Basic Details:

Ministry/Organization Name/Student Innovation:
National Technical Research Organisation (NTRO)

PS Code: SIH1677

Title: Developing a tool to provide real-time feeds of cyber incidents pertaining to Indian Cyber Space.

Team Name: HackSmiths

Team Leader Name: Harsh Kumar

Institute Name: Netaji Subhas University of Technology (NSUT)

Problem Overview

What is even the problem?

- India's Critical Information Infrastructure (CII) faces severe cyber threats, endangering national security and economic stability.

1. **Current Gap**: The NCIIPC's existing system lacks real-time monitoring, leading to no threat assessment and huge response gaps.
2. **Need for Real-Time Solution**:

- Framework Required: Development of a dynamic system to monitor and analyze cyber incidents specific to Indian cyberspace.
- Machine Learning Integration: Use ML to identify and aggregate data from diverse sources, including forums, social media, and news platforms.

3. **Inhouse Models**:

- Since its a national issue, these LLMs, RAGs, Scrapers, and servers must be in-house. Thus computing, storing and usage remains safe.

Idea/Approach Details

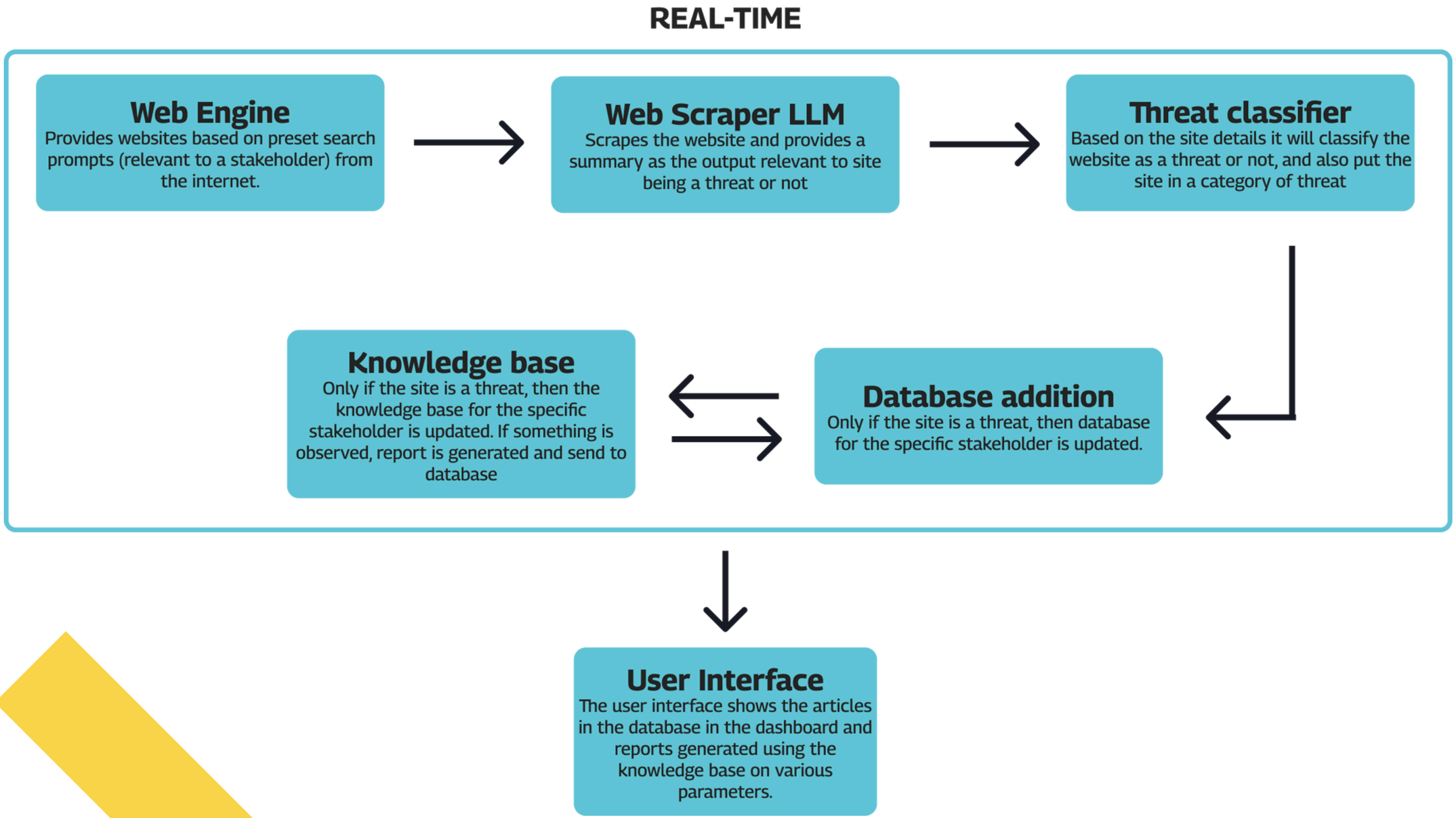
Real-Time Cyber Threat Monitoring Solution for India's CII
We propose a real-time cyber defense system to protect India’s Critical Information Infrastructure (CII) from evolving threats. The solution leverages in-house machine learning models to monitor, scrape, and classify data from a range of sources such as news platforms, forums, and social media, identifying potential threats.

Key features include:

- **Threat Classification**: Automated risk assessment using a robust classifier, categorizing threats like malware, phishing, or espionage.
- **Knowledge Base**: Secure and real-time updates to the knowledge base for detected threats.
- **In-House Models**: Ensuring privacy, data security, and full national control over infrastructure by keeping all models and servers within India.
- **User Interface**: Stakeholders receive real-time insights through an intuitive interface, with dashboards and reports enabling quick, informed responses.

This system addresses current gaps in the NCIIPC’s framework, ensuring faster response times, continuous monitoring, and enhanced national security.

Data flow and design:



Objectives:

Strengthen India’s Critical Information Infrastructure (CII) Cybersecurity

1. **Real-Time Threat Monitoring**: Implement a 24/7 surveillance system to reduce response times to cyber threats from an average of 48 hours to under 2 hours.
2. **Comprehensive Threat Coverage**: Target monitoring of 100,000+ sources, including social media, forums, and news platforms, covering 95% of cyber threat vectors impacting CII.
3. **Increased Detection Accuracy**: Achieve 95% accuracy in threat classification, reducing false positives by over 50%, and ensuring only actionable insights are flagged.
4. **Response Acceleration**: Enable threat assessment and mitigation in under 30 minutes from detection, cutting down the current response gap by over 70%.
5. **National Data Sovereignty**: Ensure that 100% of data processing, threat identification, and storage remain within national infrastructure, safeguarding critical information.

This system will significantly **reduce cyber incident impacts**, improve **national resilience**, and **close existing defense gaps**, securing India’s economic and national stability.

Tech Stack:

- **Data Collection & Scraping:** Python, Scrapy
- **Classification:** RNN, LSTM, Tensorflow, Scikit-Learn
- **NLP:**
- **Web-Backend:** Clerk, Node, Express, MongoDB
- **Deployment:** AWS EC2, Docker
- **Frontend:** React, Next.js, Tailwind CSS, Typescript
- **Additional Tools:**

Team Member Details

Team Leader Name: Harsh Kumar

Branch: BTech Stream: CSAI Year: IV RollNo: 2021UCA29

Team Member 1 Name: Avneet Singh Bedi

Branch: BTech Stream: CSAI Year: IV RollNo: 2021UCA15

Team Member 2 Name: Balvinder Singh

Branch: BTech Stream: CSAI Year: IV RollNo: 2021UCA45

Team Member 3 Name: Laksshay Sehrawat

Branch: BTech Stream: CSAI Year: IV RollNo: 2021UCA02

Team Member 4 Name: Raghav Mangla

Branch: BTech Stream: CSAI Year: IV RollNo: 2021UCA22

Team Member 5 Name: Sneha Gupta

Branch: BTech Stream: CSAI Year: IV RollNo: 2021UCA59