Problem Statements - Cyberthon 2025

Cyber Security Domains Covered :

Domain Name	No of Problem Statements
Digital Forensics & Incident Response	**04**
AI Cyber Security	**09**
Corporate Security	**05**
OSINT / Threat Intelligence	**05**
Child / Women Safety	**02**

S.No	Problem Statement ID	Problem Statement Name	Domain
1	CT-DFIR - 01	Crime Hotspot Mapping & Behavioural Analysis System	DFIR
2	CT-DFIR - 02	Tower Dump Analysis Tool For Crime Investigation	DFIR
3	CT-DFIR - 03	Network Forensics	DFIR
4	CT-DFIR - 04	Narcotics Website Takeover Tool	DFIR
5	CT-AICS - 01	Development of an NLP Model to Guide Citizens in Filing Cybercrime Reports for NCRP portal	AI Cyber Sec
6	CT-AICS - 02	Phishing Detection Tool	AI Cyber Sec
7	CT-AICS - 03	Real-Time Data Breach Alert System	AI Cyber Sec
8	CT-AICS - 04	DNS Spoofing / Email Spoofing detection	AI Cyber Sec
9	CT-AICS - 05	Cyber Crime Reporting AI Assistant	AI Cyber Sec
10	CT-AICS - 06	AI Assistant for cyber laws	AI Cyber Sec
11	CT-AICS - 07	Speech Emotion Recognition on live calls for cyber crime police	AI Cyber Sec
12	CT-AICS - 08	Fake News Detection System	AI Cyber Sec
13	CT-AICS - 09	Deep Fake Detection	AI Cyber Sec
14	CT-CS - 01	Secure Coding Analysis Tool	Corporate Sec
15	CT-CS - 02	Privacy-Preserving Data Sharing	Corporate Sec
16	CT-CS - 03	Passwordless Authentication	Corporate Sec

17	CT-CS - 04	Endpoint Security Management	Corporate Sec
18	CT-CS - 05	Automated Information Security Auditing Tool (GRC Tool)	Corporate Sec
19	CT-OSINT - 01	CCTV / Video Analytics	OSINT / Threat Intelligence
20	CT-OSINT - 02	Drone Technology	OSINT / Threat Intelligence
21	CT-OSINT - 03	Crypto Analysis & Intelligence Mapping Tool	OSINT / Threat Intelligence
22	CT-OSINT - 04	Dark Web / DarkNet / CDR Analysis Tool	OSINT / Threat Intelligence
23	CT-OSINT - 05	Decoding Virtual Numbers	OSINT / Threat Intelligence
24	CT-CWS - 01	New Age Women’s safety app	Child / Women Safety
25	CT-CWS - 02	Online child protection	Child / Women Safety

S.No	Problem Statement ID	Problem Statement Name	Domain
1	CT-DFIR - 01	Crime Hotspot Mapping and Behavioural Analysis System	DFIR

Description :

The project aims to create a user-friendly interface to assist law enforcement by mapping crime hotspots based on real-time FIR (First Information Report) data. It uses color-coded visualizations to highlight areas with high crime rates. It can filter these zones by various parameters like type of crime, time, and season. Additionally, the system extends to behavioral analysis of criminals and predictive insights, such as seasonal trends in crime patterns. The tool will also help in generating optimized patrol routes.

Objectives :

1. **Hotspot Mapping :**
    - Generate crime maps highlighting zones with frequent criminal activities.
    - Classify hotspots by crime categories such as theft, assault, or drug-related crimes.
2. **Behavioral Analysis :**
    - Analyze patterns of criminal behavior (e.g., specific times or seasons when crimes occur).
    - Predict future crime trends based on factors like societal conditions or historical data.
3. **Automatic Patrol Planning :**
    - Suggest optimal patrol routes for police based on seasonal trends and hotspots.
    - Support proactive deployment of forces to sensitive areas.
4. **Accident-Prone Area Identification :**
    - Data from iRAD (Integrated Road Accident Database) and CCTNS (Crime and Criminal Tracking Network & Systems) can be used to pinpoint accident hotspots.
5. **Legal Classification :**
    - Categorize crime data using relevant sections from laws like the Indian Penal Code, NDPS Act, Arms Act, etc., for better organization and analysis.

Expectations :

- **For Police :**
    - A simple and effective tool to monitor, predict, and manage crime.
    - Insights to allocate resources based on the severity and frequency of crime.
- **For Developers :**
    - Work with dummy/sample FIR data to build and test the system.
    - Implement color-coded visualizations for easy identification of crime hotspots.
    - Develop algorithms for behavioral and trend analysis.
- **For End Users :**
    - Intuitive interface with clear visuals and actionable insights.
    - Automated reports and patrol recommendations.

Expected Results :

1. **Hotspot Visualization :**
    - Dynamic crime maps showing high-risk areas in real-time.
2. **Proactive Policing :**
    - Data-driven patrol routes for efficient resource allocation.
3. **Predictive Analysis :**
    - Crime trend predictions based on historical and societal factors.
4. **Enhanced Safety Measures :**
    - Strengthened safety for women through strategic patrolling.
    - Identification of accident-prone zones to minimize road mishaps.
5. **Actionable Insights :**
    - Police can quickly respond to crime trends and allocate resources effectively.

S.No	Problem Statement ID	Problem Statement Name	Domain
2	CT-DFIR - 02	Tower Dump Analysis For Crime Investigation	DFIR

Description :

This project involves creating a tool to analyze cell tower dump data, which is a collection of location data for mobile phones connected to a specific tower at a given time. Law enforcement agencies use this data to identify potential suspects by finding common mobile numbers that appear at crime scenes or key locations.

Students will simulate this process using a database of dummy mobile numbers and timestamps, identifying overlaps to narrow down suspect movements. The tool will automate the analysis and provide clear, actionable insights for investigations.

Objectives :

1. **Prelims :**
    - Analyze cell tower dump data to identify common mobile numbers that appear in the same place within a specific timeframe.
    - Develop a system that can handle multiple datasets (e.g., Excel sheets with dummy data).
2. **Mains :**
    - Extend the tool to analyze multiple locations.
    - Identify mobile numbers that appear across different locations at different times.
    - Generate a route map showing the movement of suspects, including date and time stamps.
3. **Automation :**
    - Create a simple, user-friendly tool to automate the tedious task of manually sifting through tower dump data.

Expectations :

1. **For Students/Developers :**
    - Simulate cell tower data using Excel sheets with hundreds of dummy mobile numbers and timestamps.
    - Build a database system to store and analyze this data.
    - Implement features to compare and find common numbers across multiple datasets.
2. **For Law Enforcement :**
    - Provide a tool to quickly identify suspects based on cell tower data.
    - Generate clear visuals and route charts of suspect movements.
3. **For End Users :**
    - Ensure the tool is intuitive, with simple inputs like uploading data files.
    - Deliver results in a structured format, such as tables and maps.

Expected Results :

1. **Tower Dump Analysis :**
    - Identify mobile numbers common to a specific location during a specific timeframe.
    - Reduce the list of potential suspects efficiently.
2. **Multi-Location Analysis :**
    - Pinpoint numbers appearing at multiple locations (e.g., Place X, Y, Z) with their respective timestamps.
    - Visualize suspect movements using maps or timelines.
3. **Route Chart Mapping :**
    - Generate a route map showing where and when a suspect was present based on tower data.
    - Provide detailed logs for law enforcement to use in investigations.

S.No	Problem Statement ID	Problem Statement Name	Domain
3	CT-DFIR - 03	Network Forensics	DFIR

Description :

This project involves building a tool to analyze and monitor network connections, focusing on detecting hidden or masked activities behind public IP addresses. Criminals or insider threat actors often disguise their true identity by using public IPs or masking techniques, making it challenging to trace their activities. The **PROBE Tool** will help identify and trace these hidden connections by analyzing IP, MAC, and packet data.

In its advanced stage, the tool will also have the ability to terminate malicious connection requests made by the threat actor, providing an active defense mechanism. This solution will be agentless, meaning it won't require installation on individual devices, and will focus on intrusion detection and network traffic monitoring.

Objectives :

1. **Prelims :**
    - Trace and identify hidden connections linked to a public or masked IP address.
    - Analyze network traffic to uncover behind-the-scenes connections using packet data and MAC addresses.
    - Provide visibility into all devices and connections in a network, including those attempting to mask their origin.
2. **Mains :**
    - Add a feature to terminate malicious connection requests from identified threat actors.
    - Enhance the tool to actively monitor and block suspicious movements in real-time.
3. **Automation and Efficiency :**
    - Build an agentless solution for easy deployment across networks.
    - Focus on creating an intuitive interface to visualize network traffic and suspicious connections.

Expectations :

1. **For Developers :**
    - Develop a tool that can analyze network traffic without installing software on individual devices.
    - Use techniques like packet inspection and MAC/IP tracking to trace connections.
    - Simulate insider threat scenarios to test the tool’s capabilities.
2. **For Security Teams:**
    - Provide a solution to detect and trace hidden connections linked to a public IP address.
    - Enable proactive measures to block or terminate malicious activities.
3. **For End Users:**
    - Offer a simple and easy-to-use interface for network monitoring.
    - Deliver clear insights about suspicious connections and movements.

Expected Results:

1. **Network Visibility:**
    - Detailed mapping of all devices and connections in the network.
    - Ability to trace connections hidden behind public or common IP addresses.
2. **Intrusion Detection:**
    - Identify and flag suspicious activities based on IP, MAC, and packet data analysis.
    - Detect insider threat actors trying to hide or mask their activities.
3. **Threat Prevention:**
    - Terminate malicious connection requests from identified threat actors in real-time.
    - Block suspicious movements before they can escalate into significant threats.
4. **Agentless Monitoring:**
    - Provide a lightweight solution that does not require installing agents on devices, making deployment easier and faster.

S.No	Problem Statement ID	Problem Statement Name	Domain
4	CT-DFIR - 04	Narcotics Website Takeover Tool	DFIR

Description:

The Drug Website Takeover Tool is designed to assist law enforcement agencies in targeting and shutting down illegal drug-related websites operating on the surface web or dark web. These websites may promote or facilitate the sale of narcotics, launder money, or engage in other criminal activities.

The tool will identify vulnerabilities in such websites and enable law enforcement to disrupt their operations by taking control of the site, blocking access, or shutting it down entirely, depending on legal authority and jurisdiction.

Objectives:

1. **Identify Drug Websites:**
    - Locate and map websites involved in illegal drug activities using advanced scanning and reconnaissance techniques.
    - Categorize websites based on their type (e.g., sales, forums, marketplaces).
2. **Analyze Vulnerabilities:**
    - Detects technical weaknesses in the website, such as unpatched software, weak authentication, or misconfigured servers.
    - Prioritize vulnerabilities that can enable a controlled and legal takeover.
3. **Website Takeover:**
    - Provide tools to safely and efficiently take control of the website.
    - Replace illegal content with a takedown notice or redirect traffic to an educational or law enforcement page.
4. **Ensure Legal Compliance:**
    - Develop mechanisms to ensure the takeover process adheres to local and international cyber laws.
    - Log all activities for transparency and use in court proceedings, if needed.

Expectations:

1. **For Developers:**
    - Create a tool that uses ethical hacking methods to identify and exploit vulnerabilities.
    - Ensure the tool is secure and does not cause unintended damage to infrastructure.
2. **For Law Enforcement:**
    - Provide a step-by-step process to monitor, analyze, and disrupt illegal drug websites.
    - Include features for reporting and documenting actions taken for legal accountability.
3. **For Society:**
    - Help reduce the availability of illegal drugs by disrupting their online networks.
    - Contribute to awareness efforts by redirecting users to rehabilitation or anti-drug resources.

Expected Results:

1. **Identification of Illegal Websites:**
    - Map and monitor websites promoting or selling drugs.
2. **Efficient Vulnerability Exploitation:**
    - Identify technical weaknesses and use them to safely disrupt operations.
3. **Successful Website Takeovers:**
    - Replace illegal content with official law enforcement notices or educational material.
4. **Reduced Online Drug Activity:**
    - Disrupt supply chains by making it harder for criminals to operate.
5. **Enhanced Public Awareness:**
    - Redirect users to educational content about the dangers of drug abuse.

S.No	Problem Statement ID	Problem Statement Name	Domain
5	CT-AICS - 01	Cyber Crime Case Classification	AI Cyber Sec

Description :

Development of an NLP Model to guide citizens in filing cybercrime reports on the National Cyber Crime Reporting Portal (NCRP) correctly through a real time analysis of the description and incident supporting media files uploaded by the citizen.

Objectives :

To develop an NLP model that categorizes fraud based on victim descriptions, focusing on improving model accuracy.

Outputs :

Text Preprocessing : Tokenization, stop word removal, stemming, and text cleaning to prepare data.

Model Development : Selection of a suitable NLP model (e.g., Logistic Regression, LSTM, or BERT) for multi-class fraud categorization.

Accuracy Measurement : Evaluate the model based on metrics such as accuracy, precision, recall, and F1-score.

Result :

Participants will deliver a working NLP model with an emphasis on achieving the highest possible accuracy

S.No	Problem Statement ID	Problem Statement Name	Domain
6	CT-AICS - 02	Phishing Detection Tool	AI Cyber Sec

Description:

The **Phishing Detection Tool** is designed to help individuals and organizations identify and block phishing attempts. Phishing is a type of cyberattack where attackers trick users into revealing sensitive information, such as passwords, credit card numbers, or personal data, by pretending to be legitimate entities through fake emails, websites, or messages.

This tool will analyze suspicious emails, URLs, or messages, identify potential phishing indicators, and alert users about the threat. It can also provide educational feedback on why a message or site is flagged as phishing.

Objectives:

1. **Identify Phishing Attempts:**
    - Analyze emails, messages, or URLs to detect phishing attempts.
    - Flag signs like mismatched domains, fake branding, or suspicious attachments.
2. **Educate Users:**
    - Teach users about phishing tactics by explaining why something is flagged.
    - Help them recognize phishing attempts in the future.
3. **Prevent Damage:**
    - Block malicious links or attachments before users can interact with them.
    - Alert users or administrators about potential threats in real-time.

Expectations:

1. **For Developers:**
    - Build a tool that uses machine learning, pattern recognition, or rule-based systems to detect phishing attempts.
    - Ensure the tool is user-friendly and works seamlessly in email clients, browsers, or as a standalone application.
2. **For End Users:**
    - Provide easy-to-understand warnings when phishing is detected.
    - Offer clear explanations to improve user awareness about phishing tactics.
3. **For Organizations:**
    - Protect employees and systems from falling victim to phishing attacks.
    - Provide analytics and reports to improve security policies and training.

Expected Results:

1. **Accurate Phishing Detection:**
    - Successfully identify phishing emails, websites, and messages with minimal false positives.
2. **User Awareness and Training:**
    - Educate users on phishing tactics and how to avoid them.
3. **Enhanced Security:**
    - Block malicious content, preventing data breaches or financial losses.
4. **Comprehensive Reporting:**
    - Generate reports for organizations on detected threats and user interactions.

S.No	Problem Statement ID	Problem Statement Name	Domain
7	CT-AICS - 03	Real - Time Data Breach Alert System	AI Cyber Sec

Description:

The **Real-Time Data Breach Alert System** is a tool designed to notify individuals and organizations as soon as their sensitive information, such as email addresses, passwords, or credit card details, is found in data breaches. The system actively scans dark web forums, public breach databases, and other sources to detect leaks of confidential data and instantly alerts users to take action, such as changing passwords or securing accounts.

This tool helps mitigate potential damage by enabling users to respond quickly to a data breach.

Objectives:

1. **Monitor Data Breach Sources:**
    - Continuously scan the internet, including the dark web and breach repositories, for leaked personal or organizational information.
2. **Alert Users in Real Time:**
    - Notify users immediately when their data is found in a breach, along with details of what was exposed.
3. **Provide Actionable Steps:**
    - Suggest actions like resetting passwords, enabling two-factor authentication, or freezing accounts to prevent misuse of the compromised data.
4. **Educate on Data Security:**
    - Raise awareness about the importance of data security and proactive measures to avoid future breaches.

Expectations:

1. **For Developers:**
    - Build a system that integrates data breach monitoring APIs or scrapes reliable breach data sources.
    - Ensure secure handling of user data to avoid creating additional risks.
2. **For Users:**
    - Offer a simple interface where users can input email IDs, phone numbers, or other identifiers they want monitored.
    - Provide clear alerts and steps to mitigate risks when a breach is detected.
3. **For Organizations:**
    - Enable businesses to monitor corporate emails and accounts for breaches, ensuring quick responses.
    - Generate reports for administrators about breaches and organizational exposure.

Expected Results:

1. **Timely Notifications:**
    - Send real-time alerts to users when their data is found in a breach.
2. **Damage Mitigation:**
    - Help users secure accounts before attackers exploit leaked data.
3. **Increased Awareness:**
    - Educate users and organizations on the importance of strong passwords, secure systems, and data hygiene.
4. **Enhanced Security Posture:**
    - Reduce the risk of financial loss, identity theft, and other consequences of data breaches.

S.No	Problem Statement ID	Problem Statement Name	Domain
8	CT-AICS - 04	DNS Spoofing / Email Spoofing detection tool	AI Cyber Sec

Description :

The **DNS Spoofing / Email Spoofing Detection Tool** is designed to help individuals and organizations detect and prevent spoofing attacks.

- **DNS Spoofing**: A cyberattack where attackers redirect users from legitimate websites to malicious ones by altering the DNS (Domain Name System) records.
- **Email Spoofing**: A tactic where attackers forge the sender's email address to make it appear as if the email came from a trusted source, often used for phishing or spreading malware.

This tool will monitor and identify suspicious activities in DNS records or email headers, helping users detect and mitigate spoofing attempts.

Objectives :

1. **Detect DNS Spoofing:**
    - Monitor DNS records for unauthorized changes.
    - Identify mismatched or suspicious IP addresses that do not correspond to legitimate servers.
2. **Identify Email Spoofing:**
    - Analyze email headers to detect forged sender addresses.
    - Check for discrepancies in SPF, DKIM, and DMARC records.
3. **Prevent Spoofing Damage:**
    - Alert users about spoofing attempts in real-time.
    - Provide actionable steps to secure DNS settings or block malicious emails.
4. **Educate Users:**
    - Teach users to recognize the signs of DNS and email spoofing attacks.

Expectations :

1. **For Developers:**
    - Create a tool that scans DNS records and email headers for anomalies.
    - Use automation to provide real-time alerts for potential spoofing activities.
2. **For Users:**
    - Offer a user-friendly interface for analyzing DNS settings and email security.
    - Provide detailed reports and recommendations to mitigate risks.
3. **For Organizations:**
    - Enable businesses to protect their domain and email infrastructure from spoofing attacks.
    - Improve email deliverability and reduce the risk of phishing or reputation damage.

Expected Results :

1. **Timely Detection:**
    - Quickly identify DNS or email spoofing attempts before they cause harm.
2. **Improved Security:**
    - Protect users from phishing, malware, and data theft by securing DNS and email systems.
3. **Actionable Recommendations:**
    - Provide clear steps to fix vulnerabilities and prevent future attacks.
4. **Increased Awareness:**
    - Educate users about DNS and email spoofing tactics, helping them stay vigilant.

S.No	Problem Statement ID	Problem Statement Name	Domain
9	CT-AICS - 05	Cyber Crime Reporting AI Assistant	AI Cyber Sec

Description :

The **Cyber Crime Reporting AI Assistant** is a tool designed to help individuals and organizations report cybercrimes easily and efficiently. The AI assistant guides users through the process of reporting incidents such as hacking, phishing, identity theft, online harassment, and other digital crimes.

The tool simplifies the reporting process by collecting relevant details, organizing the information, and either submitting it to the appropriate authorities or providing clear instructions on how to do so. It also offers resources and guidance to help users understand their situation and take immediate action.

Objectives :

1. **Streamline Crime Reporting:**
    - Provide an easy-to-use interface for victims to report cybercrimes.
    - Ensure all necessary details are collected for a complete report.
2. **Guide Victims:**
    - Educate users about the steps to take after a cybercrime, such as securing accounts or preserving evidence.
3. **Assist Law Enforcement:**
    - Generate well-structured reports that can be used by law enforcement for investigation.
4. **Raise Awareness:**
    - Help users understand the types of cybercrimes and how to protect themselves in the future.

Expectations:

1. **For Developers:**
    - Build a conversational AI system that can understand user inputs, ask relevant questions, and guide users through the reporting process.
    - Ensure the tool is accessible across platforms (web, mobile, etc.) and respects user privacy.
2. **For Users:**
    - Offer a simple, step-by-step process to report cybercrimes without technical expertise.
    - Provide immediate guidance to mitigate the effects of the crime.
3. **For Authorities:**
    - Provide detailed, structured reports that contain all necessary information for initiating investigations.

Expected Results:

1. **Simplified Reporting:**
    - Victims can report cybercrimes quickly and without confusion.
2. **Improved Investigations:**
    - Authorities receive detailed, well-organized reports to help them act faster.
3. **Immediate Assistance:**
    - Users get actionable advice to protect themselves from further harm, such as freezing accounts or securing data.
4. **Increased Awareness:**
    - More people learn about cybercrimes and preventive measures through the AI assistant.

S.No	Problem Statement ID	Problem Statement Name	Domain
10	CT-AICS - 06	AI Assistant For Cyber Laws	AI Cyber Sec

Description :

The **AI Assistant for Cyber Laws** is a user-friendly tool designed to help individuals and law enforcement officers understand and navigate cyber laws. It provides clear answers to legal questions related to cybercrimes, such as hacking, phishing, online harassment, identity theft, and data privacy.

This assistant simplifies complex legal terms, offers guidance on reporting procedures, and helps police officers quickly access the relevant legal sections needed for case handling.

Objectives :

1. **Simplify Legal Information:**
    - Provide easy-to-understand explanations of cyber laws and legal sections.
    - Break down legal jargon into plain language for better understanding.
2. **Support Cybercrime Victims:**
    - Guide individuals on their legal rights and the steps to take when they face cybercrimes.
3. **Assist Police Departments:**
    - Help law enforcement quickly access relevant laws and procedures to handle cybercrime cases efficiently.
4. **Promote Awareness:**
    - Educate people and police officers about cyber laws and their applications.

Expectations :

1. **For Individuals:**
    - A simple interface to ask questions about cyber laws and receive clear answers.
    - Guidance on how to file complaints and take legal action.
2. **For Police Departments:**
    - Quick access to legal sections related to specific cybercrimes.
    - Information on legal procedures and reporting formats to streamline case handling.
3. **For Both Groups:**
    - Real-time access to updated information on cyber laws and regulations.

Expected Results :

1. **Increased Legal Awareness:**
    - People and law enforcement become more knowledgeable about cyber laws.
2. **Better Support for Victims:**
    - Victims of cybercrimes receive accurate advice on legal remedies.
3. **Efficient Case Handling:**
    - Police departments can refer to relevant laws and sections quickly, speeding up investigations.
4. **Accessible Legal Knowledge:**
    - Legal information is made readily available to anyone, anytime, without requiring expertise.

S.No	Problem Statement ID	Problem Statement Name	Domain
11	CT-AICS - 07	Speech Emotion Recognition on live calls for Cyber Crime Police	AI Cyber Sec

Description :

The **Speech Emotion Recognition (SER) Tool** is designed to assist cybercrime police in analyzing the tone and emotional state of individuals during live phone calls. By identifying emotions such as fear, anger, distress, or nervousness, the tool enables law enforcement officers to better assess the mental state of victims, suspects, or informants in real-time.

This tool can enhance decision-making during investigations, prioritize responses to critical calls, and provide insights into the caller's intentions or urgency.

Objectives :

1. **Real-Time Emotion Analysis:**
    - Detect and classify emotions during live calls with victims, suspects, or informants.
2. **Prioritize Critical Cases:**
    - Identify calls where emotions indicate urgency or danger, enabling quick action.
3. **Support Investigations:**
    - Provide additional context about a caller's emotional state, aiding in case analysis and handling.
4. **Improve Victim Assistance:**
    - Understand the emotional condition of victims to offer appropriate support and guidance.

Expectations :

1. **For Police Officers:**
    - A user-friendly interface that displays the detected emotions during live calls.
    - Alerts for emotions indicating distress, fear, or anger to ensure immediate attention.
2. **For Cybercrime Investigations:**
    - Tools to log emotional patterns for suspects or repeat callers to establish behavioral trends.
    - Integration with call records for a holistic view of the case.

Expected Results :

1. **Enhanced Victim Support:**
    - Help officers address victims' concerns empathetically by understanding their emotional state.
2. **Critical Call Prioritization:**
    - Detect calls from distressed victims or nervous suspects and allocate resources promptly.
3. **Efficient Case Handling:**
    - Provide emotional insights that help officers adapt their approach during interrogations or information gathering.
4. **Behavioral Analysis:**
    - Record emotional patterns over multiple interactions to aid in profiling suspects or understanding victim behavior.

S.No	Problem Statement ID	Problem Statement Name	Domain
12	CT-AICS - 08	Fake News Detection System	AI Cyber Sec

Description:

The **Fake News Detection System** is a tool designed to identify and flag fake or misleading news articles, posts, or messages. It uses artificial intelligence (AI) to analyze content, cross-check facts, and determine whether the information is genuine or fake.

This tool is especially useful for combating the spread of misinformation on social media, websites, and other communication platforms, helping individuals and authorities maintain trust in the information they consume or share.

Objectives:

1. **Identify Fake News:**
    - Analyze text content to determine its authenticity and highlight misinformation.
2. **Promote Reliable Information:**
    - Help users verify the accuracy of news or information before sharing it.
3. **Educate Users:**
    - Raise awareness about fake news and provide tips for spotting it.
4. **Assist Law Enforcement:**
    - Help authorities identify and act against sources spreading fake news, particularly content that incites fear, hate, or panic.

Expectations:

1. **For Individuals:**
    - Provide a simple interface where users can input news links or text to check its authenticity.
    - Offer a reliability score or clear verdict (e.g., “Fake,” “Real,” or “Unverified”).
2. **For Authorities:**
    - Monitor the spread of fake news and provide alerts for content that violates laws or poses risks to public safety.
3. **For General Use:**
    - Include features like fact-checking and source verification to make information more reliable.

Expected Results:

1. **Reduced Spread of Fake News:**
    - Misinformation is flagged and prevented from going viral.
2. **Informed Citizens:**
    - People can trust the information they consume and share.
3. **Support for Authorities:**
    - Law enforcement can take action against fake news creators and distributors.
4. **Increased Awareness:**
    - More people become aware of fake news and learn how to identify it independently.

S.No	Problem Statement ID	Problem Statement Name	Domain
13	CT-AICS - 09	Deep Fake Detection	AI Cyber Sec

Description :

The **Deep Fake Detection System** is a tool designed to identify manipulated media content, such as altered videos, images, or audio created using AI techniques. Deep fakes are often used to spread misinformation, commit fraud, or defame individuals. This tool uses AI algorithms to analyze media and determine whether it has been tampered with.

The system is particularly useful for law enforcement, journalists, and individuals to verify the authenticity of digital content and prevent the spread of malicious or misleading media.

Objectives :

1. **Detect Deepfakes:**
    - Identify manipulated videos, images, or audio files and flag them as fake or suspicious.
2. **Verify Authenticity:**
    - Provide users with insights into whether the media content is genuine or altered.
3. **Prevent Misinformation:**
    - Help stop the spread of false narratives created using deepfake technology.
4. **Support Law Enforcement:**
    - Assist in investigations by validating digital evidence and exposing fraudulent content.

Expectations:

1. **For Individuals:**
    - A user-friendly interface where users can upload videos, images, or audio files for verification.
    - Clear results indicating whether it is real or fake.
2. **For Authorities:**
    - Advanced analysis tools to monitor and track the use of deep fakes in criminal activities.
    - Alerts for malicious content targeting public safety or defaming individuals.
3. **Technical Features:**
    - Detection of subtle inconsistencies in media, such as unnatural blinking, mismatched shadows, or audio mismatches.
    - Continuous updates to detect the latest deepfake techniques.

Expected Results :

1. **Combat Misinformation:**
    - Identify and flag deepfakes before they can mislead people or cause harm.
2. **Enhanced Digital Trust:**
    - Help people trust the authenticity of media content they consume.
3. **Support Investigations:**
    - Provide law enforcement with tools to detect and remove fake content used in crimes.
4. **Educate Users:**
    - Increase public awareness about deep fakes and how to recognize them.

S.No	Problem Statement ID	Problem Statement Name	Domain
14	CT-CS - 01	Secure Coding Analysis Tool	Corporate Sec

Description:

The **Secure Coding Analysis Tool** is a software solution designed to analyze code written by developers and identify security vulnerabilities or flaws that could be exploited by attackers. The tool focuses on ensuring that the code adheres to secure coding standards and best practices, reducing the risk of security breaches in corporate software systems.

This tool is particularly useful in corporate environments to maintain high standards of software security, comply with regulations, and protect sensitive data.

Objectives:

1. **Identify Security Flaws:**
    - Detects vulnerabilities such as SQL injection, cross-site scripting (XSS), buffer overflows, and other common issues in the code.
2. **Promote Secure Coding Practices:**
    - Encourage developers to write code that is resilient to attacks by following best practices and standards.
3. **Automate Code Reviews:**
    - Reduce manual effort by automating the process of identifying security issues in large codebases.
4. **Compliance with Standards:**
    - Ensure the code complies with corporate security policies, industry standards (e.g., OWASP, PCI DSS), and legal regulations.
5. **Minimize Security Risks:**
    - Protect corporate applications and data from exploitation by ensuring vulnerabilities are fixed before deployment.

Expectations:

1. **Corporate Security Enhancement:**
    - Equip organizations with a reliable tool to review and secure their code during the development lifecycle.
2. **Developer-Friendly Interface:**
    - Provide clear and actionable feedback to developers, including the location of vulnerabilities and suggestions for fixes.
3. **Scalability:**
    - Support the analysis of code in multiple programming languages across various projects and teams.
4. **Integration with Development Tools:**
    - Seamlessly integrate with corporate CI/CD pipelines, IDEs, and version control systems to make secure coding part of the development workflow.

Expected Results :

1. **Reduced Vulnerabilities in Code:**
    - Eliminate security weaknesses early in the development process, reducing the risk of breaches.
2. **Improved Developer Awareness:**
    - Train developers to recognize and avoid insecure coding practices.
3. **Faster Development with Security:**
    - Automate security reviews to save time while maintaining high standards of security.
4. **Stronger Corporate Applications:**
    - Deliver robust and secure software, safeguarding corporate assets and customer data.

S.No	Problem Statement ID	Problem Statement Name	Domain
15	CT-CS - 02	Privacy-Preserving Data Sharing	Corporate Sec

Description:

The **Privacy-Preserving Data Sharing System** is a solution designed to enable secure and controlled sharing of sensitive corporate data while protecting the privacy of the individuals or entities involved. It ensures that data can be shared for collaboration, analysis, or reporting without exposing confidential or personally identifiable information (PII).

The tool uses techniques like encryption, anonymization, data masking, and differential privacy to safeguard data integrity.

Objectives :

1. **Secure Data Sharing:**
    - Enable sharing of corporate data without revealing sensitive or confidential information.
2. **Protect Privacy:**
    - Ensure that shared data adheres to privacy standards and laws, protecting individuals and corporate interests.
3. **Maintain Data Utility:**
    - Allow recipients to analyze and derive insights from the data while ensuring sensitive elements remain protected.
4. **Prevent Data Breaches:**
    - Minimize the risk of sensitive information leakage during data sharing processes.

Expectations :

1. **Corporate Data Security:**
    - Implement robust mechanisms for anonymizing or masking sensitive information before sharing.
2. **Customizable Privacy Controls:**
    - Allow organizations to define and configure privacy rules based on the type of data and intended use.
3. **Seamless Integration:**
    - Ensure compatibility with existing corporate data management systems and collaboration platforms.
4. **Data Sharing Transparency:**
    - Provide logs and reports on data sharing activities for auditing and monitoring purposes.

Expected Results :

1. **Enhanced Privacy:**
    - Sensitive information remains protected even when data is shared with external parties.
2. **Trust in Data Sharing:**
    - Builds trust among stakeholders by ensuring privacy and data security.
3. **Improved Collaboration:**
    - Facilitates secure and efficient collaboration with third parties or internal teams.

S.No	Problem Statement ID	Problem Statement Name	Domain
16	CT-CS - 03	Passwordless Authentication	Corporate Sec

Description:

The **Passwordless Authentication System** is a secure and user-friendly method for accessing corporate systems and applications without relying on traditional passwords. Instead of passwords, the system uses advanced authentication methods such as biometric verification (fingerprint, face recognition), magic links, hardware tokens, or one-time codes sent via email or mobile devices.

This approach enhances security, reduces the risk of password-related breaches, and improves the user experience by eliminating the need to remember or manage complex passwords.

Objectives:

1. **Strengthen Security:**
    - Eliminate vulnerabilities associated with stolen, weak, or reused passwords.
2. **Simplify User Experience:**
    - Provide employees with a seamless and efficient way to access corporate systems.
3. **Prevent Data Breaches:**
    - Reduce the risk of phishing, brute force attacks, and credential stuffing.
4. **Enable Modern Authentication:**
    - Support advanced security protocols like FIDO2 and WebAuthn for robust corporate security.
5. **Improve Productivity:**
    - Minimize time spent on password resets and troubleshooting authentication issues.

Expectations:

1. **Secure Access Control:**
    - Replace traditional passwords with biometric authentication, hardware tokens, or magic links for accessing corporate resources.
2. **Flexible Integration:**
    - Integrate seamlessly with corporate identity and access management (IAM) systems.
3. **Scalability:**
    - Support large-scale implementation across departments, systems, and devices.
4. **Compliance:**
    - Align with corporate security policies and regulatory standards for authentication.

Expected Results:

1. **Reduced Security Risks:**
    - Minimize the threat of password-related attacks such as phishing and credential theft.
2. **Enhanced User Convenience:**
    - Provide employees with faster and easier access to systems without compromising security.
3. **Improved Corporate Security Posture:**
    - Strengthen overall security by adopting a modern, passwordless approach.
4. **Cost Savings:**
    - Lower IT support costs by reducing password reset requests and related helpdesk activities.

S.No	Problem Statement ID	Problem Statement Name	Domain
17	CT-CS - 04	Endpoint Security Management	Corporate Sec

Description:

Endpoint Security Management is a system designed to protect all devices (called endpoints) that connect to a corporate network, such as laptops, desktops, mobile phones, and servers. These devices can be entry points for cyber threats like malware, phishing, or unauthorized access.

The system monitors, protects, and responds to potential threats on these devices, ensuring the corporate network and sensitive data remain secure. It plays a critical role in safeguarding remote workers, preventing data breaches, and complying with corporate security standards.

Objectives:

1. **Protect Endpoints from Cyber Threats:**
    - Shield devices from malware, ransomware, phishing attacks, and unauthorized access.
2. **Monitor Endpoint Activity:**
    - Track activity on all devices in real-time to detect unusual or suspicious behavior.
3. **Centralized Management:**
    - Allow IT administrators to manage security for all devices from a single platform.
4. **Enable Remote Threat Response:**
    - Quickly isolate and secure compromised devices, even in remote locations.
5. **Ensure Compliance:**
    - Meet corporate and regulatory security standards to avoid penalties and ensure data protection.

Expectations:

1. **Comprehensive Security:**
    - A robust system that protects all endpoints, including corporate and employee-owned devices (BYOD).
2. **Proactive Threat Detection:**
    - Detect and mitigate threats before they can cause harm.
3. **Seamless Integration:**
    - Work seamlessly with other corporate security systems like firewalls, antivirus, and intrusion detection systems.
4. **User-Friendly Management:**
    - Provide IT teams with easy-to-use tools for monitoring and managing endpoint security.

Expected Results:

1. **Enhanced Corporate Security:**
    - Strong protection for devices ensures the corporate network remains safe.
2. **Reduced Data Breach Risks:**
    - Quick detection and response prevent unauthorized access and data theft.
3. **Increased Employee Productivity:**
    - Secure endpoints allow employees to work safely without fear of cyber threats.
4. **Cost Savings:**
    - Preventing cyber incidents saves the organization from potential financial losses and reputational damage.

S.No	Problem Statement ID	Problem Statement Name	Domain
18	CT-CS - 05	Automated Information Security Auditing Tool (GRC Tool)	Corporate Sec

Description:

The **Automated Information Security Auditing Tool**, also known as a GRC (Governance, Risk, and Compliance) Tool, is designed to automate the process of assessing an organization's compliance with information security standards, policies, and regulations.

This tool evaluates corporate systems, processes, and practices to identify potential security gaps, track risks, and generate comprehensive audit reports. By automating the audit process, it reduces human errors, saves time, and ensures consistent adherence to regulatory requirements like GDPR, ISO 27001, or HIPAA.

Objectives:

1. **Streamline Security Audits:**
    - Automate repetitive tasks in the auditing process to improve efficiency and accuracy.
2. **Ensure Regulatory Compliance:**
    - Assess compliance with global and industry-specific information security standards and frameworks.
3. **Risk Identification and Tracking:**
    - Detects potential vulnerabilities and security risks in corporate IT systems.
4. **Generate Actionable Insights:**
    - Provide detailed reports with recommendations for mitigating identified risks.
5. **Simplify Governance and Reporting:**
    - Centralize the management of security policies, audit logs, and compliance documentation.

Expectations:

For Hackathon Participants:

1. **Develop an Automated Tool:**
    - Build a prototype that simplifies and automates the process of security audits.
2. **Innovative Solutions:**
    - Create innovative ways to track compliance, identify risks, and generate audit reports.
3. **Technical Integration:**
    - Enable the tool to work seamlessly with corporate systems like firewalls, endpoints, or cloud platforms.
4. **Focus on User-Friendly Design:**
    - Ensure the tool is easy for auditors and IT teams to use, even without advanced technical expertise.
5. **Real-World Application:**
    - Design the tool with practical, real-world use cases for organizations in mind.

For Organizations:

1. **Compliance Made Easy:**
    - Reduce the manual effort and time spent on information security audits.
2. **Improved Risk Management:**
    - Identify and address vulnerabilities quickly to strengthen the corporate security posture.
3. **Regulatory Confidence:**
    - Ensure consistent compliance with laws and standards to avoid penalties or breaches.
4. **Actionable Insights:**
    - Gain clear, actionable recommendations for closing gaps in security and compliance.
5. **Scalable and Customizable:**
    - Obtain a tool that adapts to the organization’s size, structure, and industry requirements.

Expected Results:

1. **Improved Audit Efficiency:**
    - Automated tools speed up the audit process, reducing time and effort.
2. **Enhanced Compliance:**
    - Consistent monitoring ensures the organization meets regulatory standards.
3. **Cost Savings:**
    - Automation reduces reliance on manual audits and minimizes costly compliance failures.
4. **Stronger Security Posture:**
    - Early detection of risks and gaps helps secure the organization’s IT systems.
5. **Comprehensive Reporting:**
    - Detailed reports help decision-makers understand the organization’s risk and compliance status.

S.No	Problem Statement ID	Problem Statement Name	Domain
19	CT-OSINT - 01	CCTV / Video Analytics	OSINT / Threat Intelligence

Description:

CCTV/Video Analytics for OSINT (Open-Source Intelligence) involves using advanced technology to analyze video footage from surveillance cameras to extract meaningful information. This tool can identify objects, track movements, detect unusual behavior, and recognize patterns or individuals of interest.

By leveraging video analytics, law enforcement, intelligence agencies, and investigators can quickly analyze large volumes of footage to gather actionable intelligence. The tool enhances situational awareness, aids investigations, and supports decision-making by providing insights from visual data.

Objectives:

1. **Automate Video Analysis:**
    - Reduce the manual effort required to review extensive CCTV footage by automating the process.
2. **Extract Intelligence:**
    - Identify and highlight critical events, objects, or individuals in video streams for investigation.
3. **Support OSINT Investigations:**
    - Leverage public and private CCTV footage to gather intelligence related to ongoing investigations or security threats.
4. **Real-Time Alerts:**
    - Generate real-time notifications for events like trespassing, loitering, or suspicious activities.
5. **Pattern Recognition:**
    - Identify repeated behaviors or movements that could indicate potential risks.

Expectations:

For Hackathon Participants:

1. **Build an Analytics Tool:**
    - Develop a prototype capable of processing video data to identify objects, faces, or anomalies.
2. **Focus on Efficiency:**
    - Ensure the tool works quickly and accurately, even with large amounts of video footage.
3. **Integrate OSINT Applications:**
    - Design the tool to incorporate publicly available video feeds or surveillance data into the analysis.
4. **User-Friendly Design:**
    - Create an interface that allows users to query, filter, and analyze video data effortlessly.
5. **Privacy Compliance:**
    - Ensure the tool respects privacy and complies with legal regulations during OSINT operations.

For OSINT Users (Law Enforcement/Investigators):

1. **Enhanced Investigative Capabilities:**
    - Gain access to detailed insights from CCTV footage to support evidence collection.
2. **Real-Time Threat Detection:**
    - Detect and respond to suspicious activities as they occur.
3. **Streamlined Data Processing:**
    - Automate the analysis of large volumes of video data to save time and resources.
4. **Collaboration Support:**
    - Share insights and findings with other teams securely and efficiently.

5. **Customizable Features:**

- Allow users to define specific events or objects of interest for targeted analysis.

Expected Results:

1. **Faster Investigations:**
   - Reduce the time needed to analyze hours of video footage by automating the process.
2. **Improved Situational Awareness:**
   - Provide real-time insights to law enforcement and OSINT teams for quicker responses.
3. **Actionable Intelligence:**
   - Highlight critical patterns, events, or individuals that are essential for investigations.
4. **Reduced Human Effort:**
   - Minimize manual labor while improving accuracy in video analysis.
5. **Scalable Analytics:**
   - Ensure the tool can handle various video feeds, from small to large-scale surveillance systems.

S.No	Problem Statement ID	Problem Statement Name	Domain
20	CT-OSINT - 02	Drone Technology	OSINT / Threat Intelligence

Description:

Drone technology is revolutionizing the way Open-Source Intelligence (OSINT) is gathered. Drones are equipped with cameras, sensors, and other advanced tools that allow them to capture high-quality images, videos, and real-time data from hard-to-reach areas.

In OSINT applications, drones can be used to monitor public events, map terrains, conduct environmental surveillance, and track movements over large areas. Their agility and ability to collect data from diverse locations make them invaluable tools for intelligence gathering.

Objectives:

1. **Enhanced Data Collection:**
    - Use drones to capture aerial views, monitor areas of interest, and gather high-resolution images and videos for analysis.
2. **Real-Time Surveillance:**
    - Enable live-streaming capabilities for immediate assessment of situations like public gatherings or natural disasters.
3. **Terrain Mapping and Analysis:**
    - Create detailed maps of terrains, infrastructure, or movement patterns in specific regions.
4. **Non-Intrusive Intelligence Gathering:**
    - Use drones for covert data collection without disturbing the area under observation.
5. **Support Investigations:**
    - Aid law enforcement and intelligence agencies by providing visual evidence and situational awareness.

Expectations:

For Hackathon Participants:

1. **Build a Drone OSINT Prototype:**
    - Design a system that uses drones to capture, process, and analyze data for intelligence purposes.
2. **Integrate with OSINT Tools:**
    - Ensure compatibility with existing OSINT frameworks for seamless data analysis and visualization.
3. **Focus on Automation:**
    - Develop features like automated flight paths, object detection, and real-time data streaming.
4. **User-Friendly Interface:**
    - Create an intuitive dashboard for controlling drones and viewing collected data.
5. **Privacy and Legal Compliance:**
    - Adhere to privacy laws and ethical guidelines for drone-based intelligence gathering.

For OSINT Applications (Law Enforcement/Investigators):

1. **Improved Data Accuracy:**
    - Capture precise and reliable data for investigations or intelligence operations.
2. **Extended Reach:**
    - Monitor areas that are difficult to access by traditional means, like disaster zones or remote terrains.
3. **Real-Time Monitoring:**
    - Observe ongoing events or situations and respond promptly to emerging threats.
4. **Versatility:**
    - Use drones for various applications, including traffic monitoring, border surveillance, and crime scene documentation.
5. **Enhanced Situational Awareness:**
    - Provide investigators with a bird’s-eye view of areas of interest.

Expected Results:

1. **Faster Intelligence Gathering:**
    - Drones can cover large areas quickly, reducing the time needed to gather data.
2. **Accurate Mapping:**
    - Generate precise 3D maps and models of terrains or areas under investigation.
3. **Enhanced Investigations:**
    - Provide visual evidence and actionable insights for law enforcement or intelligence teams.
4. **Cost Efficiency:**
    - Reduce the need for expensive helicopter operations or ground teams for surveillance.
5. **Safer Operations:**
    - Conduct surveillance in potentially dangerous areas without risking human lives.

S.No	Problem Statement ID	Problem Statement Name	Domain
21	CT-OSINT - 03	Crypto Analysis & Intelligence Mapping Tool	OSINT / Threat Intelligence

Description:

The **Crypto Analysis and Intelligence Mapping Tool** is designed to trace cryptocurrency transactions and provide a clear understanding of their flow. Using spider maps and detailed reports, the tool helps uncover the trails of digital assets, mapping out wallet connections and identifying potential patterns of suspicious activity.

The tool can trace IP addresses linked to specific transaction IDs and compile a tabulated report of wallet history, providing valuable insights for law enforcement agencies (LEAs) to investigate cryptocurrency-related crimes.

Objectives:

1. **Track Cryptocurrency Trails:**
    - Trace the flow of cryptocurrency from one wallet to another, creating a spider map for visualization.
2. **Provide Wallet History:**
    - Generate a detailed, tabulated report of wallet activities, showing transaction amounts, timestamps, and counterparties.
3. **Identify IP Addresses:**
    - Capture and analyze IP addresses linked to nodal transactions for added intelligence.
4. **Support LEA Investigations:**
    - Equip law enforcement agencies with tools to investigate illicit activities like money laundering, fraud, or ransomware payments.
5. **Simplify Data Representation:**
    - Present complex data in an easy-to-understand format for better analysis and decision-making.

Expectations:

For Hackathon Participants:

1. **Develop a Crypto Trail Mapping Tool:**
    - Build a prototype capable of tracing cryptocurrency flows and generating spider maps.
2. **Integrate with Blockchain APIs:**
    - Use blockchain data to track transactions and extract insights from the public ledger.
3. **Focus on Visual Representation:**
    - Create spider maps and easy-to-read tabular reports for clarity.
4. **Automate IP Address Tracing:**
    - Integrate the ability to trace and capture IP addresses linked to transactions.
5. **Ensure Accuracy and Speed:**
    - Optimize the tool to process large volumes of data quickly and accurately.

For Law Enforcement Agencies (LEAs):

1. **Comprehensive Crypto Trails:**
    - Gain detailed visibility into cryptocurrency movements for investigative purposes.
2. **Actionable Insights:**
    - Identify key wallets, transaction patterns, and potential connections to criminal activities.
3. **Enhanced Reporting:**
    - Access tabulated reports and visual maps to simplify complex investigations.
4. **IP Tracking Capability:**
    - Leverage IP data to trace transactions back to potential perpetrators.
5. **Ease of Use:**
    - Ensure the tool is user-friendly and requires minimal technical expertise to operate.

Expected Results:

1. **Complete Crypto Trails:**
    - Provide a full map of cryptocurrency flows, connecting wallets, amounts, and timestamps.
2. **IP Address Insights:**
    - Identify the source and destination IPs associated with nodal transactions.
3. **Clear Reporting:**
    - Generate detailed and easy-to-understand reports for investigative teams.
4. **Enhanced Investigative Capability:**
    - Help law enforcement agencies tackle cases involving cryptocurrency with more precision.
5. **Fraud Detection:**
    - Identify and flag suspicious patterns indicative of illicit activities.

S.No	Problem Statement ID	Problem Statement Name	Domain
22	CT-OSINT - 04	Dark Web / DarkNet / CDR Analysis Tool	OSINT / Threat Intelligence

Description:

The **Dark Web and CDR Analysis Tool** is designed to help investigators uncover links between activities on the Dark Web and call-related data from Call Detail Records (CDRs). The tool leverages OSINT (Open-Source Intelligence) and advanced data analytics to identify connections between suspicious communications, Dark Web transactions, and illegal activities.

By combining insights from the Dark Web with CDR data, investigators can identify patterns, trace networks, and gather actionable intelligence to combat cybercrime, fraud, trafficking, and other illicit activities.

Objectives:

1. **Dark Web Activity Analysis:**
    - Identify and monitor suspicious websites, forums, and transactions on the Dark Web.
2. **CDR Data Correlation:**
    - Analyze call records to find communication patterns, frequency, and geolocation data related to suspicious activities.
3. **Link Analysis:**
    - Connect Dark Web activities with CDR data to uncover hidden networks and individuals involved in illegal operations.
4. **Visual Mapping:**
    - Generate visual maps that show relationships between entities (e.g., phone numbers, IP addresses, and transactions).
5. **Support Investigations:**
    - Provide actionable insights to law enforcement agencies (LEAs) to help solve complex cases involving both digital and physical crimes.

Expectations:

For Hackathon Participants:

1. **Build a Unified Platform:**
    - Create a system that integrates Dark Web monitoring and CDR analysis into a single tool.
2. **Enable Automation:**
    - Automate data collection from the Dark Web and processing of CDRs to save time and enhance efficiency.
3. **Focus on Visualization:**
    - Include features like spider maps, timeline graphs, and relationship diagrams for better data interpretation.
4. **Ensure Data Security:**
    - Handle sensitive data (e.g., CDRs and Dark Web records) securely to prevent misuse.
5. **Develop Search Capabilities:**
    - Include search functionality to trace specific numbers, IP addresses, or keywords across both datasets.

For Law Enforcement Agencies (LEAs):

1. **Enhanced Investigative Capability:**
    - Trace communication patterns and Dark Web transactions linked to crimes like drug trafficking, cyber fraud, or human trafficking.
2. **Real-Time Alerts:**
    - Identify suspicious activities and generate alerts for timely action.
3. **Simplified Analysis:**
    - Correlate large datasets (Dark Web and CDR) efficiently to identify suspects and their networks.
4. **Evidence Generation:**
    - Provide detailed reports for legal proceedings, including visual maps and timeline analyses.
5. **Customizable Reports:**
    - Generate reports tailored to specific cases or investigative needs.

Expected Results:

1. **Uncover Hidden Connections:**
    - Identify links between suspicious phone numbers, IP addresses, and Dark Web activities.
2. **Detect Illegal Activities:**
    - Highlight patterns indicating crimes such as smuggling, cyber fraud, or ransomware payments.
3. **Actionable Insights:**
    - Provide investigators with clear leads to trace and apprehend suspects.
4. **Comprehensive Reporting:**
    - Generate detailed, easy-to-read reports that summarize findings for legal and operational purposes.
5. **Improved Collaboration:**
    - Foster collaboration between different law enforcement units by providing a centralized tool for intelligence analysis.

S.No	Problem Statement ID	Problem Statement Name	Domain
23	CT-OSINT - 05	Decoding Virtual Numbers	OSINT / Threat Intelligence

Description:

The **Virtual Number and VoIP Intelligence Tool** is designed to assist in tracing virtual numbers and Voice over Internet Protocol (VoIP) calls often used in cybercrimes like bullying, harassment, and fraud. Virtual numbers, which can originate from any country code (e.g., +1, +44), make it challenging to track perpetrators.

This tool decodes the IP and gathers basic information about VoIP calls, including SIP (Session Initiation Protocol) details. It provides intelligence on the origin of the virtual number, websites or platforms used, and basic user details, helping investigators gain insights into cybercriminal activities.

Objectives:

1. **Trace Virtual Numbers:**
    - Identify the origin and service provider of virtual numbers used in cybercrimes.
2. **VoIP Call Intelligence:**
    - Decode IP addresses associated with VoIP calls and analyze SIP trunking packets.
3. **Gather User Information:**
    - Extract and display basic details about the users operating virtual numbers and VoIP services.
4. **Domain Name Lookup:**
    - Integrate a lookup feature for identifying the domains and platforms involved.
5. **User-Friendly Interface:**
    - Provide an easy-to-use application or software for investigators to trace calls and gather intelligence quickly.

Expectations:

For Hackathon Participants:

1. **Develop a Prototype:**
    - Create a basic tool capable of tracing virtual numbers and decoding VoIP call details.
2. **Integrate SIP Analysis:**
    - Include packet detection for SIP trunking services and provide open port analysis.
3. **Design an Interface:**
    - Build an intuitive user interface to display results like call origin, IP address, and user details.
4. **Include Domain Lookup:**
    - Implement a feature to perform domain lookups for services linked to the virtual numbers.
5. **Focus on Automation:**
    - Automate data collection and analysis to simplify the investigation process.

For Law Enforcement Agencies (LEAs):

1. **Identify Call Origin:**
    - Trace the source of virtual numbers and VoIP calls used for cyberbullying or fraudulent activities.
2. **Track User Details:**
    - Retrieve details about users operating from specific platforms or domains.
3. **Simplify Investigations:**
    - Automate IP tracking, VoIP call analysis, and virtual number tracing for quicker case resolutions.
4. **Provide Actionable Intelligence:**
    - Deliver clear insights into the infrastructure and origin of the calls.
5. **Enhance Digital Forensics:**
    - Assist in building strong digital evidence for legal actions.

Expected Results:

1. **Virtual Number Tracing:**
    - Provide information about the country, platform, and user of virtual numbers.
2. **VoIP Call Decoding:**
    - Decode IPs, identify open ports, and extract SIP trunking details for calls.
3. **User Insights:**
    - Retrieve basic user details tied to the virtual number or VoIP call.
4. **Comprehensive Reports:**
    - Generate detailed reports of findings, including domain lookup results.
5. **Efficient Investigations:**
    - Save time by automating processes and simplifying technical analysis for investigators.

S.No	Problem Statement ID	Problem Statement Name	Domain
24	CT-CWS - 01	New Age Women’s safety app	Child / Women Safety

Description:

The **New Age Women Safety App** is designed to automatically sense danger and trigger an SOS alert, even when the user cannot operate their mobile device. Using multimodal data from the mobile device, such as audio, video, images, motion detection, and other sensors, the app identifies potentially dangerous situations and sends alerts to pre-defined emergency contacts or law enforcement with the user’s real-time location.

This app serves as a proactive solution to enhance women's safety by leveraging smart technologies to respond to emergencies effectively.

Objectives:

1. **Automatic Danger Detection:**
    - Use data from various mobile sensors (audio, video, motion, etc.) to identify situations where the user is in danger.
2. **SOS Alert Triggering:**
    - Automatically send an SOS alert with the user’s real-time location and surrounding data (e.g., audio clip or video).
3. **Emergency Communication:**
    - Notify pre-defined emergency contacts or law enforcement agencies with critical information about the situation.
4. **User-Friendly Operation:**
    - Ensure the app operates even if the user cannot physically interact with their mobile device.
5. **Multimodal Safety Features:**
    - Include options for voice-activated alerts, gesture recognition, or pre-configured motion patterns to trigger alarms.

Expectations:

For Hackathon Participants:

1. **Prototype Development:**
    - Build a basic version of the app that integrates multiple mobile sensors and triggers alerts based on present danger conditions.
2. **Sensor Integration:**
    - Use audio analysis (e.g., detecting screams), video analysis, and motion detection to identify emergencies.
3. **Real-Time Location Sharing:**
    - Implement GPS tracking to share the user's location in real-time with emergency contacts.
4. **Data Privacy:**
    - Ensure the app encrypts sensitive data, like location and multimedia files, to protect user privacy.
5. **Simple User Interface:**
    - Create a user-friendly design to allow easy configuration of contacts and alert triggers.

For End Users and Organizations:

1. **Automatic Safety Alerts:**
    - Provide a reliable mechanism to send alerts in dangerous situations without user intervention.
2. **Enhanced Responsiveness:**
    - Improve response time by sharing real-time location and contextual data with emergency responders.
3. **Customization:**
    - Allow users to set personalized emergency contacts and customize alert triggers (e.g., keywords, gestures).
4. **Scalable Use:**
    - Support a wide variety of devices and environments, ensuring usability across demographics.

Expected Results:

1. **Enhanced Safety:**
    - Enable women to feel safer with an app that proactively monitors and reacts to dangerous situations.
2. **Quick Alerts:**
    - Ensure immediate SOS notifications with accurate location and contextual data for effective assistance.
3. **Ease of Use:**
    - Provide a seamless and intuitive app experience that requires minimal user input.
4. **Multimodal Danger Detection:**
    - Reliably detect emergencies through multiple data points (e.g., sudden falls, suspicious noises, or abnormal movement).
5. **Scalable and Reliable:**
    - Deliver a robust application that works effectively across various mobile platforms and environmental conditions.

S.No	Problem Statement ID	Problem Statement Name	Domain
25	CT-CWS - 02	Online child protection	Child / Women Safety

Description:

The **Online Child Protection System** is designed to safeguard children from online threats such as cyberbullying, grooming, exploitation, inappropriate content, and other forms of digital harm. This tool monitors online activities, detects potentially harmful interactions or content, and provides alerts to parents, guardians, or law enforcement agencies. Using AI and advanced algorithms, the system aims to create a safe online environment for children while respecting privacy and ethical considerations.

Objectives:

1. **Monitor Online Activities:**
    - Track and analyze children's interactions on social media, gaming platforms, and other online environments to identify potential risks.
2. **Detect Harmful Behavior:**
    - Use AI to detect threats such as cyberbullying, grooming, exploitation, and access to inappropriate content.
3. **Real-Time Alerts:**
    - Notify parents or guardians immediately when harmful activities are detected.
4. **Promote Awareness:**
    - Educate children and parents about online safety and best practices for secure digital interactions.
5. **Privacy Protection:**
    - Ensure ethical handling of sensitive data to protect children's privacy.

Expectations:

For Hackathon Participants:

1. **Prototype Development:**
    - Build a tool or app capable of monitoring and analyzing online content for harmful patterns.
2. **AI Integration:**
    - Use natural language processing (NLP) and machine learning to detect harmful keywords, suspicious messages, or risky behaviors.
3. **Real-Time Reporting:**
    - Develop an alert system to notify parents or guardians of threats in real time.
4. **User-Friendly Interface:**
    - Design a dashboard that is easy to navigate for parents and provides clear reports of detected risks.
5. **Ethical Implementation:**
    - Incorporate privacy-focused mechanisms to ensure children's data is secure and used responsibly.

For Organizations:

1. **Proactive Protection:**
    - Equip parents and guardians with a reliable tool to monitor and protect their children's online presence.
2. **Threat Mitigation:**
    - Reduce the risk of online exploitation, grooming, and exposure to harmful content.
3. **Collaboration:**
    - Facilitate cooperation between families, schools, and law enforcement to address online threats effectively.
4. **Customizable Monitoring:**
    - Allow users to set preferences for what types of content or interactions should be flagged.

Expected Results:

1. **Enhanced Safety:**
    - Ensure children are protected from online threats by identifying and mitigating risks in real time.
2. **Parental Awareness:**
    - Help parents and guardians stay informed about their child's online interactions and potential risks.
3. **Empowered Children:**
    - Educate children about safe online behavior and foster awareness of digital dangers.
4. **Ethical and Responsible Use:**
    - Provide a tool that respects privacy while offering effective protection.
5. **Wider Impact:**
    - Contribute to reducing cases of online child exploitation and promoting a safer digital environment for children.