AI-Enabled Cyber Incident & Safety Web Portal for Defence

Mr C K Navinkumar, Ms Dr. M. USHA DEVI M.Sc., M.Phil., Ph. D., NET,SET
[1]Student, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore
[2]Assistant Professor Department of Computer Science, Rathinam College of Arts and Science, Coimbatore.

Abstract:

Cyber threats such as phishing, malicious links, identity theft, and social engineering increasingly target defence personnel and their families. Existing cyber crime portals do not prioritize defence-related complaints and often rely on manual processing, causing delays in threat response. This work proposes an AI-Enabled Cyber Incident & Safety Web Portal for Defence, which combines cyber complaint reporting, keyword-based AI threat detection, secure database storage, and a CERT admin monitoring dashboard in one integrated system. The portal analyzes suspicious messages using rule-based NLP detection and provides real-time alerts to users. The system is implemented using Flask, SQLite, HTML, and CSS, and deployed as a web application with centralized monitoring through a CERT dashboard.

Keywords: Cyber Security, Phishing Detection, CERT, AI Threat Detection, Flask, Cyber Incident Portal, Defence Security

1. INTRODUCTION

Cyber attacks targeting defence-linked users have become increasingly sophisticated. Attackers often exploit personal devices, fake messages, malicious URLs, and social engineering tactics to compromise sensitive information. Existing reporting platforms are general-purpose systems and do not offer dedicated monitoring for defence-related threats.This project introduces a dedicated cyber incident portal that enables users to report suspicious content, receive automated threat alerts, and allow administrators to monitor complaints centrally through a CERT dashboard.

The main contributions of this work are:

Development of a defence-focused cyber complaint portal Implementation of AI-based suspicious content detection

Secure complaint storage and monitoring dashboard

Deployment of a working web application for cyber incident management

2. LITERATURE SURVEY

Previous research has shown that AI and machine learning can significantly improve cyber threat detection. Existing phishing detection systems use machine learning, NLP, and URL classification models to identify malicious activity. However, many of these systems focus only on detection and not integrated incident reporting.

Studies on cyber security portals emphasize the need for real-time monitoring, user alerting, and centralized incident response. These findings support the development of an integrated cyber reporting and threat analysis system.

3. DATASET COLLECTION

The dataset used in this project consists of cyber threat-related data collected from various sources for analyzing and detecting suspicious activities. Since the project focuses on identifying phishing messages, malicious links, and cyber fraud indicators, the dataset includes samples of suspicious text patterns and commonly used attack keywords. Data was gathered from publicly available cyber security awareness resources, phishing examples, online threat reports, and manually created sample inputs used for testing and validation.

The collected dataset includes attributes such as message text, suspicious keywords, threat status, timestamp, and complaint ID. Keywords such as *OTP, verify, urgent, click, password,* and *login* were included because they frequently appear in phishing or fraudulent messages. These attributes help the system analyze user-submitted complaints and classify them as safe or suspicious. The dataset was cleaned and organized before being used in the system. Invalid or duplicate entries were removed, and the data was structured in a format suitable for the keyword-based AI detection module. This dataset serves as the

foundation for training and testing the cyber threat detection logic used in the proposed system. In future enhancements, larger real-world cyber threat datasets can be integrated to improve detection accuracy using advanced machine learning models.

4. PROPOSED WORK

The proposed work focuses on developing an AI-Enabled Cyber Incident & Safety Web Portal for Defence to provide a secure and intelligent platform for reporting and detecting cyber threats. The system is designed specifically for defence personnel, their families, and veterans, who may be targeted through
phishing messages, malicious links, identity fraud, or other cyber attacks.The proposed system works in multiple stages. First, users submit suspicious messages or cyber complaints through a web-based interface. The system validates the input and processes the complaint using a keyword-based AI detection module. The AI module analyzes the submitted text by checking for suspicious keywords such as OTP, verify, urgent, click, password, and login, which are commonly associated with phishing or cyber fraud.Based on the analysis, the system classifies the complaint as Safe or Suspicious and immediately provides alerts to the user. All complaints and results are securely stored in the SQLite database for record maintenance and future analysis.The proposed work also includes a CERT (Computer Emergency Response Team) Admin Dashboard, where administrators can view, monitor, and manage all reported incidents. This enables centralized monitoring, faster response, and better cyber threat management.

The overall workflow of the proposed system includes:

1. Complaint Collection
2. Input Validation
3. AI Threat Detection
4. Result Generation
5. Database Storage
6. CERT Dashboard Monitoring

5. SYSTEM ARCHITECTURE

The system architecture defines the overall structure and interaction of the components used in the AI-Enabled Cyber Incident & Safety Web Portal. The proposed system follows a client-server architecture, where users interact with the system through a web interface, and the backend processes requests, performs threat analysis, stores data, and provides access to the admin dashboard.
The architecture consists of five major components: **User Interface, Backend Server, AI Detection Module, Database, and CERT Admin Dashboard**.The **User Interface** acts as the front-end component through which users access the system using a web browser. It provides pages for login, complaint submission, and viewing analysis results. This interface is developed using HTML and CSS to ensure simplicity and ease of use.The **Backend Server**, developed using Python and the Flask framework, handles all user requests and controls the core functionality of the application. It receives user inputs, processes complaint submissions, interacts with the AI module, and communicates with the database.The **AI Detection Module** performs cyber threat analysis using a keyword-based detection algorithm. It scans the submitted complaint for
suspicious words and classifies the input as safe or suspicious. The analysis result is then returned to the user and stored in the database.The **Database (SQLite)** stores all complaint records, including complaint text and threat status. It acts as a central repository for maintaining user-submitted data and supports retrieval of records for monitoring purposes.The **CERT Admin Dashboard** allows administrators to access the system, monitor reported incidents, and manage complaints through a centralized interface. This component helps in threat tracking, prioritization, and response management.The workflow of the system architecture is as follows: the user submits a complaint through the web interface, the backend server forwards the input to the AI detection module for analysis, the result is stored in the database, and the CERT admin can access and monitor the data through the dashboard. This architecture ensures efficient communication between components and supports secure and reliable cyber incident management.

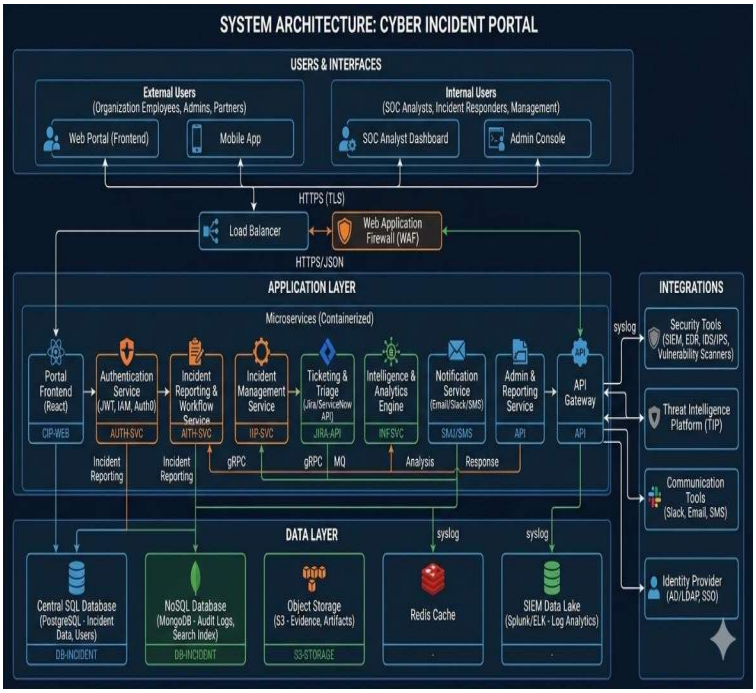

Fig 5.1 System Architecture of Cyber Incident Portal

6. METHODOLOGY

The methodology of the proposed system explains the step-by-step process used for cyber threat detection and incident management. The system begins with **Complaint Collection**, where users submit suspicious messages or links through the web portal. Next, **Input Validation** is performed to ensure the submitted data is valid and not empty.

The complaint is then processed in the **AI-Based Threat Analysis** stage, where a keyword-based detection algorithm checks for suspicious words such as **OTP, verify, click, urgent,** and **password**. Based on the analysis, the system classifies the complaint as **Safe** or **Suspicious** and displays the result to the user.

After analysis, the complaint and its status are stored in the **SQLite database** for record maintenance. Finally, the **CERT Admin Dashboard** allows administrators to monitor and manage all reported incidents.

The methodology follows the sequence: **Complaint Collection → Input Valida**

7. RESULTS

The proposed system successfully analyzes user-submitted complaints and identifies whether the content is safe or suspicious based on keyword-based AI detection. The results show that suspicious messages containing keywords such as **OTP, verify, click, urgent,** and **password** are correctly classified as **Suspicious**, while normal messages are classified as **Safe**.

The system also generates instant alerts to users when suspicious content is detected, helping them take immediate action. All complaints and their results are stored successfully in the SQLite database and displayed through the CERT Admin Dashboard for monitoring and management.

The overall results demonstrate that the proposed system effectively performs cyber threat detection, complaint management, and centralized monitoring, providing a practical solution for cyber incident reporting and response.

8. CONCLUSION

The proposed AI-Enabled Cyber Incident & Safety Web Portal provides a secure and efficient platform for reporting and detecting cyber threats. The system successfully allows users to submit suspicious messages or links, analyzes them using keyword-based AI detection, and provides alerts when threats are identified.

The inclusion of a CERT Admin Dashboard enables effective monitoring and management of reported incidents. The system improves cyber security awareness, supports faster threat detection, and offers a practical solution for handling cyber incidents related to defence personnel. Overall, the project demonstrates how AI and web technologies can be used to enhance cyber security and incident response.

9. REFERENCES

Here is a sample **References** section for your project (paper format style):

[1] Breiman, L. "Random Forests." *Machine Learning*, vol. 45, pp. 5–32, 2001.

[2] Chen, T. and Guestrin, C. "XGBoost: A Scalable Tree Boosting System." *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785–794, 2016.

[3] Goodfellow, I., Bengio, Y., and Courville, A. *Deep Learning.* MIT Press, 2016.

[4] Stallings, W. *Network Security Essentials: Applications and Standards.*
Pearson Education, 6th Edition.

[5] Scikit-learn Developers. "Machine Learning in Python." Scikit-learn Documentation.

ISSN: **3107-6513**

[6] Python Software Foundation. *Python Documentation.*

[7] Pallets Projects. *Flask Web Framework Documentation.*

[8] SQLite Development Team. *SQLite Documentation.*

[9] OWASP Foundation. *OWASP Top 10 Web Application Security Risks.*

[10] National Institute of Standards and Technology (NIST). *Cybersecurity Framework.*

If your guide expects **references specifically about phishing detection / cyber incident response / CERT**, I can tailor them further.