CyberScope

“ Real-Time Insights into Cyber Incidents”

Synopsis submitted to
Shri Ramdeobaba College of Engineering & Management, Nagpur in partial fulfillment of requirement for the award of the degree of

Bachelor of Technology (B.Tech)

In

COMPUTER SCIENCE AND ENGINEERING

(Cyber Security)

By

Vaidehi Chavan (17)

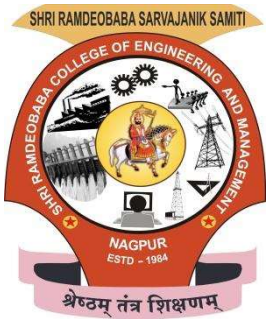
Arnav Dekate (30)

Paras Sawalkar (46)

Manas Badhani (70)

Guide

Prof. Monika Bagade



Department of Computer Science and Engineering – Cyber Security

Shri Ramdeobaba College of Engineering & Management, Nagpur 440 013

(An Autonomous Institute affiliated to Rashtrasant Tukdoji Maharaj Nagpur University Nagpur)

August 2024 - 25

1. Introduction

The rapid advancement of technology has brought immense benefits, but it has also exposed critical digital infrastructures to growing cyber threats. As a result, safeguarding these infrastructures, particularly those that are deemed crucial to national security, has become an urgent priority for governments worldwide. In India, the **National Critical Information Infrastructure Protection Centre (NCIIPC)** is responsible for ensuring that the country's critical information infrastructure remains protected from cyber-attacks. The increasing complexity and sophistication of cyber threats demand innovative solutions that can proactively detect, monitor, and respond to these threats.

This project aims to address one of the problem statements of the **Smart India Hackathon (SIH) 2024** by developing a web-based platform that autonomously aggregates and structures cybersecurity incident data. By utilizing a combination of advanced Machine Learning, data scraping techniques, and interactive visualization tools, the platform will enable stakeholders to gain valuable insights and take proactive measures to mitigate cyber risks. The platform will be tailored specifically to the Indian cyberspace and will play a critical role in supporting the NCIIPC's efforts to protect India's national security.

2. Objectives

The objectives of the project are multifaceted and designed to address the various challenges posed by cyber incidents. These objectives include:

1. **Awareness Building:**
   To inform users about the latest cybersecurity incidents and emerging threats.
2. **Educational Resource:**
   To provide informative content that helps users understand cybersecurity concepts and best practices.
3. **Data-Driven Insights:**
   To analyze and present trends in cybersecurity incidents, enabling users to make informed decisions regarding their digital safety.
4. **Community Engagement:**
   To foster a community of users who are proactive about cybersecurity and can share knowledge and experiences.

3. Problem Statement

The current lack of automated tools for collecting and analyzing cybersecurity data poses significant challenges for the NCIIPC in its mission to protect India's critical digital assets. With the frequency and severity of cyber-attacks growing, real-time access to accurate and comprehensive data is essential for mitigating risks. However, manually collecting and structuring this information from a wide variety of sources is an impractical task.

The National Critical Information Infrastructure Protection Centre (NCIIPC) is tasked with protecting India's most sensitive digital assets. To effectively do this, NCIIPC requires real-time, detailed information about cyber threats and incidents occurring within Indian cyberspace. Currently, there is a lack of comprehensive tools to automatically gather and analyze such data from across the web. This project aims to bridge this gap by creating a web-based platform that can autonomously collect, structure, and present cyber incident data, enabling better threat assessment and response.

4. Proposed Methodology

1.Backend Architecture

The backend of CyberScope is built using Node.js and Express.js, providing a robust server-side environment that handles data processing, storage, and API management.

1.1 Data Scraping and Processing

- Web Scraping:
  - Selenium WebDriver: Utilized to automate the process of searching for cybersecurity-related incidents on search engines. It performs the following steps:
    - Navigates to the search engine.
    - Enters a predefined query related to cybersecurity incidents.
    - Extracts links and relevant content from the search results.
- Content Cleaning:
  -
  - The cleanseText function processes the scraped text to remove unnecessary characters, ensuring that only meaningful content is retained. This includes:
    - Removing invisible characters (e.g., zero-width spaces).
    - Filtering out non-ASCII characters to maintain text integrity.
- Text Classification:
  - Natural Library: Implements a Naive Bayes classifier to determine the relevance of the scraped content. The classifier is trained on specific keywords related to cybersecurity incidents (e.g., "breach," "malware," "vulnerability"). The classification process involves:
    - Adding documents to the classifier with labels (e.g., "relevant" or "irrelevant").
    - Training the classifier to improve accuracy over time.

1.2 Data Storage

- PostgreSQL Database:
  - Relevant and meaningful incidents are stored in a PostgreSQL database. Each entry includes:
    - URL: The source link for reference.
    - Text: The summarized content of the incident.
    - Timestamp: The date and time the incident was recorded.
- Summarization:
  - Before storage, the content is summarized using the node-summary library. This ensures that only concise, relevant information is saved, making it easier for users to digest the information.

1.3 Insights Generation

- Data Analytics:
    - The backend includes functionality to generate insights from the stored data. This involves:
        - Aggregating incident data over the past 30 days.
        - Calculating trends, such as the frequency of incidents and types of threats.
        - Saving the analysis in a JSON file for easy access and visualization.

2. Frontend Architecture

The frontend of CyberScope is developed using React.js, providing a responsive and dynamic user interface that enhances user experience.

2.1 User Interface Components

- Navbar Component:
    - A navigation bar that allows users to easily access different sections of the application, including Home, Services, and About Us.
- Showcase Component:
    - A visually appealing section that introduces the purpose of CyberScope, highlighting the importance of cybersecurity awareness. It includes:
        - A compelling headline.
        - A brief description of the services offered.
- IncidentsCard Component:
    - This component fetches and displays recent cybersecurity incidents from the backend. Each incident card includes:
        - Title: A brief description of the incident.
        - Date: The date the incident occurred, formatted for user readability.
        - Summary: A concise summary of the incident.
        - Link: A call-to-action that allows users to read more about the incident on the source website.
- Services Component:
    - Outlines the various services offered by CyberScope, including:
        - Analyze: Personalized assessments to improve cybersecurity posture.
        - Detect: Real-time detection and monitoring systems for potential threats.
        - Develop: Tailored security solutions to build resilient continue systems that protect against cyber threats.

- About Us Component:
    - Provides information about the mission and vision of CyberScope. This section emphasizes the commitment to empowering individuals and organizations through cybersecurity awareness and education. It includes:
        - A statement of purpose.
        - Information about the team's expertise and dedication to cybersecurity.

2.2 API Integration

- The frontend communicates with the backend via RESTful API calls using Axios. Key functionalities include:

- Fetching Incident Data: The frontend makes GET requests to the backend to retrieve the latest incidents stored in the PostgreSQL database.
- Error Handling: The application gracefully handles errors during API calls, providing user feedback in case of issues.

3. Data Flow and Interaction

The data flow within the CyberScope application is designed to be seamless and efficient, ensuring that users receive the most relevant information in real-time. The following outlines the key interactions and processes:

1. User Interaction:
    - Users access the CyberScope application and are greeted with the showcase and navigation options.
    - Users can navigate to different sections, such as Services and About Us, or focus on recent incidents.
2. Backend Processing:
    - Upon initialization, the backend scrapes relevant links and content based on predefined search queries related to cybersecurity incidents.
    - The scraping process involves automated browsing, content extraction, and classification.
    - Relevant incidents are summarized and stored in the PostgreSQL database.
3. Frontend Display:
    - The frontend makes API calls to retrieve the latest incidents from the backend.
    - The incidents are displayed dynamically in the IncidentsCard component, allowing users to view summaries and access detailed articles.
4. Insights Generation:
    - The backend periodically analyzes the stored incident data to identify trends and generate insights.
    - These insights can be visualized in future iterations of the application, providing users with a better understanding of the cybersecurity landscape.

4. Insights and Analytics

CyberScope aims to provide users with valuable insights derived from the aggregated incident data. The backend performs analytics to present information such as:

- Trends in Cybersecurity Incidents:
    - Analyzes the frequency of incidents over the past month, categorized by type (e.g., breaches, malware attacks).
    - Visual representation of trends (e.g., line graphs or bar charts) can be implemented in future updates.
- Incident Categorization:
    - Classifies incidents based on severity, type, and source, allowing users to filter information according to their interests.
- User Engagement Metrics:
    - Tracks user interactions with the application, such as the most viewed incidents or sections, to tailor content and improve user experience.

5. User Experience and Interface Design

The user experience (UX) of CyberScope is a critical aspect of the project. The design focuses on simplicity, accessibility, and responsiveness to ensure users can easily navigate and access information. Key design principles include:

- Responsive Design:
  - The application is optimized for various devices, including desktops, tablets, and smartphones, ensuring a consistent experience across platforms.
- Intuitive Navigation:
  - Clear navigation menus and sections help users find the information they need quickly.
- Visual Hierarchy:
  - Important information, such as recent incidents and educational resources, is prominently displayed to capture user attention.
- Engaging Visuals:
  - Use of images, icons, and infographics to enhance the understanding of complex cybersecurity concepts.

5. Tools and Technologies

- **Programming Languages**: HTML, CSS, JavaScript, Python
- **Web Development Frameworks**: ReactJS for frontend development, NodeJS for backend processing
- **Classifier**: Naïve Bayes Classifier
- **Web Scraping**: Selenium for data extraction
- **Data Processing**: Node Summery
- **Databases**:PostgreSQL for structured data storage and management.

7. FlowChart Diagram:

fig. Workflow Diagram of CyberScope

Future Enhancements

To ensure CyberScope remains relevant and valuable to users, several enhancements and features are planned for future iterations of the application:

- User Accounts and Personalization:
  - Implement user authentication to allow users to create accounts, save preferences, and receive personalized content based on their interests.
- Real-Time Notifications:
  - Introduce a notification system to alert users about new incidents or updates related to their specified interests.
- Community Features:
  - Develop a forum or discussion board where users can share experiences, ask questions, and discuss cybersecurity topics.
- Advanced Analytics Dashboard:
  - Create a dedicated dashboard for users to visualize trends and insights in cybersecurity incidents, allowing them to explore data interactively.
- Educational Resources:
  - Expand the content library to include articles, videos, and tutorials on cybersecurity best practices, threat mitigation strategies, and response planning.

8. Conclusion

This project is poised to provide significant value to NCIIPC and other stakeholders responsible for safeguarding India's Critical Information Infrastructure. By delivering real-time, actionable intelligence on cyber threats, the platform will enhance the nation's ability to anticipate, detect, and respond to cyber incidents, thereby strengthening national security.

Roll No	Name of Students	Name of Mentor
17	Vaidehi Chavan	Prof. Monika Bagade
30	Arnav Dekate	
46	Paras Sawalkar	
70	Manas Badhani	

Approved By

(Dr Rashmi Welekar)	**(Prof. Monika Bagade)**	**(Prof. Chanchal Dahat)**
Program Coordinator	**Mentor**	**Project Coordinator**