SIH
SMART INDIA
HACKATHON
2023

Basic Details of the Team and Problem Statement

Ministry/Organization Name/Student Innovation:

Indian Space Research Organization (ISRO)

PS Code: SIH1524

Problem Statement Title: Domain Name Server (DNS) Filtering Service using Threat Intelligence feeds and AI/ML Techniques

Team Name: Algorithm Alchemist

Team Leader Name: Aditya Jha

Institute Code (AISHE):

Institute Name:

Government Polytechnic Mumbai

Theme Name: Space technology

Idea/Approach Detail

✓ ***Network Monitoring and Security:***

- **Wireshark** and **Zeek** are vital for network monitoring, data collection, incident detection, and troubleshooting.

✓ ***Enhanced Security with DNS Filtering:***

- DNS filtering **safeguards** against **cyber threats** by **blocking** malicious domains and enabling secure communication through HTTPS, UDP, and DTLS.

✓ ***Cybersecurity and Blockchain Collaboration:***

- Cybersecurity and blockchain work together to **identify** threat emails, **labeling** them as **spam** for improved email security.

✓ ***Proactive Threat Notifications:***

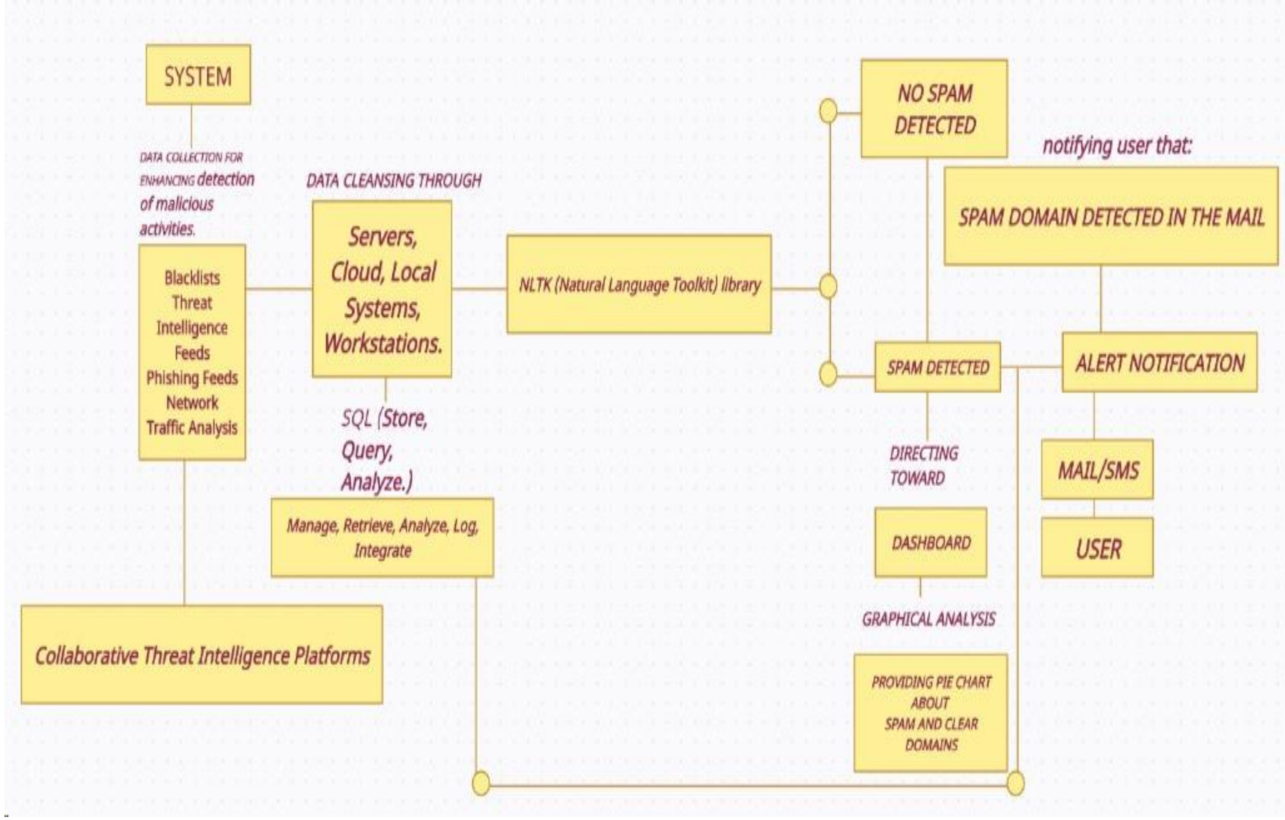
- **Automated notifications** flag emails with potential threats or spam by **analyzing** fake source code, **enhancing** user awareness.

✓ ***Cybersecurity Cell for User Safety:***

- A dedicated cybersecurity cell **notifies** users of email threats, effectively preventing potential **cyber-attacks** and enhancing safety.

✓ ***User-Controlled Measures:***

- Users can take action by **blocking** or **reporting** flagged spam emails via **DNS filtering**, ensuring proactive protection against **potential**



SYSTEM

DATA COLLECTION FOR ENHANCING detection of malicious activities.

Blacklists
Threat Intelligence Feeds
Phishing Feeds
Network Traffic Analysis

DATA CLEANSING THROUGH

Servers, Cloud, Local Systems, Workstations.

SQL (Store, Query, Analyze.)

Manage, Retrieve, Analyze, Log, Integrate

NLTK (Natural Language Toolkit) library

Collaborative Threat Intelligence Platforms

NO SPAM DETECTED

notifying user that:

SPAM DOMAIN DETECTED IN THE MAIL

SPAM DETECTED

ALERT NOTIFICATION

DIRECTING TOWARD

DASHBOARD

GRAPHICAL ANALYSIS

PROVIDING PIE CHART ABOUT SPAM AND CLEAR DOMAINS

MAIL/SMS

USER

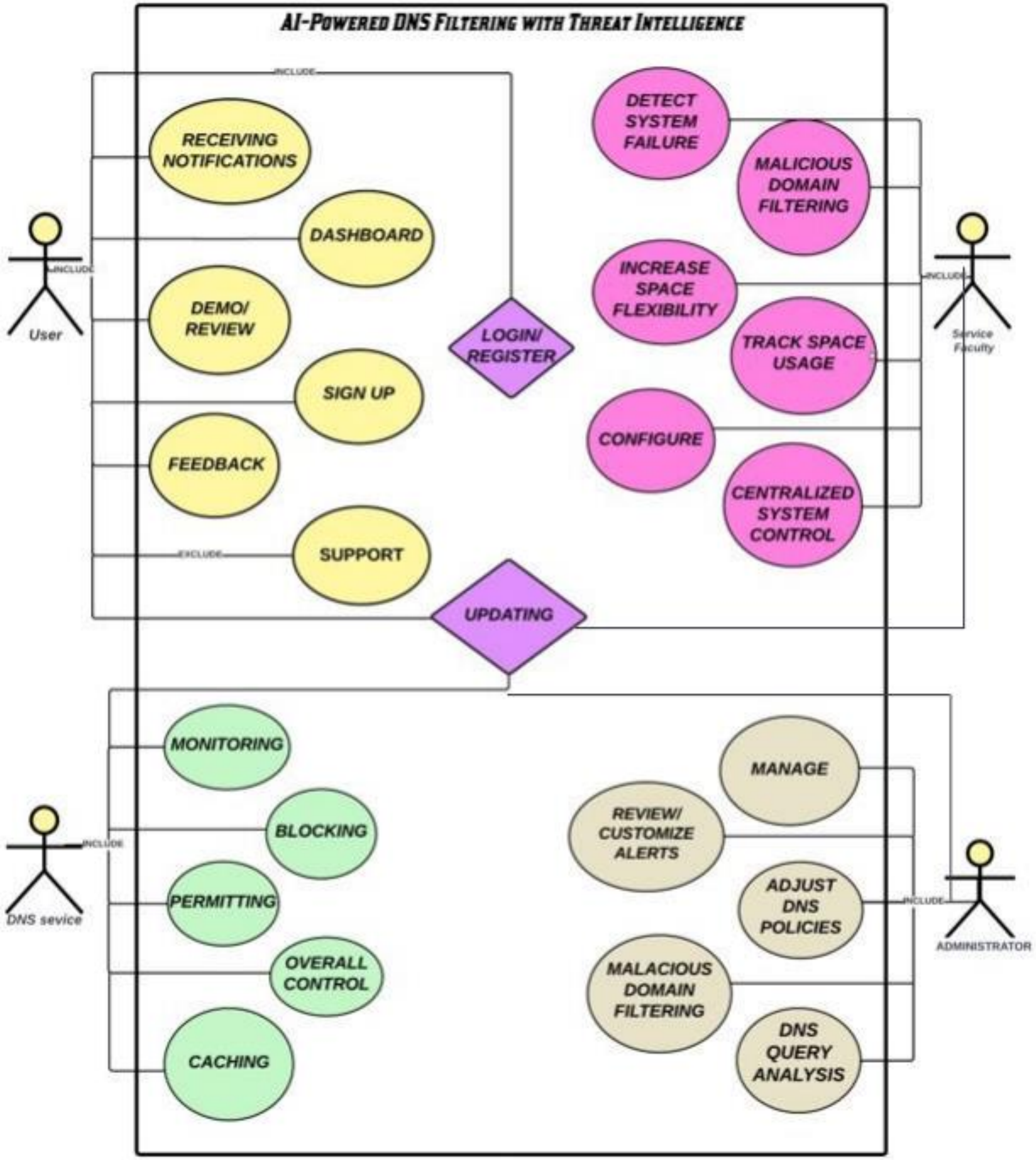
Idea/Approach Details

Dependencies:

- **Programming:** Python, Block Chain, Cyber Security
- **Web Development:** HTML, CSS
- **Networking Protocols:** DNS (UDP, DTLS, HTTPS)
- **Data Analysis:** Statistics, Pattern Recognition
- **Machine Learning:** TensorFlow, scikit-learn, Scipy
- **Security:** Firewalls, IDS/IPS
- **Database:** My SQL, NoSQL
- **Tools:** Wireshark, Git, ELK Stack

Showstopper:

- ➢ Service must handle lots of DNS queries quickly. If it's slow, network performance and security will suffer.
- ➢ Striking a balance between effective filtering and minimizing false positives prevents disruptions and user frustration.
- ➢ Accurate, updated threat data ensures effective service. Outdated or wrong data may miss threats or block real domains
- ➢ Challenging: Detecting DNS tunneling is hard due to evolving techniques. Staying ahead is vital for security against malicious actors.



Team Member Details

Team Leader Name: Aditya Jha

Branch : **Diploma** Stream : **AIML** Year : **1st year**

Team Member 1 Name: Rutuja Morankar

Branch : **Diploma** Stream : **AIML** Year : **1st year**

Team Member 2 Name: Pranjal Sutar

Branch :**Diploma** Stream : **AIML** Year : **1st year**

Team Member 3 Name: Nikhil Sawant

Branch : **Diploma** Stream : **AIML** Year : **1st year**