**DISGUISE FORTIPS DRAFTS**

-> Disguise Fortips is an IT Platform that will be furnished with services, allowing anyone from anywhere to tip-off, promising to maintain anonymity.

Submit a detailed approach paper on developing an IT platform-enabled mechanism through which a person can give tip-off about any suspicious activity/ crime to law enforcement officials

==================================Important ->=============================

The system identifies tipsters by their tip number only, which it assigns to the tip.

////The Website allows tipsters to upload photos or video and is able to send the location of the video by a GPS.

=================================== Rough================================

1. IT platform. --<

2. Proof in form of pics, audio, video. --< (Om Khade)

3. Anonymous. --<

4. Will provide a code number (key) for future tip-offs. --<

5. Questionnaire based on domain selection. --<(Prasad Choulwar)

6. Voice data with encrypted voice notes. --< (Astha Kashyap)

7. Audio -> analysis through sentiments. --<(Om khade)

8. Calculating trust-score of a person on the basis of the question answered. --<

9. This info will be forwarded to the concerned authority. (Prasad Choulwar)

10.Audio -> analysis through sentiments and Voice stress analysis.-----------------<(Om khade)

11.Voice Bot for voice calls. --<(Astha Kashyap)

12.Chat bots for form analysis.--<(Astha Kashyap)

13.Ip address mapping through proxy server. --< (Saurav)

//14.Reward system for fully genuine tips.

//15.Blockchain cloud technique for users data storage.

//16. VoIP for calling

17. Toll free numbers calling anonymously. (Saurav)

=================================Draft-2==================================

->Disguise Fortips is an IT platform which will be a portal for submission of anonymous tip-offs regarding any suspicious activity / crime to law enforcement officials. The platform is designed in such a way that it won't be asking for any personal data nor it will be able to detect the user's Ip address because of a proxy server which will bind the user's Ip address for any cyber threats.

->There would be 3 modes of submitting the tip-offs.

->Firstly, the tip-offs can be submitted through an online encrypted anonymous form where there would be domains of crimes in which certain questionnaire are created to detect the authentication of tips. This form will also have an options of uploading the proof of the data which will act as a solely point for authenticity of info.

->Secondly, the witness will have options for tipping through voice data, which will get encrypted in a default voice note for maintaining anonymity. There will be genuine questions based on the information provided.

->Thirdly, the witness will have an option of tipping through calls where all necessary questions are asked through voice bots and those calls would be recorded once for detection of authenticity through lie detection through voice stress analysis which will eradicate the prank calls and all kinds of intentional reports for distraction.

->There would be chatbots for solving queries regarding Disguise Fortips.

->Anonymous login will be an option for witnesses for tipping more information which will provide an advantage for the authenticity based on previous tips.

->Blockchain cloud technique is used for user's data storage which will divide the data into different blocks and encrypt the data and will provide extra security to the information.

->Create a toll free number which will not record or show the caller ID on the call center telephones(i.e. No phone number shown)

==================CALCULATION OF TRUST-SCORE===========================

-> Feeding the tip-offs to the ML model.

-> Prediction of similar tip-offs based on the historical events(including the recent data).

-> Accuracy of data through prediction. (score1 = accuracy % ) wrt to date, time and recent activity.

-> Proof analysis (score2 = accuracy %) authenticated through local authority.

-> Lie detection using Voice stress analysis (score3 = stress measure in voice % )

-> Short mcq questions with a timer for creating a serious environment regarding authenticity of tips. (score4 = scores from analysis of answers)

-> Scores will be calculated on the basis of previous tips success rate if anonymous login is opted. (score5 = score of previous success% )

========================================================================

========================================================================

CRIME CATEGORIES ->

Counterfeiting and piracy

Domestic abuse

Doorstep crime (rogue traders)

Drink/drug driving

Drugs

Environmental crime

Poaching and wildlife trafficking

Gun crime

Harassment

Rape and sexual offences

Hate crime

Illegal tobacco

Modern slavery

Murder (incl. attempted/planned murder)

Possession of weapons

Robbery

Rural crimes

Terrorism

Vandalism

Vehicle

Violence

Corruption and police misconduct

Wanted person / fugitive

Weapons Wildlife crime

Other

========================================================================

========================================================================

CRIME CATEGORIES ->

Immigration

Poaching and wildlife trafficking

Smuggling weapons, drugs

Terrorism

Riots & Vandalism

Corruption and govt. misconduct

Human trafficking

Bomb blasting

Harming harmony

Wanted person/fugitive

Planning of murdering a special person

=============================Documents -> ==============================

<https://www.researchgate.net/publication/221152152_Voice_Stress_Analysis>

https://crime-in-india.github.io/

https://www.ijcrt.org/papers/IJCRT2005299.pdf

https://en.wikipedia.org/wiki/Voice\_stress\_analysis

https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0226257

=======================================================================

WE HAVE TO DEVELOP AN APPROACH PAPER ONLY.

========================================================================

This will also build a threat of getting caught in criminals.

========================================================================

1. Tip-off Input -> Questionnaire ->

=========================REFERENCES ->================================

Felipe Mateus Marcolla1 , Rafael de Santiago2 a and Rudimar Lu´ıs Scaranto Dazzi1

“Novel Lie Speech Classification by using Voice Stress”,

Available at:<https://www.scitepress.org/Papers/2020/90387/90387.pdf>

Léon J. M. Rothkrantz, Pascal Wiggers, Jan-Willem A. van Wees and Robert J. van Vark

“Voice Stress Analysis”,

Available at: [(PDF) Voice Stress Analysis](https://www.researchgate.net/publication/221152152_Voice_Stress_Analysis)

Paul Heaton and Luis Garicano, “Do Computers Help Police fight crime?CentrePieceWinter 2007/08”, Available at: [Do computers help police fight crime?](http://cep.lse.ac.uk/pubs/download/cp247.pdf)

Telugu Maddileti ,Vaddemani Sai Madhav , K V Sai Sashank ,G. Shriphad Rao, “Crime Data Analysis Using Machine Learning Models”

Available at: [Crime Data Analysis Using Machine Learning Models | International Journal of Advanced Science and Technology](http://sersc.org/journals/index.php/IJAST/article/view/15887)

Lawrence McClendon, Natarajan Meghanathan, “Using Machine Learning Algorithms to Analyze Crime Data”. Available at:

<https://www.researchgate.net/publication/275220711_Using_Machine_Learning_Algorithms_to_Analyze_Crime_Data/citations>

Alkesh Bharati, Dr Sarvanaguru RA.K “Crime Prediction and Analysis Using Machine Learning”

Available at: [Crime Prediction and Analysis Using Machine Learning](https://www.irjet.net/archives/V5/i9/IRJET-V5I9192.pdf)

=======================================================================

-> Proof

Increase in crime rate and fear in mind of witness motivate us to make this type of platform.

Ignorance of crime even after witnessing it.

===================CANDIDATE DECLARATION AND LEGAL TERMS=============

MIC & BPR&D is proud to host the MANTHAN (“Hackathon”). The Hackathon is governed by this Hackathon Participation Agreement (“Agreement”).

By entering the Hackathon, you (“Participant”) agree to abide by the Agreement which is a binding legal agreement between Participant, MIC & BPR&D with respect to the Hackathon.

**Eligibility**

Participants must be India citizens, and at least 18 years of age to participate, and must hold valid Indian identification certificate [Auth by govt.].

**Ownership of Entries**

Participants are not allowed to use the open-source tools provided by any of the third party provider in addition to other commercially known open source tools.

Participants are also encouraged to use their own proprietary solutions to develop creative and efficient algorithms. If you are representing a company, your company’s proprietary software assets are also allowed to be used with the appropriate permission within your organization.

Participants represents and warrants that they have permission to use such proprietary data and that it does not infringe on the intellectual property or proprietary rights of any third party, including, without limitation, any third party, patents, copyrights, or trademarks.

Please reference the Terms and Conditions data to confirm that all IP rights remain with the participant and/or the organization they are representing.

**Prize and Awards**

At the end of the hackathon teams will present their solution to the Expert Panels. All participants will undergo mandatory evaluation process scheduled by Batch incharge.

Process for evaluation will be anonymous. Process will be determined based on number of entries in grand finale.

Prize conferred as winning amount is divided in categories >> Student Category and Startup Category

**Publicity and Privacy**

Except where prohibited, by participating in the Hackathon, Participant understands that the Hackathon may be photographed, videotaped, recorded, etc. and hereby grants MIC and BPR&D the right to use or refrain from using Participant’s name

and/or likeness any and all footage about Participant’s participation in the Hackathon and Participant’s Hackathon submission in any manner or media that MIC and BPR&D sees fit without Participant’s review or approval and without compensation.

By participating in the Hackathon, Participants agree that their personal data provided as part of the Hackathon may be used for the purposes of the Hackathon.

Participation in the Hackathon constitutes Participant’s full and unconditional agreement to and acceptance of these Terms and Conditions (“Terms”). The term “you” refers to you, the “ Participant”.

**Licensing and Intellectual Property Rights**

MIC and BPR&D claims all licenses or intellectual property rights in Participant’s submission, except for the limited license to review the submission as part of Hackathon judging and awarding of prizes.

**Liability Release and Indemnity**

UNDER NO CIRCUMSTANCES WILL MIC & BPR&D BE LIABLE FOR ANY DIRECT,

INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH, ARISING OUT OF OR RELATING IN ANY WAY TO THE HACKATHON AND/OR THIS AGREEMENT.

Participant shall indemnify and hold MIC & BPR&D and its officers, directors, employees, successors and assigns harmless against any claims, losses, damages, liabilities and expenses (including reasonable attorneys’ and other professionals’ fees)

incurred by MIC & BPR&D in connection with, arising out of or relating in any way to the Hackathon and/or this Agreement.

**Disclaimer**

IN NO EVENT WILL MIC & BPR&D AND ITS SPONSORS BE LIABLE TO YOU FOR ANY DIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS OR PROFITS)

ARISING OUT OF OR IN CONNECTION WITH YOUR PARTICIPATION IN THE HACKATHON, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE),

STRICT LIABILITY OR OTHERWISE, AND WHETHER OR NOT SPONSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. Some

jurisdictions do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

**Governing Law and Severability**

This Agreement and its terms & conditions are governed by the law of India, without reference to rules governing choice of laws. Any action, suit or case arising out of, or in connection with,

this Hackathon or the Terms must be brought in either the Central or state courts located in the republic of India. All disputes, claims and causes of action arising out of or in connection with the Hackathon,

prizes or the Agreement shall be resolved individually, without resort to any form of class action, and exclusively by the courts of the Republic of India and each of the Participants submit to the exclusive jurisdiction and venue of such courts for the purpose of any such action.

If for any reason any provision of this Agreement is adjudicated to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this Agreement will continue in full force and effect.

**General**

The Hackathon is subject to Central, state, and local laws and regulations. The Hackathon is offered by MIC & BPR&D, which are not responsible

for (i) late, lost, damaged, incomplete, or misdirected Entries, responses, or other correspondence, whether by email or postal mail or otherwise; (ii) theft, destruction, unauthorized access to or alterations of Entries;

or (iii) phone, electrical, network, computer, hardware, software program or transmission malfunctions, failures, or difficulties.

MIC & BPR&D reserve the right, in their sole discretion, to cancel, modify or suspend the Hackathon in whole or in part, in the event of fraud,

technical or other difficulties or if the integrity of the Hackathon is compromised, without liability to the Participants. MIC & BPR&D reserve the right to disqualify any Participant,

as determined by MIC & BPR&D, in their sole discretion.

========================================================================

========================== Question Hour for session ==========================

1. How to submit and update the Theme 20 problem statement?

2. Where to submit the approach paper ?

3. What are the guidelines for the approach paper according to MANTHAN 2021 ?

4. How to do a presentation of an approach paper in front of jury panels ?

5. Video submission can be there with explanations abt approach paper.

6.

========================================================================

------------------------------------------------------SAURAV-------------------------------------------------------------

===============================Proxy Server===============================

A proxy server is a server that sits between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to

the real server. A proxy server can improve network performance by functioning as a caching server.

========================================================================

SECURITY

Dynamic AES 256-bit encryption is the safest encryption method and strongest encryption standard.

Dynamic encryption is a way to design block cipher algorithms, and AES has several dynamic variants in specialized literature.

Web Application Security: Exploitation and Countermeasures for Modern Web Applicationsel

------------------------Web Application Security Techniques and Tools--------------------------

1. SAST

Static Application Security Testing solutions scan the source code for vulnerabilities and security risks. It is typically rule-based, and scan results typically include false positives, so you’ll need to carefully analyze and filter the results to identify real security issues.

Web application reference =>

https://mobidev.biz/blog/best-practices-to-secure-web-applications-from-vulnerabilities

https://expertinsights.com/insights/what-is-email-encryption-how-does-it-work-and-how-can-it-protect-your-organization/

https://www.researchgate.net/publication/354046742\_From\_ES\_to\_Dynamic\_AES

Reference =>

https://www.researchgate.net/publication/354046742\_From\_ES\_to\_Dynamic\_AES

https://www.researchgate.net/publication/317615794\_Advanced\_Encryption\_Standard\_AES\_Algorithm\_to\_Encrypt\_and\_Decrypt\_Data

https://www.researchgate.net/publication/355342226\_A\_SURVEY\_ON\_DIFFERENT\_ENCRYPTION\_TECHNIQUES\_FOR\_IMAGE\_VIDEO\_AUDIO\_AND\_DOCS

https://ijarcce.com/wp-content/uploads/2012/03/IJARCCE6E-s-khan-Image-And-Audio-Based.pdf

https://www.sciencedirect.com/science/article/abs/pii/S0020025516311458

Image Encryption and Analysis using Dynamic AES

Video Encryption Techniques: A Review

https://www.meity.gov.in/writereaddata/files/WI3\_Cloud%20Security%20Best%20Practices\_06112020.pdf

Toll free numbers are with IVR + voice bot modal

IVR -> language selection

voice bot => crime selection /domain

recording every particular questions for segregated analysis.

---------------------------------Summary writing-----------------------------

Encryption Algorithm to be selected =>

Criteria for selecting algorithms =>

1.SECURITY

AES has the best ability to protect sensitive data from attackers and is not allowed them to break the encrypt data as compared to any cryptographic algorithms.

2. COST

AES is able to have high computational efficiency and can be used in a wide range of applications especially in broadband links with a high speed.

3.ALGORITHM AND IMPLEMENTTATION

The flexibility,simplicity and suitability of the algorithm for diversity of hardware and software implementation

Server security =>

1. CloudFlare

2. cloud.nicsi.nic.in

-> Platform as a Service (PaaS)

-> Infrastructure as a Service (IaaS)

-> Software as a Service (SaaS)

-> Storage as a Service

-> Load Balancer as a Service

-> Resource Monitoring as a Service

-> Vulnerability Assessment Service

-> Application Performance Management (APM) Service

-> Public IP Service

-> Data Analytics (DA) as a Service (CEAD)

-> Anti-virus Service

-> Web Application Firewall (WAF) Service

Vulnerability which is to be defenced ->

1. Injection

2. Broken Authentication

3. Sensitive Data Exposure

4. XML External Entities (XXE)

5. Broken Access Control

6. Security Misconfiguration

7. Cross Site Scripting (XSS)

8. Insecure Deserialization

8. Insufficient Logging and Monitoring

1. Porous defense vulnerability

-----------------WEbsite vulnerability-------------------------

It’s safe to say that today’s applications are often actually a combination of many sepa‐

rate but symbiotic applications working together in unison. This can be attributed to

the development of more cleanly defined network protocols and API architecture

patterns.

The average modern-day web application probably makes use of several of the follow‐

ing technologies:

• REST API

• JSON or XML

• JavaScript

• SPA framework (React, Vue, EmberJS, AngularJS)

• An authentication and authorization system

• One or more web servers (typically on a Linux server)

• One or more web server software packages (ExpressJS, Apache, NginX)

• One or more databases (MySQL, MongoDB, etc.)

• A local data store on the client (cookies, web storage, IndexDB)

most web applications used Simple Object Access Protocol (SOAP)-

structured APIs. REST has several advantages over SOAP:

• Requests target data, not functions

• Easy caching of requests

• Highly scalable

Vulnerabilities =>

1. Cross-Site Scripting (XSS) vulnerabilities

2. Cross-Site Request Forgery (CSRF)

3. XML External Entity (XXE)

4. Injection

5. Distributed Denial of Service (DDoS)

6. Denial of Service (DoS)

Defenses =>

1. hashing credentials

XSS protection => A web application firewall (WAF)

CSRF protection => validating a secret token, validating the HTTP Referer header

DDOS -> Captcha ( prevention)

Cloud flare native

Threshold set krna h …

Group of subnet or ip address

Get or pull requests have an ip address header.

Client-Server infrastructure.

IP + name + email => private info

Pre-emptive testing through metasploit + burp-suite. Vulnerability analysis. ( Diagnose the application )

WAF needs more resources for WAF.

Known TOR IP LIST.

TOR IP RECOGNITION.

DATA ENCRYPTION in rest

Entry and exit

Dns security

Tls version 1.3

Data in transit.

Encryption at database level and disk level.

Disk level => d drive encrypt.

------------------------------------------------------------------------------------------------------------------------------

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* \*\*ASTHA\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*//

============================= Voice Encryption=============================

**Homomorphic encryption** makes it possible to analyze or manipulate encrypted data without revealing the data to anyone. Something as simple as looking for a coffee shop when you’re out of town reveals huge volumes of data with third parties as they help you satiate your caffeine craving—the fact that you’re seeking a coffee shop, where you are when you’re searching, what time it is and more. If homomorphic encryption were applied in this fictional coffee search, none of this information would be visible to any of third parties or service providers such as Google. In addition, they wouldn’t be able to see what answer you were given regarding where the coffee shop is and how to get there.

Voice Encryption:

Simple Inversion:

Inversion scrambling inverts the frequencies and volume of the voice signal. The Icom UT-109 Scrambler Unit uses the simple inversion technique.

Hopping Inversion:

This method adds a greater degree of security than simple inversion. Using this method, the frequencies and frequency rates change irregularly. This causes a voice signal that that appears to "hop" all over a number of different frequencies and frequency rates.

Rolling Code Inversion:

Rolling code inversion uses a method where the voice signal is inverted at a constantly changing rate. It starts at an upward inversion frequency direction and climbs to the upper limit. Then, it reverses direction and inverts at lower frequencies until it reaches the lower limit. The Icom UT-110 Scrambler Unit uses this inversion technique.

<https://www.twilio.com/docs/voice/tutorials/voice-recording-encryption#how-encryption-works>

<https://wethegeek.com/best-voice-changer-apps-during-call-for-android-and-iphone/>

====================================================================

Lying through text:

-> taking longer time to make stories

-> overly complex answer to a relatively simple question

-> Avoiding Certain Questions

-> Going Out of Their Way to Proclaim Honesty

-> their wording sounds suspiciously scripted

Spotting lie question:

Honestly, you said that on my behalf?

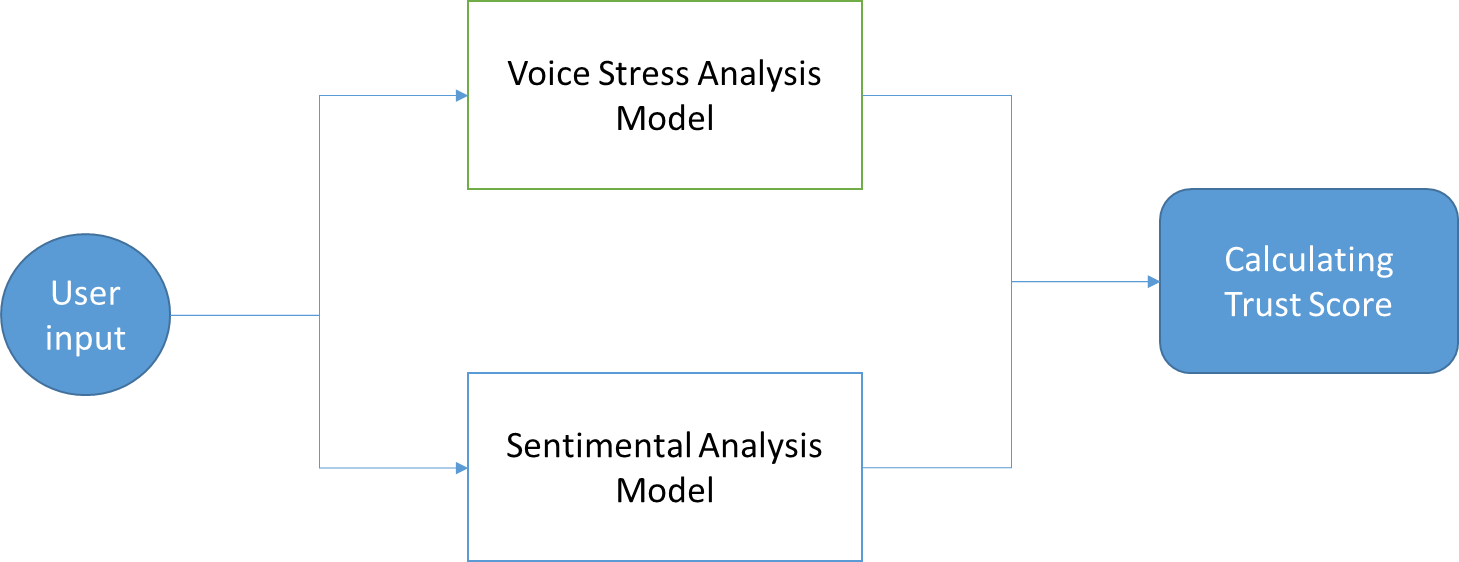
Honestly, you wrote that entire proposal yourself.

Honestly, that happened?

These queries are a gentle method of pinning a person to answer. If they dodge these questions, you may have spotted your liar.

================================OM======================================

===========================Voice Stress Analysis ->========================



We will be asking instantaneous questions to the witness after they have submitted the information through any of three modes during those questions Voice Stress Analysis will be used on the response provided to calculate the trust score.

//When victim is calling if panic or urgency is detected through our model then it means that they need urgent help so the call will be transferred to the nearest authorities

## **1 INTRODUCTION**

Voice Stress Analysis

Voice stress analysis detects stress or threat in a subject. His body reacts, and his muscles are ready to get into action. These preparations also affect the voice because of the tension in the respiratory system and tissues. For this reason, the voice can be used to detect stress (Liu, 2004)

The Voice Stress Analysis model has the objective to measure the disturbances from the voice pattern of a subject. They can be caused by physical stress that is triggered when lying when unexpected questions are asked through a voice bot on a website or on call.

The end goal is to use voice analysis of individuals reporting the crime to detect stress levels and classify the spoken information into two states: truth or lie, similar research shows that the Long Short-Term Memory (LSTM) neural network shows interesting levels of accuracy when developed and trained.

## **2 BACKGROUND**

In this section, the background related to Voice Stress Analysis is reported. Voice concepts are briefly discussed in the section ““Pitch, Jitter and Voice Stress”.The neural networks selected to develop our experiments are reported in the section “Long-Short Term Memory Neural Networks”. Finally, some related works are presented and discussed.

======================================================================

Telephone Default

* No caller ID on the call centre telephones (i.e. no phone number shown)

//Your telephone call is not recorded

Submitting information online

* We do not have access to personal data.
* We do not record your IP address, details of the computer you are using or your location.

=======================================================================

====================Voice Bot framework==========================

1. Select preferred language

2. Select crime category

3. Questionnaire will be conducted to take information from tipster

First a question will be asked by the bot and tipster will be told to answer,

Voice Activation Detection (VAD) is applied followed by Automatic Speech Recognition (ASR) and Automatic Speaker Diarization (ASD) to identify the major speaker, remove noise (if there are multiple speakers), to transcribe the verbal statement, extract the start and end time of each statement, if user stops for more than 5 seconds option to continue to next question is provided.(bot askes “to continue to next question press 2”)

If the user continues to the next question the response of the previous question is saved in the audio format and mapped to the respective question in the database.

For this analysis data has to be created as no similar data is available for model training.

—----------------------------------------------------------------------------------------------------------------------------

Automatic Speaker Diarization (ASD)

And in the world of audio transcription, this requires a level of technology, known as speaker diarization to enable this **process** and provide accurate data and quality audio recording content to end-users

Sue E. Tranter, Douglas A. Reynolds, “An overview of automatic speaker diarization systems” Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.208.1556&rep=rep1&type=pdf

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*//

-----------------------------------------------------Prasad—--------------------------------------------------------

When the victim or witness came on the portal of disguise fortips he can submit the tip in 3 ways

1> Tip-Offs submission through Anonymous Online Forms

2> Tipping through encrypted voice data (online)

3> Tipping through offline calls over Toll-free numbers

after this our system ask him for generating a key or he have already key he can enter or create the key

but it is totally depend on victim/witness

This key we use for storing data of validation either his information is right or not if found right then

we will increase the trust score regarding that key . key is associated with passphrase so that no one can misuse it.

after this we have main crime categories the system will divide obtained tip in specific crime and contact nearest reachable

authority to take action at crime location

{{{PPT SLIDE}}}

Our main motive of the system is to give quick response as well as avoid the crime from happening so the nearest authority is the best solution.

The network of local police is much bigger as compare to any other agencies so primary visitors or helpers are the police

if the complaint is against the police then, the tip should directly transferred to the regarding agencies like Anti corruption Bureau

or CBI. in some cases police are the only one who take the action against that specific crime like wanted person, pickpockets ; so they are primary

and main case in-charge .

if the we get the tip regarding fire like activities then directly get connected to fire brigade similar for forest department if the tips regarding

poaching and wildlife trafficking get to us then also we contact and give information to forest officers if these departments are not present at that

location then nearest authority will take action suddenly

After the action taken by local police or local authority

the respective cases are hand-over to related agencies after arrival

Smuggling weapons, drugs to Narcotics control Bureau

Corruption and govt. misconduct is to CBI/IT/ED/ACB

Planning of murdering a special person Bomb blasting Terrorism is to Reserved Forces or NSG

Terrorism is to Armed forces and Reserved Forces

These agencies will take the cases and work accordingly

To operate these type of system we required huge amount of data which can be provided by National Crime Record Buro (NCRB)

Which will help us to identify historic data of suspects as well as suspected places whether crimes are happening there or not.

======================sample questionnaire ================================

1. Please select a language of your choice

2. Select a crime category:

Immigration

Poaching and wildlife trafficking

Smuggling weapons, drugs

Terrorism

Riots & Vandalism

Corruption and govt. misconduct

Human trafficking

Bomb blasting

Harming harmony

Wanted person/fugitive

Planning of murdering a special person

3.Please give details of the person(s) you wish to report, including name(s) and address(es).

4. Which offence do you wish to report them for?

Murder or, Attempted or planned murder.

5. Please give details of the victim(s).

Activity

6. When did, or when will this happen?

Do you know when it happened, or when it is going to happen? (Required info)

7. What is the location of the murder or attempt? Please give us a full address if possible or anything else that will help us identify the location.

8. Please describe the incident.

9. Do any of the people involved in the crime have access to a weapon or weapons? If yes, can you give details of the weapon.

10. What happened to the clothing worn by the offender(s)?

Background

11. What, if any, is the relationship between the victim(s) and the offender(s)?

12. Please provide details of any phone numbers or social media accounts used by those involved.

13. Do the offender(s) work? If yes please provide us the job role, employer and the address of employer.

14. Please give details of any vehicles used.Please tell us everything you know about the vehicle(s) - registration plate, colour, make, model.

15. Please describe the offender(s). Include offender's ethnicity, sex, age, rough height or build, hair colour/style, distinguishing features (including facial hair/tattoos).

16. Please describe the victim(s).

17. Is there anything else you would like to add that may assist the investigation of this crime?

18.Would you like to keep in contact?

========================================================================

**INTRODUCTION / EXECUTIVE SUMMARY**

<Tagline>,

In a decade, criminal activities are increasing day-by-day, harming national security, public assets and citizens. Our patrolling system is not enough in managing all criminal offenses efficiently. Even though people who have witnessed the crime are afraid of speaking up due to fear of getting stuck in the hassle of investigations. Also, people fear to get exposed in the eyes of criminals or an abettor. The in-efficiency of agencies in maintaining the anonymity of the witness builds a huge gap between the citizens of the country and the respective security forces.

To reduce this gap we are introducing a web portal that will allow people to report the conspiracy that they have witnessed and also keep their identity secure. Criminals will be frightened of getting caught.

**PROBLEM DEFINITION**

Developing an IT platform-enabled mechanism through which a person can give a tip-off about any suspicious activity/ crime to law enforcement officials. Considering the following while conceptualizing the mechanism.

Anonymity of the person giving tip-off should be strictly maintained.

Mechanism should validate genuineness of the tip-off and minimize issues such as prank calls and intentional misreporting for vengeance or distraction, which waste the time of law enforcement officials.

Historical data-based statistics may be considered for establishing genuineness of the tip-off, for example, similar tip-offs from others on the same issue which have been deemed valid, trust score of the person giving tip-off, likelihood of reported issue to occur in the said area etc.

Mechanism may also evaluate mental awareness and perception of the person giving a tip-off by running a small questionnaire based on the selected crime category.

**Solution Approach**

Disguise Fortips is an IT platform which will be a portal for submission of anonymous tip-offs regarding any suspicious activity / crime to law enforcement officials. The platform is designed in such a way that it would not be asking for any personal data nor will it save users Ip address. Tipster’s identity will be totally secure and their data will not be leaked in any condition.

There are 3 modes of submitting the tip-offs.Firstly, the tip-offs can be submitted through an online form. Secondly, the witness will have an option for tipping through voice data, which will get encrypted in a default voice note for maintaining anonymity. Thirdly, the witness will have an option of tipping through calls using toll-free numbers where all necessary information will be collected through voice bots.There will be an option of creating an anonymous login for tipsters, so that they can provide information in future. Authenticity is verified on the basis of the historical data analysis, verification through local authority and success rate of previous tips given by tipsters through anonymous login.

**IMPLEMENTATION &**

**Model Development**

Three models

**Crime Analysis**

Crime Analysis is relevant to this project not only in the context of its use in tip verification, but also in providing for a component in the tipping process that is underutilized or missing (Authentication).Through research it was discovered that tips are chosen for follow-up based on an informal prioritization system where tips perceived to be important by the reviewer are investigated first. The hope, it seems, is that there will be one tip that will lead to the resolution of case and that this approach can help locate that single tip.Yet, problem-oriented[Reference no] and evidence-based[Reference no] policing both suggest that important information might also be gleaned from analyzing tips for underlying patterns and trends using a more advanced, non-manual system. Crime analysis techniques can help to facilitate these goals, but It can be time consuming and police might spend hours sifting through data trying to figure out if crime fits into known patterns or discover new patterns. Once a pattern is detected, the information can be used to predict, anticipate and prevent crime.

This takes us to a more empirical, data driven approach also called predictive policing. Which can be achieved by using Machine Learning thanks to the recent advancement in Deep Learning and abundant amount of crime data available online, since 2012 “ Open Data Policy of India (NDSAP) ”.

**Background:**

In this section, background related to evaluating models is explained.Voice Stress Analysis model and Sentimental Analysis Model are briefly discussed.

**Voice Stress Analysis**

Voice stress analysis detects stress or threat in a subject. His body reacts, and his muscles are ready to get into action. These preparations also affect the voice because of the tension in the respiratory system and tissues. For this reason, the voice can be used to detect stress (Liu, 2004)

The Voice Stress Analysis model has the objective to measure the disturbances from the voice pattern of a subject. They can be caused by physical stress that is triggered when lying when unexpected questions are asked through a voice bot on a website or on call.

The end goal is to use voice analysis of individuals reporting the crime to detect stress levels and classify the spoken information into two states: truth or lie, similar research shows that the Long Short-Term Memory (LSTM) neural network shows interesting levels of accuracy when developed and trained.[reference no]

—----------------------------------------------------------------------------------------------------------

->There would be 3 modes of submitting the tip-offs.

->Firstly, the tip-offs can be submitted through an online encrypted anonymous form where there would be domains of crimes in which certain questionnaires are created to detect the authentication of tips. This form will also have an option of uploading the proof of the data which will act as a solely point for authenticity of info.

->Secondly, the witness will have options for tipping through voice data, which will get encrypted in a default voice note for maintaining anonymity. There will be genuine questions based on the information provided.

->Thirdly, the witness will have an option of tipping through calls where all necessary questions are asked through voice bots and those calls would be recorded once for detection of authenticity through lie detection through voice stress analysis which will eradicate the prank calls and all kinds of intentional reports for distraction.

->There would be chatbots for solving queries regarding Disguise Fortips.

->Anonymous login will be an option for witnesses for tipping more information which will provide an advantage for the authenticity based on previous tips.

->Blockchain cloud technique is used for user's data storage which will divide the data into different blocks and encrypt the data and will provide extra security to the information.

->Create a toll free number which will not record or show the caller ID on the call center telephones(i.e. No phone number shown)

Creating a website through which user can send tips anonymously

—-----------------------------------------TIMELINE—-------------------------------------------