IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Artificial Intelligence-Based Fraud Phone Call Identification and Analysis

1. Karri Jaya Sri 2 L. Dasarada Ramiah , 3. V. Anil Santhosh

1. MTech Scholar and student of C.S.E, International School of Technology and Sciences for Women (Autonomous), East Gonagudem, Rajanagaram–Andhra Pradesh,

2. Assistant Professor of C.S.E., International School of Technology and Sciences for Women (Autonomous), East Gonagudem, Rajanagaram–Andhra Pradesh.

3. Professor and HOD of C.S.E., International School of Technology and Sciences for Women(Autonomous), East Gonagudem, Rajanagaram–Andhra Pradesh.

Abstract:

As generation advances, fraudulent phone calls which includes spam and dangerous calls have grown to be a huge difficulty within the telecom zone, resulting in thousands and thousands of bucks in losses annually on an international scale. humans and organizations are more and more at hazard from fraudulent phone calls, frauds, and spam thru cellular devices. machine mastering (ML) and artificial intelligence (AI) have become effective techniques for figuring out and evaluating harmful or fraudulent calls. a top-level view of AI-based techniques for unsolicited mail or fraud detection and evaluation is provided on this have a look at, along with a discussion of the troubles and possible fixes. excessive accuracy and precision are attained by means of the precise fraud call detection method that is cautioned. A dataset of real fraudulent calls was used to evaluate the cautioned approach. And consequences display that the technique executed excessive accuracy in detecting malicious calls and identifying capacity signs of frauds or spams. The analysis of fraud calls also provided insights into the tactics and strategies hired via fraudsters, which can be used to increase countermeasures.

Key words: Artificial Intelligence, Fraud Phone Call Identification, Analysis

I. Introduction

An ever-evolving risk that impacts people, agencies, and the government is smartphone-based spam or scams [7]. The Federal trade commission (FTC) in the u.s.a. were given over 3 million reports of fraud in 2021, ensuing in a $3 billion-greenback loss normal. Spammers use an expansion of ploys, which includes impersonation, spoofing, and virtual manipulation, to get right of entry to private statistics, scouse borrow money, or harm someone's photo. around the globe, it ended in economic and facts losses. Inherently, fraud smartphone calls are designed to reason stress and anxiety. The traditional techniques [14] of detecting malicious phone calls involve guide evaluation of name information and recordings and figuring out fraudulent patterns. however, those strategies are time- consuming, highly-priced, and might not provide correct results or effective in identifying new forms of scams. therefore, there's a want for a terrific approach that can discover and analyse fraud smartphone calls as it should be and efficiently.

II. LITERATURE SURVEY

Detection of Telephony unsolicited mail and scams the usage of Recurrent Neural network (RNN) set of rules, or decades, malicious telephone calls, which includes spam and scams, were a challenging difficulty that led to millions of monetary losses yearly international. This paper presents a device getting to know-based totally telecommunications solution that doesn't depend upon the phone network infrastructure. the main challenge of this ten-12 months-antique difficulty is developing powerful functionalities without getting access to the infrastructures of smartphone networks. First, the previous unsolicited mail call information set is accrued. To anticipate malicious calling, the dataset contains some of label-based totally functions. Our primary recognition is on detecting malicious calls the usage of the Recurrent Neural network (RNN) technique. We study diverse device-learning strategies the use of the suggested capabilities, and its miles concluded that the exceptional approach can lessen fraudulent calls to 90% whilst retaining over ninety% binary name accuracy. The effects also display that, with the useful resource of an evaluation study, the models may be applied correctly without a massive overhead latency.

Statistics mining, fraud detection and cellular telecommunications: call pattern analysis with unsupervised neural networks. due to the growing use of mobile phones, big amounts of records are being captured. Operators can get a aggressive facet in advertising, fraud detection, and customer service and retention by means of using the statistics and information gleaned from these databases. One approach of detecting fraud is searching out symptoms of suspicious changes in user conduct. the call information that defines utilization styles reflects the intentions of cellular telephone users, even though it is not possible to display their intentions. A single smartphone creates a sizeable utilization pattern over the years. despite the fact that subscriber call facts are logged for billing functions, we do now not anticipate that the data is suggestive of fraudulent call styles; this is, the calls made for billing purposes are unlabelled. consequently, greater research is wanted so as to distinguish fraudulent use. To make the method of detecting fraud less difficult, an unsupervised learning system may also examine and group name patterns for every subscriber. as a way to profile consumer calls over time in a cellular communications network, this examine examines the unsupervised mastering skills of neural networks. Our studies compare and applies the algorithms of lengthy quick-time period reminiscence (LSTM) recurrent neural networks and Self-Organizing Maps (SOM) on person call records statistics as a way to carry out a descriptive fact mining on user's name patterns. Our investigation indicates the mastering potential of both strategies to discriminate user name patterns.

The LSTM recurrent neural network set of rules providing a better discrimination than the SOM set of rules in phrases of long-term collection modelling. LSTM discriminates exclusive varieties of temporal sequences and corporations them in line with a diffusion of features. The ordered functions can later be interpreted and classified in step with unique necessities of the mobile provider. for that reason, suspicious call behaviours are isolated in the cell telecommunication network and may be used to become aware of fraudulent name patterns. We deliver consequences the usage of masked call statistics from a real cellular telecommunication network.

Evaluation and detection of SIM box fraud in mobility networks, A well-known illegal practice on cellular networks is voice site visitors' termination fraud, frequently called Subscriber identity Module box (SIMbox) fraud. global mobile operators therefore lose billions of bucks according to yr. furthermore, by using overwhelming the nearby base stations that serve those gadgets, SIMboxes jeopardize the infrastructure of the mobile network. The fraudulent site visitors from SIMboxes that use a variety of SIM playing cards is examined in this article. one of the important cell operators inside the US sends it loads of hundreds of thousands of anonymised voice name detail data (CDRs). Fraudulent SIMboxes are known to provide an abnormally excessive volume of outgoing calls, overload voice transmission, and feature unchanging physical locations. Novel classifiers for the detection of counterfeit SIM bins in mobility networks are suggested in mild of those findings. to boost the detection fee, their outputs are properly merged. The set of rules' capacity to pick out new counterfeit SIMboxes was established by the operator's fraud branch.

III. SYSTEM ANALYSIS

due to its reliance on conventional techniques and rule-based totally systems, the modern-day "Detection and analysis of Fraud smartphone Calls using synthetic Intelligence" device frequently finds it difficult to hold up with changing fraud strategies. The accuracy of traditional call filtering structures in differentiating between fraudulent and legitimate calls is confined. The device's lack of ability to adjust to changing fraud patterns is because of the lack of sophisticated gadget mastering models. moreover, a constrained comprehension of the changing strategies used by fraudsters is the result of the absence of thorough evaluation tools. This emphasizes that a extra advanced method is required, that's why artificial intelligence and device gaining knowledge of are being incorporated to improve the accuracy of fraud detection and provide insightful statistics about the tactics utilized by awful actors.

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.

Limited Learning Capability:
Conventional systems lack the ability to learn and adapt over time. They do not leverage the full potential of machine learning algorithms to dynamically identify new patterns of fraudulent behaviour.

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.

Inability to Analyse Complex Patterns:
The system may struggle to analyse complex fraud patterns, especially those involving subtle variations or combinations of tactics, limiting its effectiveness in detecting nuanced fraudulent activities.

Scalability Issues:
As fraud attempts increase in sophistication and volume, the existing system may face scalability challenges, affecting its ability to handle a growing number of transactions and calls in real-time.

B. Methodology

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 behaviour. The 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.

IV.SYSTEM DESIGN

SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

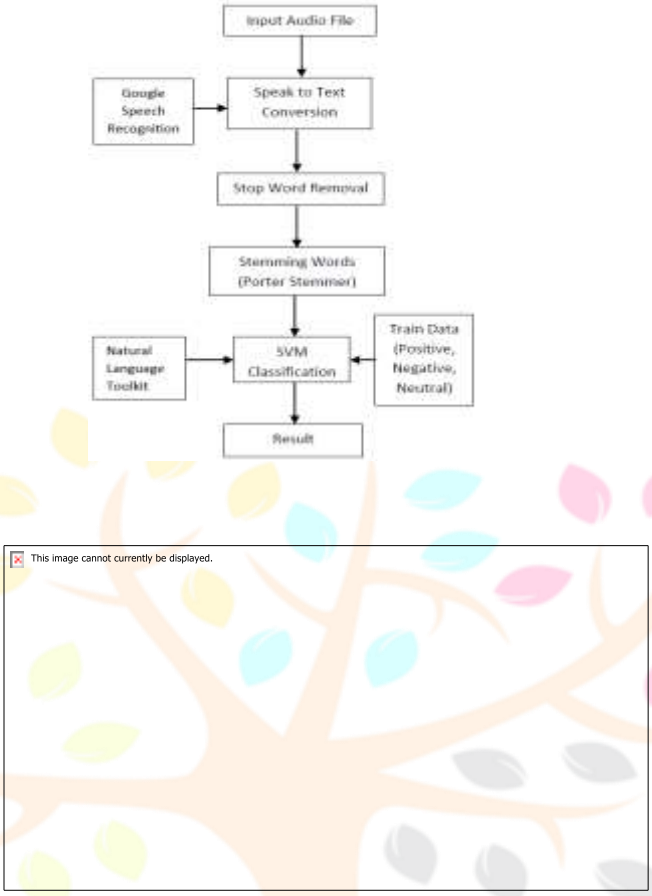


Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

MODULES

Data Preprocessing Module:

This module is responsible for cleaning and preparing the incoming call data. It involves tasks such as noise reduction, data normalization, and handling missing or inconsistent information to ensure the data is suitable for analysis.

Fraud Detection Module:

The core of the system, this module utilizes advanced machine learning algorithms and anomaly detection techniques to identify patterns indicative of fraudulent phone calls. It constantly learns from new data to adapt and improve its detection capabilities over time.

Analysis and Insights Module:

This module performs in-depth analysis on detected fraudulent calls, extracting valuable insights into the tactics and methods employed by fraudsters. It provides a detailed understanding of evolving fraud patterns, aiding in the development of effective countermeasures.

User Feedback Integration Module:

Focused on user interaction, this module incorporates a feedback loop mechanism. It collects and analyzes user feedback on flagged calls, refining the system's performance based on real-world usage and user experiences to reduce false alarms.

Scalability and Real-Time Processing Module:
Ensuring the system's efficiency in handling a large volume of calls, this module addresses scalability concerns. It is designed to facilitate real-time processing, allowing the system to maintain responsiveness even in dynamic telecommunication environments with a high influx of calls.

VI . RESULTS AND DISCUSSION

T
he proposed approach was evaluated on a dataset of 1000 genuine and fraudulent calls. the approach achieved a high accuracy of 95% and precision of 97%, outperforming the existing approaches. Hence, the approach was able to detect fraudulent phone calls brilliantly

Fig 2. User Result based on proposed model

Fig 3. Comparison Graph

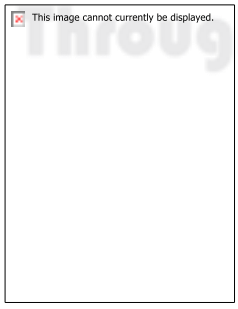
VI I. CONCLUSION AND FUTURE WORK

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 analyse fraud phone calls using artificial intelligence. For achieving this goal, support vector machine (SVM) and recurrent neural algorithm (RNN) is used. SVM is used to train the dataset [13], whereas RNN is used to test the train dataset. The approach achieved a high accuracy and precision. Hence, it will be a good solution to detect and analyse fraud or malicious calls.

REFERENCES :

[1] Fawcett, T., Provost, F. Adaptive Fraud Detection. Data Mining and Knowledge Discovery 1, 291–316 (1997).doi:10.1023/A:1009700419189
[2] H. Weng et al., "Online E-Commerce Fraud: A Large-Scale Detection and Analysis," 2018 IEEE 34th International Conference on Data Engineering (ICDE), Paris, France, 2018, pp. 1435-1440, doi: 10.1109/ICDE.2018.00162.
[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 Conference 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.

Biography of authors:



Karri. Jaya Sri was a M.Tech Scholar and student of student of C.S.E., International School of Technology and Sciences for Women(Autonomous), East Gonagudem, Rajanagaram–Andhra Pradesh. **Jaya Sri** is a dedicated research scholar specializing in Data Since , Python and Machine Learning (ML), focusing on innovative approaches to solve complex real-world problems. With a strong academic foundation and a passion for computational technologies.

L. Dasarada Ramiah (M.Tech) was an Associate Professor of C.S.E., International School of Technology and Sciences for Women(Autonomous), East Gonagudem, Rajanagaram–Andhra Pradesh. **Dasarada Ramiah (MTech)** is a dedicated research scholar specializing in Artificial Intelligence (AI) and Machine Learning (ML), focusing on innovative approaches to solve complex real-world problems. Their research interests include developing advanced algorithms for predictive modelling, integrating hybrid ML-DL frameworks, and exploring the ethical and societal impacts of AI systems.

V. Anil Santhosh was an Assistant Professor and HOD of C.S.E., International School of Technology and Sciences for Women(Autonomous), East Gonagudem, Rajanagaram–Andhra Pradesh. Anil Santhosh is a dedicated research scholar specializing in Artificial Intelligence (AI) and Machine Learning (ML), focusing on innovative approaches to solve complex real-world problems. Their research interests include developing advanced algorithms for predictive modelling, integrating hybrid ML-DL frameworks, and exploring the ethical and societal impacts of AI systems. Their work primarily focuses on applications in renewable energy forecasting, natural language processing, and computer vision.