SMART INDIA HACKATHON 2024

SMART INDIA HACKATHON 2024

- **Problem Statement ID –** 1677
- **Problem Statement Title-** Developing a tool to provide real-time feeds of cyber incidents pertaining to Indian Cyber Space
- **Theme-** Blockchain & Cybersecurity
- **PS Category-** Software
- **Team ID-**
- **Team Name-** HackSmiths

CYBER SAINIK: The idea

SMART INDIA HACKATHON 2024

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.

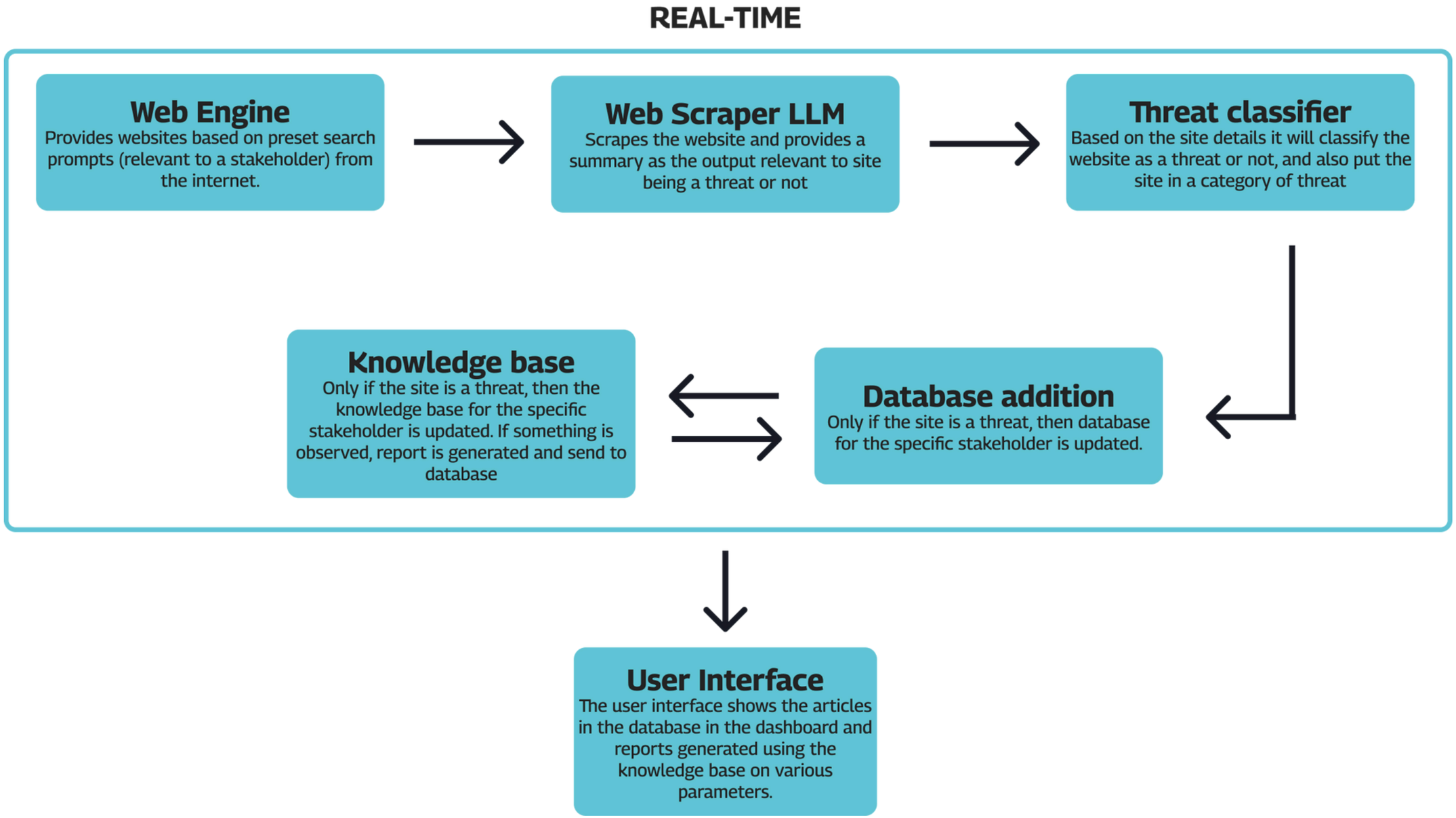
Key features include:

- **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.

Technical Overview

SMART INDIA HACKATHON 2024



FEASIBILITY AND VIABILITY

SMART INDIA HACKATHON 2024

The feasibility and viability of the real-time Cyber Threat Monitoring System for India's Critical Information Infrastructure (CII) are both highly practical and essential.

Technological Feasibility: Leveraging existing machine learning models, web scraping tools, and secure infrastructure, the system can be developed in-house, ensuring data privacy and compliance with national regulations. Proven technologies like Next.js, Node.js, and MongoDB enhance reliability, scalability, and seamless deployment.

Operational Viability: Real-time data scraping from multiple sources (forums, social media, and news platforms) allows continuous threat monitoring. This supports stakeholders in making immediate, informed decisions.
Cost Effectiveness: By maintaining a secure, in-house deployment and reducing reliance on third-party infrastructure, the system ensures long-term financial viability while offering better control and customization.

In conclusion, this solution provides a robust, scalable, and efficient method to safeguard India’s CII from ever-evolving cyber threats.

IMPACT AND BENEFITS

SMART INDIA HACKATHON 2024

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.

RESEARCH AND REFERENCES

SMART INDIA HACKATHON 2024

- **Growing Cyber Threat Landscape:** India is facing a 300% increase in cyberattacks on its critical infrastructure over the past five years, including sectors like energy, telecom, and finance. The lack of real-time monitoring has led to significant gaps in threat detection and response.
- **Market Size:** The global cybersecurity market is projected to reach $345.4 billion by 2026, with India's share growing rapidly due to its increasing digitalization efforts. Investments in cyber defense systems are expected to surge by 15-20% annually in the coming years.
- **Impact on CII:** A robust, real-time cyber threat monitoring solution could reduce the average incident response time from 48 hours to under 2 hours, minimizing disruptions and securing vital assets.
- **Cost of Cyber Incidents:** Each cyberattack on critical infrastructure in India could result in financial losses of over $1 million. By proactively addressing these threats, the system can save millions of dollars annually and bolster national security.
- **Government Support:** With government initiatives like Digital India and increased spending on cybersecurity, this project aligns with national priorities and meets urgent needs.