the **Journal of Big Data**. Their study offers an updated overview of methods for detecting spam in online reviews and provides insights into recent advancements and challenges. The authors discuss various machine learning models and their applications in review spam detection, offering a valuable resource for researchers and practitioners in this field. Subudhi and Panigrahi [13] introduced the Quarter-Sphere Support Vector Machine (QS-

SVM) for fraud detection in mobile telecommunication networks. Published in *Procedia Computer Science*, their study presents a novel SVM-based approach for identifying fraudulent activities. The authors evaluate the performance of QS-SVM and compare it with other fraud detection methods, highlighting its effectiveness and potential for improving telecommunication fraud detection. Aras and Güvensan [14] discussed challenges and key points for fraud detection in aviation, presented at the 2021 International Conference on Innovations in Intelligent Systems and Applications (INISTA). Their paper explores the unique challenges faced in detecting fraud within the aviation industry and presents strategies for addressing these challenges. The authors provide insights into the application of advanced fraud detection techniques in aviation, contributing to the development of more effective fraud prevention measures.

3. PROPOSED ALGORITHM

The process of detecting fraudulent phone calls involves several key steps from dataset preparation to model evaluation. Initially, a dataset containing labeled phone call messages is gathered. This dataset undergoes preprocessing to clean and prepare the data for modeling. Traditional methods, such as Naive Bayes, are employed to build a baseline model, while more advanced techniques, such as Long Short-Term Memory (LSTM) networks, are explored to potentially improve performance. A detailed performance comparison between the traditional and proposed methods is conducted to assess improvements. Finally, the trained LSTM model is used to predict outcomes on test data, showcasing its effectiveness in detecting fraudulent calls.

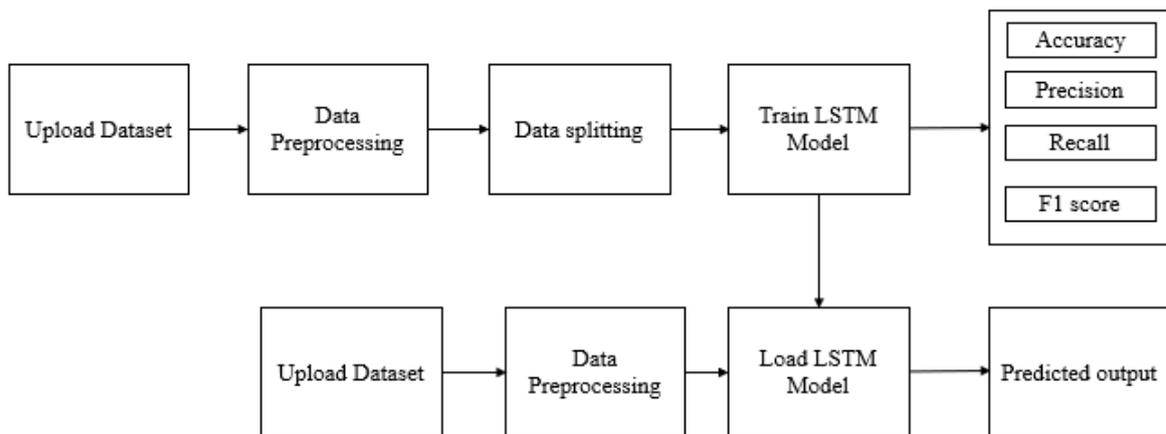


Figure 1: Block Diagram

Step 1: Dataset The process begins with the acquisition of a dataset containing phone call messages labeled as either 'normal' or 'fraud'. This dataset is the foundation for training and evaluating the fraud detection models. It is crucial that the dataset is representative of real-world scenarios to ensure that the model generalizes well to unseen data.

Step 2: Dataset Preprocessing (Null Value Removal, Label Encoding) Once the dataset is loaded, the next step involves preprocessing to clean the data. This includes removing any null values that could adversely affect model performance. The labels in the dataset, which denote whether a message is 'normal' or 'fraud', are encoded into numerical values. This step transforms categorical data into a format suitable for machine learning algorithms, ensuring that the model can interpret and process the data effectively.

Step 3: Label Encoding Label encoding involves converting categorical labels into numerical format. In this case, 'normal' is encoded as 0 and 'fraud' as 1. This transformation is necessary because machine learning algorithms typically require numerical input to perform computations. Label encoding ensures that the model can accurately process and learn from the labeled data.

Step 4: Existing (Naive Bayes Algorithm) A traditional machine learning approach, such as the Naive Bayes algorithm, is employed as a baseline model. Naive Bayes is a probabilistic classifier based on Bayes' theorem, which assumes independence between features. This step involves training the Naive Bayes model on the preprocessed dataset to establish a benchmark for performance evaluation. The results from this model provide a reference point for comparing more advanced algorithms.

Step 5: Proposed (LSTM Algorithm) To explore potential improvements in fraud detection, a Long Short-Term Memory (LSTM) network is proposed. LSTM is a type of Recurrent Neural Network (RNN) capable of learning long-term dependencies and sequences, making it suitable for analyzing textual data. This step involves designing, training, and tuning the LSTM model to capture complex patterns and contextual information in phone call messages.

Step 6: Performance Comparison A comprehensive performance comparison is conducted between the Naive Bayes and LSTM models. Metrics such as accuracy, precision, recall, and F1 score are used to evaluate and compare the effectiveness of both algorithms. This comparison highlights the strengths and limitations of each approach, providing insights into the advantages of the LSTM model over traditional methods.

Step 7: Prediction of Output from Test Data with (LSTM Algorithm) Trained Model Finally, the trained LSTM model is used to predict outcomes on a separate test dataset. This step demonstrates the model's ability to generalize to new, unseen data. By applying the LSTM algorithm to the test data, predictions are generated, which can then be compared with the actual labels to assess the model's performance and accuracy in real-world scenarios.

4. RESULTS AND DISCUSSION

Figure 2 shows the model was trained on 3565 samples and validated on a separate set of 992 samples, completing 10 training epochs. During the 10th epoch, all training samples were processed, resulting in a low training loss of 0.0059 and a high accuracy of 99.89%, indicating strong performance on the training data. On the validation set, the model had a loss of 0.1106 and an accuracy of 97.20%, suggesting good generalization.

```

Train on 3565 samples, validate on 892 samples
Epoch 1/10
3565/3565 [=====] - 16s 4ms/step - loss: 0.2902 - acc: 0.8931 - val_loss: 0.1739 - val_acc: 0.9350
Epoch 2/10
3565/3565 [=====] - 15s 4ms/step - loss: 0.1051 - acc: 0.9731 - val_loss: 0.1014 - val_acc: 0.9742
Epoch 3/10
3565/3565 [=====] - 15s 4ms/step - loss: 0.0580 - acc: 0.9868 - val_loss: 0.0853 - val_acc: 0.9742
Epoch 4/10
3565/3565 [=====] - 16s 4ms/step - loss: 0.0379 - acc: 0.9913 - val_loss: 0.0888 - val_acc: 0.9753
Epoch 5/10
3565/3565 [=====] - 16s 4ms/step - loss: 0.0264 - acc: 0.9930 - val_loss: 0.0912 - val_acc: 0.9664
Epoch 6/10
3565/3565 [=====] - 16s 4ms/step - loss: 0.0195 - acc: 0.9950 - val_loss: 0.0841 - val_acc: 0.9753
Epoch 7/10
3565/3565 [=====] - 19s 5ms/step - loss: 0.0156 - acc: 0.9958 - val_loss: 0.0876 - val_acc: 0.9720
Epoch 8/10
3565/3565 [=====] - 15s 4ms/step - loss: 0.0099 - acc: 0.9975 - val_loss: 0.0965 - val_acc: 0.9720
Epoch 9/10
3565/3565 [=====] - 15s 4ms/step - loss: 0.0095 - acc: 0.9975 - val_loss: 0.1049 - val_acc: 0.9709
Epoch 10/10
3565/3565 [=====] - 15s 4ms/step - loss: 0.0059 - acc: 0.9989 - val_loss: 0.1106 - val_acc: 0.9720

```

Figure 2: LSTM output

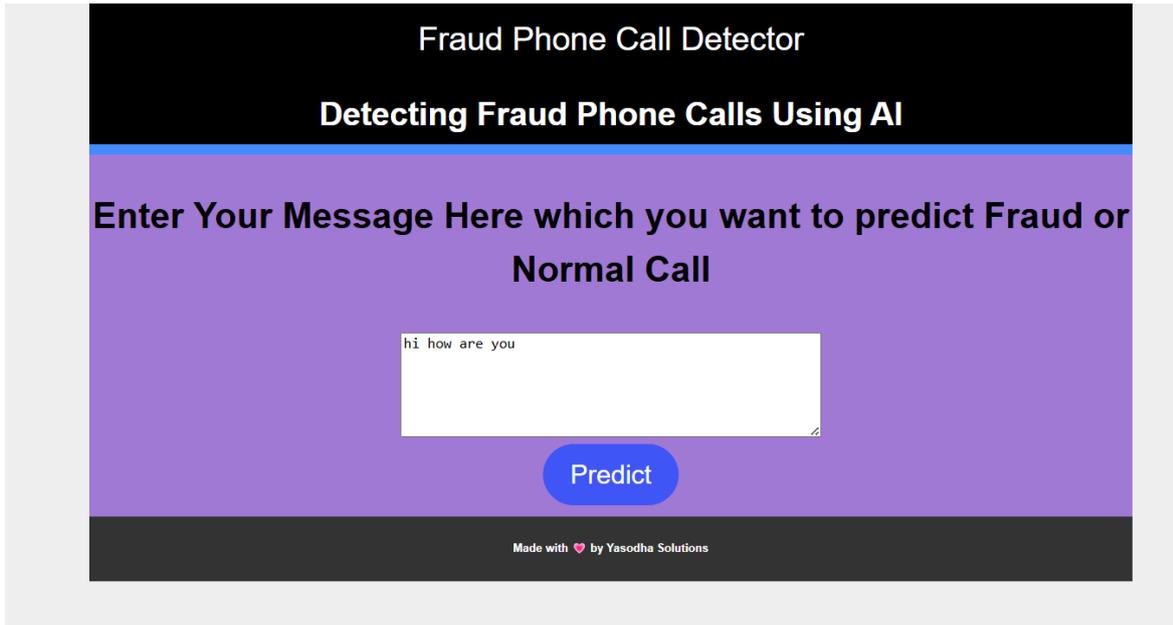


Figure 3: After gave input Message

Figure 3 shows that After we gave input (phone call messages)

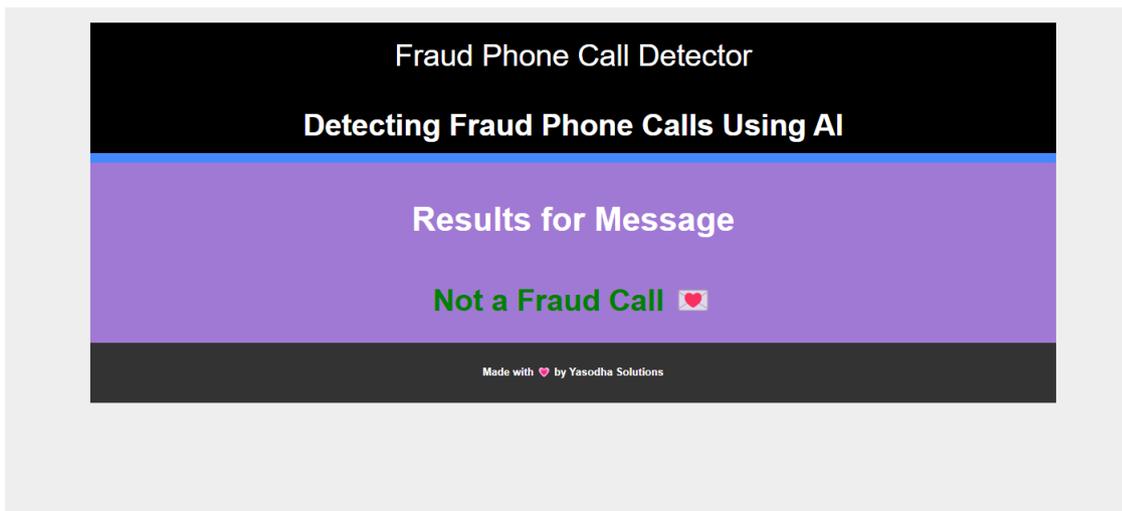


Figure 4: Detected Output

Figure 4 shows that the for an given input is has detected as not Fraud call.



Figure 5: Another Input phone Call Messages

Figure 5 shows that the phone call message we have to predict (for this text).



Figure 6: predicted output

Figure 6 shows that the above phone call message is Fraud call.

5. CONCLUSION

The project aimed to develop a fraud detection system for identifying fraudulent phone calls using machine learning techniques, specifically leveraging Natural Language Processing (NLP) and the Multinomial Naive Bayes classifier. The system's effectiveness was demonstrated through a well-defined process encompassing data preprocessing, feature extraction, model training, evaluation, and deployment. The initial phase involved meticulous data preprocessing, which was crucial for transforming raw textual data into a structured format suitable for machine learning models. The text cleaning processes, such as removing special characters, converting text to lowercase, and stemming, ensured that the data was free from noise and inconsistencies. By employing the Bag of Words model, the text data was converted into numerical features, enabling the application of classification algorithms. The Multinomial Naive Bayes classifier was chosen for its proven efficiency in handling text classification problems. This algorithm performed well in categorizing messages as either

fraudulent or normal, demonstrating robust performance metrics, including accuracy, precision, recall, and F1-score. The model's ability to generalize well to unseen data was validated through rigorous testing, which confirmed its reliability in real-world scenarios. The integration of the model into a Flask web application provided a practical solution for end-users, allowing them to interact with the system in real time. The application facilitated easy input of messages and immediate feedback on their status as fraudulent or normal. This user-friendly interface demonstrated the system's practical utility and accessibility.

REFERENCES

- [1] T. Fawcett and F. Provost, "Adaptive Fraud Detection," *Data Mining and Knowledge Discovery*, vol. 1, pp. 291-316, 1997.
- [2] H. Weng et al., "Online E-Commerce Fraud: A Large-Scale Detection and Analysis," 2018 IEEE 34th International Conference on Data Engineering (ICDE), pp. 1435-1440, 2018. [Online] Available: <https://ieeexplore.ieee.org/document/8462781>.
- [3] S. M. Gowri, G. Sharang Ramana, M. Sree Ranjani and T. Tharani, "Detection of Telephony Spam and Scams using Recurrent Neural Network (RNN) Algorithm," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1284-1288, 2021. [Online] Available: <https://ieeexplore.ieee.org/document/9444567>.
- [4] Olusola Adeniyi Abidogun, "Data mining fraud detection and mobile telecommunications: call pattern analysis with unsupervised neural networks," PhD diss. University of the Western Cape, 2005. [Online] Available: <https://etd.uwc.ac.za/handle/11394/1891>.
- [5] S. Sandhya, N. Karthikeyan and R. Sruthi, "Machine learning method for detecting and analysis of fraud phone calls datasets," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 6, March 2020, ISSN 2277-3878. [Online] Available: <http://www.ijrte.org>.
- [6] Mohammad Iquebal Akhter and Mohammad Gulam Ahamad, "Detecting Telecommunication fraud using neural networks through data mining," *International Journal of Scientific & Engineering Research*, vol. 3, no. 3, March 2012. [Online] Available: <http://www.ijser.org>.
- [7] I. Murynets, M. Zabarankin, R. P. Jover and Panagia, "Analysis and detection of SIMbox fraud in mobility networks," *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pp. 1519-1526, 2014. [Online] Available: <https://ieeexplore.ieee.org/document/6845596>.
- [8] M. Crawford, T. M. Khoshgoftaar, J. D. Prusa et al., "Survey of review spam detection using machine learning techniques," *Journal of Big Data*, vol. 2, no. 23, 2015.
- [9] A. Marzuoli, H. Kingravi, D. Dewey and R. Pienta, "Uncovering the Landscape of Fraud and Spam in the Telephony Channel," 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 853-858, 2016. [Online] Available: <https://ieeexplore.ieee.org/document/7882614>.
- [10] B. Teh, M. B. Islam, N. Kumar, M. K. Islam and U. Eaganathan, "Statistical and Spending Behavior based Fraud Detection of Card-based Payment System," 2018 International Conference on Electrical Engineering and Informatics (ICELTICs), pp. 78-83, 2018.
- [11] H. Tu, A. Doupe, Z. Zhao and G.-J. Ahn, "Sok: Everyone hates 'robocalls': A survey of techniques against telephone spam," 2016 IEEE Symposium on Security and Privacy (SP), pp. 320-338, 2016.

- [12] M. Crawford, T. M. Khoshgoftaar, J. D. Prusa, A. N. Richter and H. Al Najada, "Survey of review spam detection using machine learning techniques," *Journal of Big Data*, vol. 2, pp. 1-24, April 2015.
- [13] Sharmila Subudhi and Suvasini Panigrahi, "Quarter-Sphere Support Vector Machine for Fraud Detection in Mobile Telecommunication Networks," *Procedia Computer Science*, vol. 48, pp. 353-359, 2015, ISSN 1877-0509. [Online] Available:
- [14] M. T. Aras and Amaç Güvensan, "Challenges and Key Points for Fraud Detection in Aviation," 2021 International Conference on Innovations in Intelligent Systems and Applications (INISTA), pp. 1-6, 2021.