Tata Communications Cyber Security Hackathon

Title: Tata Communications Cyber Security Hackathon 2023

Event Sponsor: Tata Elxsi

In the technical fest: Daksh 2023

Conducted By: Team 1nf1n1ty

Prizes Worth: Rs. 1,00,000

1. 1st - Rs. 50,000
2. 2nd - Rs. 30,000
3. 3rd - Rs. 20,000

Timeline:

1. 28/03/2023 - Registration Starts
2. 02/04/2023 - Last Date for Abstract Submission
3. 03/04/2023 - Announcement of Shortlisted Abstracts
4. 07, 08, 09 - Sprint followed by valediction

Form Contents

Basic Rules:

1. This is a team participation hackathon. You can have at most 5 members in your team.
2. Teams having the right blend in gender will be appreciated.
3. You can either invite your friends to form a team or you can request other teams to add you as a member.
4. The Product / Project should not be plagiarised. If found plagiarised, it would be disqualified.
5. Entire idea / prototype and related IPR belongs to the team building it.
6. The project code/demo should be made available in the GIT and YouTube for the final evaluation. Submission of fully functional PoC is mandatory.
7. Judges' decision is final and non-appealable.
8. Teams once formed cannot be changed.

Prototypes will be judged, based on the following non-technical criteria.

1. Adaptability
2. Agility
3. Sustainability

4. Value impact

Prototypes will be judged, based on the following technical criteria.

1. Code
2. Design
3. Overall usability
4. Prototype build

Problem Statements:

1. Problem Statement 1: Create a secure Aadhaar-based voting system that ensures the integrity and confidentiality of the voting process.
    a. Expectations:
        i. Develop a system that can authenticate voters using their Aadhaar card and allow them to vote in a secure and private manner.
        ii. Design a user-friendly interface for voters to cast their votes and monitor the status of their vote.
        iii. Ensure that the system can handle a large number of voters and provide reliable and accurate vote counting results.
        iv. Ensure the security and confidentiality of the voting process, including preventing any form of tampering or manipulation of the voting data.

2. Problem Statement 2: Develop a system that can detect and prevent social engineering attacks by analysing social media profiles and identifying potential suspects.
    a. Expectations:
        i. Develop a system that can crawl and analyse social media profiles of users and detect any suspicious behaviour or activity.
        ii. Implement machine learning algorithms to detect social engineering attacks, such as phishing, pretexting, and baiting.
        iii. Develop a user-friendly interface for the end-users to report any suspicious behaviour or activity on social media platforms.
        iv. Ensure the system can alert the concerned authorities in real-time in case of any potential social engineering attacks.

3. Problem Statement 3: Develop a breach detection system to monitor and identify unauthorised changes to an aircraft's control system.
    a. Expectations:
        i. Develop a system that can monitor and analyse the communication data between different aircraft control systems and identify any unauthorised changes.
        ii. Implement machine learning algorithms to detect any suspicious behaviour or activity on aircraft control systems.
        iii. Develop a user-friendly interface for the pilots and air traffic controllers to report any anomalies or unauthorised changes in the aircraft's control system.
        iv. Ensure the system can alert the concerned authorities in real-time in case of any potential security breaches.
        v. Develop a system that can handle a large amount of aircraft control system data and provide reliable results.

4. Problem Statement 4: Develop a system to crawl, classify, and index illegal websites on the darknet to help law enforcement agencies track down and apprehend cybercriminals.
    a. Expectations:
        i. Develop a system that can crawl and analyse the darknet websites and identify any illegal activities, such as drug trafficking, weapons trading, and human trafficking.
        ii. Implement machine learning algorithms to detect any suspicious behaviour or activity on the darknet websites.
        iii. Develop a user-friendly interface for the law enforcement agencies to report any illegal activities on the darknet websites.
        iv. Ensure the system can alert the concerned authorities in real-time in case of any potential illegal activities on the darknet websites.
        v. Develop a system that can handle a large amount of darknet data and provide reliable results.

5. Problem Statement 5: Create a secure proximity authentication system that uses smart devices to authenticate users in a secure and privacy-preserving manner.
    a. Expectations:
        i. Develop a system that can use smart devices, such as smartphones and smartwatches, to authenticate users in a secure and privacy-preserving manner.
        ii. Develop a user-friendly interface for the end-users to configure and monitor their proximity authentication settings.

iii. Ensure the system can handle a large number of users and provide reliable authentication results.

6. Problem Statement 6: Develop a pluggable interface that can secure IoT devices and networks against cyber attacks.
    a. Expectations:
        i. Develop a lightweight interface that can be easily integrated with various IoT devices and networks.
        ii. Ensure the interface can detect and prevent common cyber attacks, such as DDoS attacks, malware injections, and unauthorised access attempts.
        iii. Implement advanced encryption and authentication protocols to secure the data transmission and storage of IoT devices and networks.
        iv. Develop a user-friendly interface for configuring and monitoring the security settings of IoT devices and networks.
        v. Ensure the interface is scalable and can support a large number of IoT devices and networks.