DETECTION OF FRAUDULENT OR DECEPTIVE PHONE CALLS USING ARTIFICIAL INTELLIGENCE

Mrs J. RATNAKUMARI[1] SHAIK NAILO ASMIN THAHENATH[2] TOLUSURI SRI LAKSHMI[3] PERAVALI NAGA DILEEP KUMAR[4] KADIYAM VEERAIAH[5]

[1]Department of CSE & AI, Chalapathi Institute of Engineering and Technology, LAM, Guntur, Andhra Pradesh, India.
[2]Department of CSE & AI, Chalapathi Institute of Engineering and Technology, LAM, Guntur, Andhra Pradesh, India.
[3]Department of CSE & AI, Chalapathi Institute of Engineering and Technology, LAM, Guntur, Andhra Pradesh, India.
[4]Department of CSE & AI, Chalapathi Institute of Engineering and Technology, LAM, Guntur, Andhra Pradesh, India.
[5]Department of CSE & AI, Chalapathi Institute of Engineering and Technology, LAM, Guntur, Andhra Pradesh, India

ABSTRACT: With an increase advancement of technology, fraud phone calls, including spam's and malicious calls have become a major concern in telecommunication industry and causes millions of global financial losses every year. Fraudulent phone calls or scams and spams via telephone or mobile phone have become a common threat to individuals and organizations. Artificial Intelligence (AI) and Machine Learning (ML) has emerged as powerful tools in detecting and analyzing fraud or malicious calls. This project presents an overview of AI-based fraud or spam detection and analysis techniques, along with its challenges and potential solutions. The novel fraud call detection approach is proposed that achieved high accuracy and precision. The Proposed approach was evaluated using a dataset of real-world fraudulent calls. And results demonstrate that the approach achieved high accuracy in detecting malicious calls and identifying potential indicators of frauds or spam's. The analysis of fraud calls also provided insights into the tactics and methods employed by fraudsters, which can be used to develop countermeasures.

KEYWORDS: Malicious, Artificial Intelligence, Fraudulent, Machine learning

1. INTRODUCTION

An ever-evolving danger that affects people, businesses, and the government is phone-based spam or scams [7]. The Federal Trade Commission (FTC) in the United States got over 3 million reports of fraud in 2021, resulting in a $3billion-dollar loss overall. Spammers use a variety of ploys, including impersonation, spoofing, and digital manipulation, to access private information, steal money, orharm a person's image. Around the globe, it resulted in financial and information losses. Inherently, fraud phone calls are designed to cause stress and anxiety. The traditional methods [14] of detecting malicious phone calls involve manual review of call details and recordings and identifying fraudulent patterns. However, these methods are time-consuming, expensive, and may not give accurate results or effective in identifying new types of scams. Therefore, there is a need for a good technique that can detect and analyse fraud phone calls accurately and efficiently.

2. LITERATURE SURVEY

Artificial intelligence techniques such as machine learning, deep learning, neural language processing have been applied to detect and analyse fraud phone calls. These techniques can provide accurate results for already existing models and systems. The authors [3] introduces a solution based on machine learning for telecommunication without making any harm to telephone network infrastructure. The experiment was stimulated by mat plot lib. The findings show that the method proposed is 87% accurate. The paper [5] introduces a mining-based phone call recognition framework. The experiment show that the technique can achieve the high reputation precision regarding 97.6% [5] which exhibits that the proposed methods has a brilliant execution with best draws. The research proposed the solution of detecting fraud phone calls by using historical data to pre process the data [6]. And as a result, artificial neural network is better method for detecting telephone frauds due to speed and accuracy.

3. SYSTEM ANALYSIS

3.1EXISTING SYSTEM

The existing system for "Detection and Analysis of Fraud Phone Calls using Artificial Intelligence" primarily relies on traditional methods and rule-based systems, often struggling to keep pace with evolving fraud tactics. Conventional call filtering techniques exhibit limitations in accurately distinguishing between legitimate and fraudulent calls. The absence of advanced machine learning models hinders the system's ability to adapt to dynamic fraud patterns. Additionally, the lack of comprehensive analysis tools results in a limited understanding of fraudsters' evolving strategies. This underscores the need for a more sophisticated approach, prompting the integration of Artificial Intelligence and Machine Learning to enhance fraud detection accuracy and provide valuable insights into the techniques employed by malicious actors.

LIMITATIONS OF EXISTING SYSTEM

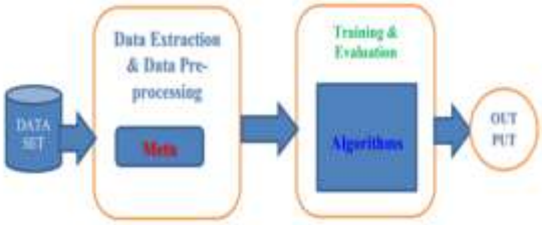
Rule-Based Approach Limitation: The existing system relies on rule-based approaches, making it less adaptive to emerging and sophisticated fraud techniques that often evolve beyond predefined rules.

False Positive Challenges: The current system may generate false positives, inaccurately flagging legitimate calls as fraudulent. This can lead to user frustration and decreased trust in the effectiveness of the fraud detection system.

3.2 PROPOSED SYSTEM

The proposed system for "Detection and Analysis of Fraud Phone Calls using Artificial Intelligence" represents a paradigm shift, leveraging advanced machine learning algorithms for dynamic adaptation to evolving fraud tactics. By integrating cutting-edge anomaly detection techniques, the system aims to overcome the limitations of rule-based approaches, enhancing accuracy and significantly reducing false positives. This solution incorporates a comprehensive learning model, continuously evolving through real-time data analysis to identify emerging patterns of fraudulent behavior. Implementation of deep learning algorithms allows for a nuanced analysis of complex fraud patterns, providing a more robust and efficient detection mechanism. Additionally, the proposed system prioritizes user feedback and employs a feedback loop mechanism to further refine its accuracy and reduce false alarms. Scalability is a core focus, ensuring the system's effectiveness in handling the escalating volume of calls while maintaining real-time responsiveness. Overall, the proposed system aims to establish a state-of-the-art framework, offering heightened accuracy, adaptability, and insights into evolving fraud strategies in the realm of phone calls.

4. SYSTEM ARCHITECTURE



The architecture relies on a comprehensive dataset and metadata for analysis. 2. Machine learning algorithms are deployed to detect patterns in the data. 3. The output provides real-time insights into the authenticity of phone calls.

i. First remove duplicate data and missing values from the set.
Transform categorical features such as call type, caller ID into numerical features. Using label encoding.
ii. Normalization of the numerical features, such as call duration, frequency, is done by using z-score normalization.
iii. Selection of suitable artificial intelligence-based model such as navy bayes, support vector machine (SVM), decision tree etc. Implement the model and train the preprocessed data. Here, navy bayes is selected for training and testing of the dataset.

5. MODULES

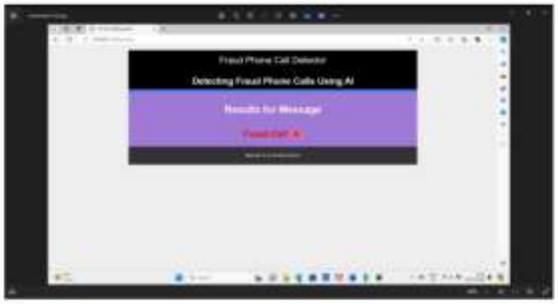
Data collection: The dataset of phone call recordings, along with metadata such as call duration, location, phone numbers, etc. is collected from real world source like. Dataset is taken from real world sources such as Kaggle. The dataset contains 1000 genuine and fraudulent calls and the following features such as State, area code, a phone number, date and time, IP address, code, etc. this dataset is divided into two parts training set and testing set.

Data Pre-processing: Data cleaning and pre-processing is used for dataset to remove noise, distortions, and irrelevant information.

Model Evaluation: Selection of suitable artificial intelligence-based model such as support vector machine (SVM), decision tree, Naive Bayes etc. Implement the model and train the pre processed data. Here, support vector machine and recurrent neural network is selected for training and testing of the dataset.

User Interface (UI) Development: Constructs an intuitive and interactive user interface (UI) for CADM, facilitating user interaction and visualization of results generated algorithms.

6. RESULT



Fraud Phone Call Detector

Detecting Fraud Phone Calls Using AI

Results for Message

Fraud Call! ⚠

[illegible]

7. CONCLUSION

Fraudulent phone calls are a growing concern that affects individuals as well as organizations worldwide. The main purpose of this paper is to detect and analyze fraud phone calls using artificial intelligence. For achieving this goal, support vector machine (SVM), navy bayes and etc algorithms are used. The approach achieved a high accuracy and precision. Hence, it will be a good solution to detect and analyze fraud or malicious calls.
Future scope: For achieving this goal, recurrent neural algorithm (RNN) algorithm is used. To achieved a high accuracy and precision. Hence, it will be a good solution to detect and analyze fraud or malicious calls.

REFERENCES

[1] P. Sornsuwit,and S. Jaiyen, “A new hybrid machine learning for cybersecurity threat detection based on adaptive boosting,”Applied Artificial Intelligence, 33(5), pp.462-482, 2019.
[2] K.Shaukat, S. Luo, S.Chen, and D. Liu, “Cyber threat detection using machine learning techniques: A performance evaluation perspective,”inIEEE international conference on cyber warfare and security. IEEE, October2020,pp. 1-6.

[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), Coimbatore, India, 2021, pp. 1284-1288, doi: 10.1109/ICACCS51430.2021.9441982.

[4] Abidogun, Olusola Adeniyi. "Data mining, fraud detection and mobile telecommunications: call pattern analysis with unsupervised neural networks." PhD diss., University of the Western Cape, 2005.

[5] S. Sandhya, N. Karthikeyan, R. Sruthi “Machine learning method for detecting and analysis of fraud phone calls datasets” International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

[6] Mohammad Iquebal Akhter, Dr. Mohammad Gulam Ahamad “Detecting Telecommunication fraud using neural networks through data mining” international Journal of Scientific & Engineering Research, Volume 3, Issue 3, March-2012.

[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,Toronto,ON,Canada,2014,pp.1519-1526,doi: 10.1109/INFOCOM.2014.6848087.

[8] Crawford, M., Khoshgoftaar, T.M., Prusa,J.D. et al. Survey of review spam detection using machine learning techniques. Journal of Big Data 2, 23 (2015). doi:10.1186/s40537-015-0029- 9.

[9] Marzuoli A, Kingravi H, Dewey D and Pienta R. (2016). Uncovering the Landscape of Fraud and Spam in the Telephony Channel 2016 15th IEEE International Conference on Machine Learning and Applications(ICMLA). 10.1109/ICMLA.2016.0 153. 978-1-5090-6167-9. (853- 858).

[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 SSConference on Electrical Engineering and Informatics (ICELTICs), Banda Aceh, Indonesia, 2018, pp. 78-83, doi:10.1109/ICELTICS.2018.8548878.

[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, H. Al Najada, "Survey of review spam detection using machine learning techniques", Journal of Big Data, 2, pp. 1-24, 42015.