International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-June-2026, ISSN (Online): 2395-566X

A Machine Learning Approach for Identification and Analysis of Fraudulent Voice Communication Calls

[1]Professor Mayuri Dongre, [2]Saurabh Bhoyar, [3]Sanskar Karnewar
[1]Department of MCA, G H Raisoni College of Engineering and Management, Nagpur, Maharashtra, India.
Email Id: mayuri.k.dongre@gmail.com
[2]Department of MCA, G H Raisoni College of Engineering and Management, Nagpur, Maharashtra, India.
Email Id: saurabhbhoyar420@gmail.com
[3]Department of MCA, G H Raisoni College of Engineering and Management, Nagpur, Maharashtra, India
Email Id: sanskarkarnewar@gmail.com

Abstract — Fraudulent voice calls have become a prominent cyber threat in the contemporary telecommunication environment as the usage of online banking, UPI transactions, mobile wallets, and instant messaging services becomes widespread. The perpetrators of cybercrime resort to fraudulent activities such as voice calls, phishing attacks, OTP manipulation, lottery scams, insurance scams, loan scams, and identity deception. The consequences include substantial monetary damage and grave security vulnerabilities. Existing techniques for spam detection in phone calls depend upon manual reporting, blacklisting, and basic rules-based filtering algorithms. However, these methods prove ineffective against newly emerging and evolving forms of fraud, particularly when the perpetrator changes their phone number and employs advanced social engineering techniques. Therefore, there is a need to develop an efficient and automated fraud detection system. In this paper, we propose a machine learning-based method to detect and analyze fraudulent phone calls. Using the following indicators for call behavior analysis, duration of a call, frequency of calls, suspicious phrases, time of calls, and voice pattern recognition, our approach is intended to identify and classify every call as either fraudulent or legitimate. For better prediction and detection, such machine learning models as Naive Bayes, Logistic Regression, Random Forest, and Support Vector Machine (SVM) will be applied.

Keywords— Fraudulent Voice Calls, Machine Learning, Scam Call Detection, Voice Phishing (Vishing), Random Forest, Support Vector Machine (SVM), Telecommunication Security

I. INTRODUCTION

Voice-based scams have emerged as one of the major problems in the digital age. According to the FTC, robocalls and phone scams amounted to losses totaling over $10 billion in 2023, with people around the world falling victim to deception due to manipulation, urgency tactics, and social engineering techniques. The development of Voice over Internet Protocol technology has made it cheaper and easier than ever before to conduct large-scale telephone scams that can involve ID spoofing and automated calls.

In recent times, there has been an increase in cases of voice call fraud in tandem with the development of digital banking, online payments, mobile banking, and telecommunications. Scammers disguise themselves as bankers, insurance personnel, government officials, customer service staff, or lottery providers to lure unsuspecting victims into divulging private data such as OTP codes, bank information, ATM pin numbers, passwords, and personal identification information. UPI, mobile wallets, and internet banking have facilitated quicker transactions. However, it has also opened avenues for malicious parties to exploit this opportunity for personal gain. Voice phishing attacks, or vishing, have emerged as a common type of cybercrime. Vishing involves cybercriminals using voice and manipulating victims through social engineering techniques to steal access to monetary resources. It is common for the attackers to change their phone numbers, thus rendering blacklisted spam detection futile.

The current methods used in fraud detection include spam numbers reported by users, filters, and complaints. These measures fail to detect new or unidentified scammer phone numbers in real-time and fail to recognize any suspicious behaviors from the caller. There is a need for an intelligent fraud detection system to counter the increasing cases of fraud and cybercrime. The current study addresses the use of machine learning technology in detecting and classifying fraudulent voice calls. The suggested system aims to improve the accuracy of the detection of fraud, minimize financial loss, and ensure user safety through timely alerts. Moreover, the system paves the way for further development of systems and tools aimed at preventing other types of fraud, for example, voice deepfakes.

II. LITERATURE REVIEW

There have been many means introduced by individuals for making communications and conducting financial transactions digitally, which has led to an increase in malicious phone calls made by scammers. There are many scams used by these scammers, including simulation bank calls, OTP scams, insurance frauds, lottery scams, and impersonations. Owing to the shortcomings in the use of the traditional approach to spam detection through blacklists, there have been attempts to implement machine learning and artificial intelligence techniques to detect fraud calls [1] [2].

Several researchers show the effectiveness of machine learning techniques in detecting fraudulent calls since they are able to identify certain behavior and communication patterns of the calling party. Previous research mainly focused on call duration, call frequency, and location of the caller as features for distinguishing between fraudulent calls and legitimate calls [1] .

Researchers also looked into the application of behavioral analysis techniques for the purposes of fraud detection. Behaviors, including frequent calls from unknown numbers, brief missed calls, and strange timings, proved to be some of the key indicators of voice fraud, which provided an improvement over conventional spam number recognition due to their real-time nature [3].

Voice characteristics proved helpful for detecting voice fraud as well. Speaking pace, usage of suspicious words repeatedly, stressed tone, voice modulation, and style of conversation were some of the features that helped classify fraud calls using audio-based spam detection models based on machine learning classifiers including Naive Bayes, SVM, and random forests [3] [4].

Telecommunication-based fraud detection was also explored using deep learning models. Deep neural networks helped find hidden fraud patterns in telecommunication datasets by analyzing complex patterns exhibited by fraudsters. The use of deep learning models improved performance in classifying scam calls [4].

Vishing, which means voice phishing, is one of the most harmful kinds of cybercrime. Research found that scammers manipulate users psychologically during phone calls to steal personal data, such as OTP codes, passwords, and banking information. This shows that voice security needs to include prediction methods based on machine learning algorithms [2].

Additionally, recent studies have looked into deepfake voice fraud. Here, artificial intelligence technology creates realistic voices to carry out scams. It is clear that identifying this issue demands strong anti-fraud solutions because a user may not be able to tell if it is their real voice or not [5].

Security experts have examined attacks on speech recognition systems, where fraudsters used these technologies to give hidden commands. The findings indicated that machine learning algorithms are crucial for building effective voice security systems since they can spot attacks [6] [7].

1. Algorithms and Authors

Table 1: Algorithms and Authors

Sr. No	Algorithm Name	Author Name	Publication Year
1	Naive Bayes Classifier	Thomas Bayes	18th century
2	K-Nearest Neighbors	Evelyn Fix & Joseph Hodges	1951
3	Artificial Neural Networks	Frank Rosenblatt	1958
4	Logistic Regression Model	David Cox	1958
5	Ensemble of Decision Trees	Leo Breiman	2001

III. METHODOLOGY

1. Data Collection

The first part of the methodology involves collecting data on calls in the form of telecommunications data, logs of calls, and patterns of fraud calls reported by users. Some of the parameters collected are call numbers, called numbers, duration of calls, frequency of calls, timing of calls, repeat calls, suspicious words used, and labels on whether the call is legitimate or not.

If more advanced fraud analysis is needed, some voice characteristics, such as speech characteristics, repeat suspicious words, stress levels, and speech characteristics, may also be added. This will enhance the performance of the fraud detection system through combined analysis.

2. Data Preprocessing

Raw call data usually have missing values, duplicate data, and irrelevant information, which may affect the accuracy of machine learning algorithms. Thus, data preprocessing is

carried out before training the model. It entails deleting null values, duplicates, inconsistent data, and changing categorical data to numeric data by label encoding.

Normalization and standardization may be required in some cases to enhance the efficiency of machine learning algorithms. After preprocessing, the dataset is split into training and test sets.

3. Feature Extraction
The feature extraction process is important in fraudulent call detection since the effectiveness of the model is determined by the quality of selected input variables. Some of the key features utilized in this study include the number of daily calls, the length of calls, repetition of suspicious keywords, abnormal call timing, the prevalence of unknown numbers, calling behaviour history, and fraud history

In addition to the numerical features, some voice communication features are also employed in this study including speech rate, voice stress, word repetition, and suspicious speech pattern.

4. Machine Learning Model Training
The machine learning models are developed based on extracted input features to classify calls into two categories (fraudulent vs. genuine). The machine learning algorithms employed in this study include Naive Bayes, Logistic Regression, Random Forest, and SVM.

All models are tested on the prepared dataset. Random Forest and SVM models have an advantage over other algorithms due to the ability to manage multiple features related to fraud activities.

5. Model Evaluation
The performance of the machine learning models is measured by certain standard criteria to evaluate the accuracy and reliability of their predictions. The major evaluation parameters used in our research are Accuracy, Precision, Recall, F1-Score, and Confusion Matrix.

These parameters allow comparing the effectiveness of the developed algorithms and detecting which one shows the best results in terms of fraud prediction. According to our experimental investigation, the whole system should reach accuracy rates ranging from 90% to 95%. As for the best-performing algorithm, it would be the Random Forest.

6. Fraud Detection and Alert Generation
When choosing the algorithm that demonstrates the best performance, the system determines whether an incoming call is either fraudulent or safe for the user. In case any suspicious activities are identified, an alert will be generated to warn the user about a potential scam.

In such a way, people will be protected from being victims of such kinds of financial scams as OTP schemes, fake banks, loan scams, lottery, and impersonation scams.

IV.. SYSTEM IMPLEMENTATION

System implementation for the identification and analysis of fraudulent voice communication calls is based on machine learning algorithms that categorize the incoming calls either as fraudulent or normal. The process of system implementation involves various activities such as data set preparation, machine learning algorithm building, database management, user interface designing, and finally fraud prediction.

1. Data Set Preparation
The first activity that needs to be done for system implementation is the creation of the data set. This data set comprises of all the details related to the calls such as caller number, receiver number, duration of call, frequency of call, timing of call, suspicious words, caller behaviours, etc. This data is stored in the format of .CSV file.

This data is pre-processed through removal of duplicates, handling of missing data, and conversion of categorical data into numeric form.

2. Model Development
Machine learning models are developed using Python and the Scikit-learn library. Algorithms such as Naive Bayes, Logistic Regression, Random Forest, and Support Vector Machine (SVM) are trained using the prepared dataset.

Feature extraction is performed to identify important fraud indicators such as repeated scam keywords, abnormal calling frequency, short call duration, and unknown caller behavior. The trained model predicts whether a call is fraudulent or genuine based on these features.

Among all models, Random Forest is selected as the best-performing model because it provides the highest accuracy and better handling of multiple fraud-related features.

3. Database Management
SQLite database is used to store call history, fraud labels, suspicious caller records, user login details, and prediction results. The database helps maintain historical fraud records for future analysis and improves system reliability.

The database also stores user feedback and manually reported scam calls, which can be used for updating the training dataset and improving model performance over time.

4. User Interface Development
A user-friendly interface is developed using Flask technology on both frontend and backend. The interface will allow login facility, inputs for fraud predictions, call analysis results, and alerts regarding the fraud cases.

The users will be allowed to either fill the details of the calls manually or import the call data in order to make predictions about the call being a fraudulent one or not. The interface will show whether the call is a fraud one or a legitimate one, the probability percentage, and fraud alerts.

5. Fraud Prediction Process
As soon as a call is made, the system will capture its details and send them to the machine learning model for predicting whether it is a fraud one or not. If any suspicious behavior is detected, the system marks that call as fraudulent and triggers a fraud alert for the user. In case no suspicious activities are identified, then the call is considered legitimate. This process allows real-time detection of fraud cases such as OTP frauds, bank phishing calls, loan frauds, and lottery scams.

6. Performance Evaluation
The developed system is assessed by means of accuracy, precision, recall, f-score, and confusion matrix measures. The system produced an approximate overall accuracy of about 93%, where Random Forest produced the best outcomes.

In conclusion, it can be noted that the implementation of the proposed system proved machine learning to be a viable approach to identifying fraudulent voice communication calls and preventing cyber fraud.

V. RESULT AND ANALYSIS

For evaluating the effectiveness of the proposed machine learning system in the identification and classification of the fraudulent voice communication calls, call attributes like the call duration, call frequency, caller information, usage of suspicious keywords, time of call, and the history of frauds were taken into account. Preprocessing included the removal of redundant or duplicate values and extraction of significant features in order to achieve an accurate classification of calls.

Different types of classifiers including Naïve Bayes, Logistic Regression, Random Forest Classifier, and Support Vector Machine (SVM) were employed in the experiment to identify fraud. Their accuracy was evaluated through Accuracy, Precision, Recall, F1-score, and Confusion matrix criteria.

From the result of the experiment, it can be seen that Random Forest classifier gave the best predictive performance. Multiple features related to fraud could be efficiently classified using the model without issues of overfitting. The SVM method also proved effective with high precision and recall rates. However, Logistic regression provided quicker prediction with slightly decreased accuracy in the case of complicated fraud patterns. Naïve Bayes gave better results in simpler situations.

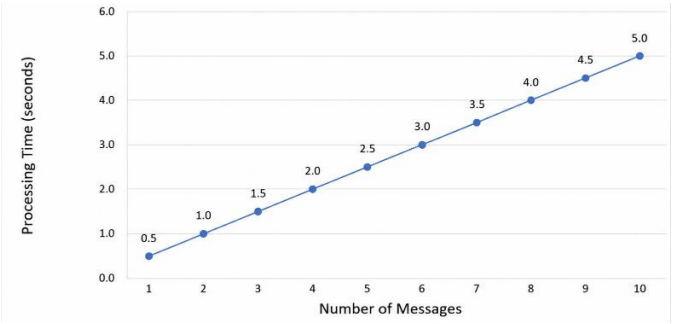

Fig 1 : Line Graph (Message Count vs Processing Time Graph)

From this diagram, we can see that as the input messages increase, there is an increase in processing time in a linear manner. This indicates that the system works effectively and can process several messages effectively.

VI. CONCLUSION

The proposed work discusses an intelligent system for detecting and analyzing fraudulent calls using machine learning techniques. Call parameters such as duration, frequency, presence of suspicious words, and behavioral characteristics are considered as input features to classify the calls into fraudulent or genuine categories. Various machine learning classifiers, including Naïve Bayes, Logistic Regression, Random Forest, and SVM, were tested. Among them, the performance of the Random Forest classifier was outstanding at around 93%.

REFERENCES

1. S. N. A. T. T. S. L. P. N. D. K. K. V. J. Ratnakumari, "Detection of Fraudulent or Deceptive Phone Calls Using Artificial Intelligence," in Turkish Journal of Computer and Mathematics Education (TURCOMAT), Turkey, 2024.
2. A. T. e. al., "Vishing: Detecting Social Engineering in Spoken Communication—A First Survey and Urgent Roadmap to Address an Emerging Societal Challenge," in Computer Speech & Language, Netherlands, 2025.
3. R. T. Q. S. C. X. L. Z. Yan, "Telesonar: Robocall Alarm System by Detecting Echo Channel and Breath Timing," in ACM Conference on Embedded Networked Sensor Systems (SenSys), Boston, USA, 2023.
4. D. E. B. M. Elizalde, "Audio-Based SPAM Call Detection," in The Journal of the Acoustical Society of America, USA, 2021.
5. K. P. J. W. N. M. Müller, "Human Perception of Audio Deepfakes," in arXiv Preprint, USA, 2021.
6. H. A. e. al., "Practical Hidden Voice Attacks Against Speech and Speaker Recognition Systems," in arXiv Preprint, USA, 2019.
7. N. D. H. e. al., "Adversarial Attacks on Speech Recognition Systems for Mission-Critical Applications: A Survey," in arXiv Preprint, USA, 2022.