“Artificial intelligence based Intelligent System for Telephonic Security, Threat Identification and Alert System”

Gunashree S , Dr B Sivakumar , Mahalakshmi G, RenuPrasad K N

student of UG, Department of ETE, Dr Ambedkar Institute of Technology, Bengaluru, Karnataka

Professor and Dean, Dr Ambedkar Institute of Technology, Bengaluru, Karnataka

student of UG, Department of ETE, Dr Ambedkar Institute of Technology, Bengaluru, Karnataka

Student of UG, Department of ETE, Dr Ambedkar Institute of Technology, Bengaluru, Karnataka

ABSTRACT:

Spam is an unwanted calls or SMS sent on mobile whose content may be malicious. Scammers send fake text messages or call to the user to trick people into responding to their SMS or calls. They may hack personal information, password, account number, etc. To avoid being tricked by scammers, proposed a model based on Machine Learning Algorithms. Detection of such calls is difficult as scammers evade detection through tactics such as changing numbers they call from, modifying the call script, etc. The increase of spam calls in recent years has become a major annoyance for both consumers and businesses, resulting in lost time, lower productivity, and possible privacy concerns While some smartphone applications such as true caller can detect such calls or text based on caller ID, call origination, etc., such techniques cannot easily adapt to new scams. They can detect the spam only when the phone number is registered as scam by national cybercrime. This disclosure describes the use of an AI model to detect suspicious calls. The AI model is trained on a dataset of spam/scam calls and other calls to detect spam/scam calls. With user permission, when the user receives a call from an unknown number, call content is a transcribed into text and analyzed in real time to determine if the call is likely suspicious. When such a call is detected, alerts are provided to the user by sending SMS through GSM to ensure that the user does not share sensitive information. As our project says, there are different threats or spams in real world scenario, AI model will completely analyze the call and categorize it into different form and alert the user which type of fraud it is whether it is a phishing, emotional manipulation, banking fraud, lottery scams, etc. As there were multiple threats, AI model will be trained based on the detected frauds.

Key words: Artificial intelligence (AI), Scams, Algorithm, SMS

1. INTRODUCTION:

With the rapid advancement of communication technologies, telephone networks have become a prime medium for both

legitimate and malicious interactions. Traditional systems often struggle to detect and mitigate telephonic threats such as fraud calls, phishing attempts, bomb threats, or extortion calls in real-time. To address this critical gap, the development of AI-based telephonic security threat identification and alert systems has emerged as a trains formative solution. This system leverages artificial intelligence, machine learning (ML) algorithms to analyze incoming and outgoing calls. It can detect suspicious keywords, tone of voice, conversation patterns, and caller behaviour indicative of security threats. Upon identifying a potential threat, the system automatically triggers real-time alerts to relevant authorities or internal security teams, ensuring a swift and informed response. By continuously learning from new data and adapting to evolving threat patterns, this AI-based system significantly enhances telecommunication security, supports law enforcement efforts, and helps protect individuals and organizations from various forms of telephonic attacks.

1.1 Problem statement: There are different Spam Calls which are emerging today such as telemarketing scams, banking Frauds, Charity Scams, Lottery scams etc. Through these calls the user may share their bank details or personal details hence, the user will be trapped in spams. In order to identify the spam calls and also to categorize the calls we are implementing the AI based project called Artificial Intelligence based telephonic security treat identification and alert system.

1.2 Significance: Enhanced security: The system can detect and alert potential security threats, enabling swift action to prevent or mitigate harm. Proactive approach: AI-powered threat detection allows for proactive measures, reducing the risk of security breaches and protecting individuals and organizations. Improved response times: Automated alert systems enable rapid response to potential threats, minimizing the impact of security incidents.

1.3 Impact: Law enforcement and national security: The system can aid in detecting and preventing crimes, such as terrorism, human trafficking, or organized crime, ultimately contributing to public safety. Corporate security: Businesses can benefit from enhanced protection against security threats, such as espionage, sabotage, or insider threats, safeguarding their assets and reputation. Government agencies: The system can support government agencies in detecting and preventing security threats to national security or public safety. Individuals and communities: By detecting and preventing security threats, the system can contribute to a safer environment for individuals and communities.

2. Literature Survey:

1. Cyber-Analytics: an examination of machine learning algorithms for spam filtering, Taiwo Ajanind Tammy Ferrante(2024)

   This paper will signify how python programing and its libraries will support to filter the spam calls

2. Artificial intelligence based fake or fraud call detection, Durga Bhavani (2024)

   This paper will emphasize the importance of preprocessing of data. This include removing of null values that could adversely effect the model performance. It will ensure that model can interpret and process the data effectively.

3. Spam call protection using machine learning ,Akash S(2024)

   This paper will Emphasize has to classify various scams and how to identify the calls which has never seen before that exhibit completely new behaviour.

4. Suspicious call Detection and Mitigation Using Conversational AI Kolati Mallikarjuna Rao and Bavvi Kumar Patil,(2023)

   The use of conversational AI to detect spam can reduce the number of spam calls. The conversational AI agent can be trained to adapt to new strategies employed by spam callers.The conversation of user is extracted into the raw text which has converted by whisper and it is given as input for AI model.

5. Spammer Detection and Fake User identification on Social Networks Faiza Masood, Ghana Ammad, Hasan Ali Khattak, Mohsen Guizani, (2019)

   This paper will emphasize how to detect the spam contents what are the keywords that can be given as data to the AI model.

3. Implementation:

This is a block diagram which explains how the data is processed from initial stage that is converting audio to text file to the final stage that is categorizing the threats, measure the risk and spam ratings and sending a alert SMS to user Phone.

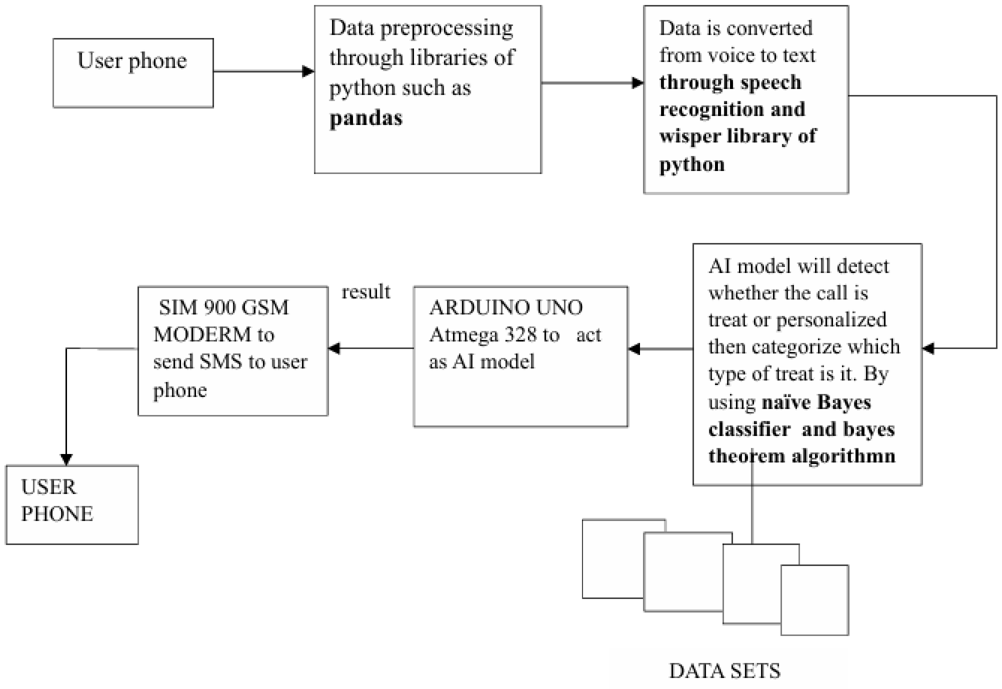

User phone
Data preprocessing through libraries of python such as **pandas**
Data is converted from voice to text **through speech recognition and wisper library of python**
AI model will detect whether the call is treat or personalized then categorize which type of treat is it. By using **naïve Bayes classifier and bayes theorem algorithmn**
ARDUINO UNO Atmega 328 to act as AI model
result
SIM 900 GSM MODERM to send SMS to user phone
USER PHONE
DATA SETS

Fig 3.1 Block diagram of Artificial intelligence based telephonic security, threat identification and alert system

In this paper we are using user system as mobile where we can receive the call from another person. The person will receive a call it can be a fraud call or the personalized call on their phones. The program call analysis will be monitoring the call, if any of the recorded call is pushed to the drive it will extract the data and convert it into the wave format by using the libraries Librosa, Speech recognition. The data in wave format will be compressed and clean. We can extract a raw data from original data. The waveform will be in analog form. We use sampling technique to convert analog signal to digital signal with sampling frequency of 16000Hz and 6 PCM, because the computer or AI model will analyze the data only in the binary format. Conversion to text format: The program call processing will extract the data from waveform and transcribe it into the text format by using wave library. It is used for reading the audio files in waveform and transcribing into text.

3.1 Training the AI model:

The data sets will be given to AI model in the CSV files. To load those datasets to the AI model we use Pandas library.

We use Term frequency and inverse document frequency (TF -IDF) algorithm in order to categorize the threats.

The term frequency will measure how often the word appeared in the data given. Then the inverse document frequency will measure how important a word across the entire collections of data sets. We will import this algorithm as TfidfVectorizer it will turns the text to numbers by measuring how important each word is and remove the stop word is, the, etc., and the logistic regression will learn which words are most associated to which category. Then it will also extract the amount of spam and risk associated with the words in the data. Then it will give the notification about the measure of spam and risk in the call to the user.

Formula of term frequency = (Number of times word appears in the data/ Total number of keys in the data)

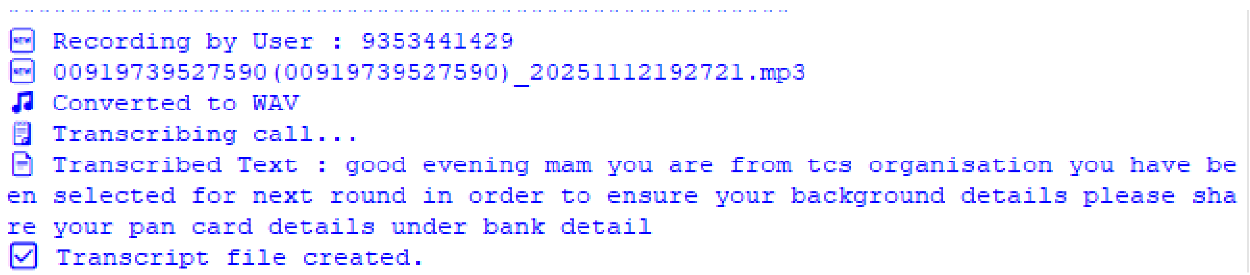
Formula of IDFT= log (total number of data sets /Number of document containing the key word) TF-IDF (Term Frequency–Inverse Document Frequency) is a statistical method used in natural language processing and information retrieval to evaluate how important a word is to a document in relation to a larger collection of documents. This

algorithm is implemented using Scikit learn library.

Arduino Uno: The predicted category of threat and the predicted spam rate and risk rate will be sent to Arduino UNO which will communicate with GSM modem. Global system mobile communication: It will act as communication channel between Arduino Uno and user phone which will send the message to the phone about the predicted threat and measure of spam and risk in the call processed. Then it will alert the user by sending the SMS to the user phone. User Mobile: The SMS alert will be sent to user system that is user mobile phone, so that user can block the number or report as spam call. Hence the call can be secured

4. Results:

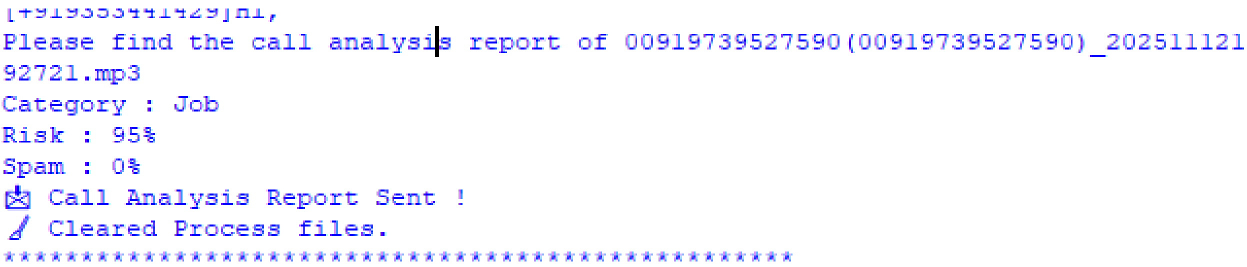
The body of the program is a call analysis which will detect the recorded calls then it will transcribe the audio format to the text format



```
Recording by User : 9353441429
00919739527590(00919739527590)_20251112192721.mp3
♫ Converted to WAV
Transcribing call...
Transcribed Text : good evening mam you are from tcs organisation you have be
en selected for next round in order to ensure your background details please sha
re your pan card details under bank detail
☑ Transcript file created.
```

Fig 4.1: Transcribing of audio to text

Then the AI model will predict the result based upon data sets given to It and the IF-IDF algorithm while training. It will categories the threat and send the SMS to the user phone.



```
[+919353441429]hi,
Please find the call analysis report of 00919739527590(00919739527590)_202511121
92721.mp3
Category : Job
Risk : 95%
Spam : 0%
Call Analysis Report Sent !
Cleared Process files.
*************************************************
```

Fig 4.2 Predicted Result

The above results will predict the category of the spam is job and the measure of the spam rate is 0% and the risk rate is 95%.

In the similar way we had predicted the results for different category such as Financial, Telemarketing and Job. Along with it we had predicted the risk and spam rating for the above categories.

4.1 Results that has been predicted by the AI model

Data	Category	Risk	Spam
Sample 1: Your account has been blocked temporily due to suspicious activity. Please share your bank details to unblock your account	Financial	95%	90%
Sample 2: This is from TCS organization, you are selected to the next round for background verification pls share your PAN card details	Job	85%	70%

Sample 3: This is from Jio customer care pls send your Phone number details to verify the details	Telecom	75%	65%

.

5. Conclusion:

In this project we will develop AI based telephonic security threat identification and Alert system cable of analyzing voice calls to detect potential threats. By integrating speech recognition by the Pandas libraries and the bayes theorem and naive bayes algorithms the system will accurately identify suspicious phrases, Aggressive tones, and keywords indicative of threats such as terrorism or violence. Thes approaches will significantly enhance the safety and security infrastructure in both government and private communication networks. The implementation of this project will demonstrate the potential of AI to contribute to national and organizational security.

5.1 **Discussion**:

We have discussed which of the libraries and algorithm can be used in this project to detect the spam calls. For preprocessing of the data. we are using the Pandas library, which will remove the null values in the data. To convert data from Audio to text we use speech recognition and the Whisper library. To give large set of data in the form of arrays to the AI model we are using the NumPy libraries All these libraries are built in Jupiter software. We import these Library from the software. Then we discussed about the algorithm which can be used to detect the spam calls and categorize those calls. We use Naive Bayes and Bayes theorem in order to detect the spam calls, and discussed how we can detect the malicious calls and how to differentiate between normal and suspicious calls by using this algorithm. As we train the Model by giving some datasets related to malicious calls. The algorithm extracts relevant features from call recordings, such as voice characteristics (e.g., tone, speed, pitch), keywords in the speech, and call duration. Existing call data is labelled as legitimate (e.g., normal customer service calls) or malicious (e.g., phishing attempts, scams).

6. Future Scope:

There is chance of leaking a confidential information. so as for the future use we can perform encapsulation on the data that has been captured so the data or information will not be leaked in the pathway. Advanced Biometric and Deepfake Defense. Voice Biometric Continuous Authentication: Moving beyond simple "Is this person a fraudster?" to "Is this the legitimate account holder?" The system will continuously verify the caller's identity (voice print) throughout the call, flagging if the voice suddenly changes or degrades (indicating a recording or deepfake). Generative AI (Deepfake) Threat Shielding: Incorporating models specifically trained to detect subtle, non-human artifacts in audio generated by Voice Cloning/Deepfake software, which are being used to impersonate company executives or clients. 2. Multi-Modal and Behavioral Analytics Omnichannel Risk Scoring: Expanding the analysis to correlate phone call data with other interaction channels (email, chat, web activity). For example, a low-risk phone call might become high-risk if it's immediately preceded by a failed web login or a suspicious email. Emotional and Psycholinguistic Analysis: Deeper use of Affective Computing to analyze subtle shifts in pitch, stress, cadence, and speaking rate, which are powerful indicators of deception, stress, or malicious intent, even if the spoken words are neutral. 3. Predictive and Autonomous Response. Predictive Analytics (Zero-Day Attack): Using sophisticated reinforcement learning to proactively identify new, zero-day attack scripts or social engineering tactics before they become widespread. The system can predict the next likely phrase of an attacker. Agentic AI Response: Developing systems where the AI can take autonomous, instantaneous actions in real-time, such as: o Silent Call Redirection: Transferring a high-risk call to a specialized fraud team without the scammer knowing. o In-Call Agent Assist: Providing the human agent with real-time, on-screen prompts (e.g., "Ask for secret code X," "Do not transfer the call," "Verify identity now"). o Dynamic Blocking: Instantaneously blocking a number after a single confirmed fraud attempt to prevent network propagation

REFERENCES

“Suspicious Call Detection and Mitigation Using Conversational AI” written by Kolati Mallikarjuna Rao and Bavvi kumar patil published in the year 2023.

“Artificial intelligence based fake or fraud phone call detection” written by B Durga Bhavani, Uppalla Nikitha 2, patolla nandini, netrika reddy published in the year 2024.

“Spam call protection Using machine learning” written by” Akash S published in the year 2024.

“A Multi-Channel Spam Detection System Utilizing Natural Language Processing and Machine Learning” written by Mohini Tyagi, Pradeep Kumar Singh, Shivam Kumar Yadav, Sanjay Kumar Soni published in the year 2024.

“Cyber-analytics: an examination of machine learning algorithms for spam filtering” written by Taiwo Ajani, Tammy Ferrante published in the year 2024.

“Machine Learning-Based Fraud SMS or Email Identification and Categorization” written by. lasya pithani, K. Chinna Nagaraju, V. Anil Santhosh published in the year 2023.

“Comparison of Machine Learning Algorithms for Spam Detection” written by Azeema Sadia, Fatima Bashir, Reema Qaiser Khan, Amna Bashir, and Ammarah Khalid published in the year 2023.

“Spam Call Detection Using Machine Learning” written by Potnuru Divya published in the year 2023.

Network Security Empowered by Artificial Intelligence.

Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector published by US department of Treasury.

Artificial Intelligence (AI) in Security Aspects of Industrie 4.0.

https://www.legitsecurity.com/aspm-knowledge-base/best-ai-cybersecurity-tools.

https://www.geeksforgeeks.org/naive-bayes-classifiers/

https://www.geeksforgeeks.org/bayes-theorem-in-artificial-intelligence/