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.