Prof. Bhoge.S.S, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

CIS: CYBER IMMUNITY SCORE

Project Guide : Prof. Bhoge.S.S
Rohan Pawar ,Kedar Tible, Bhargav Fanse , Suchit Navsare
Tssm's Bhivarabai Sawant College of Engineering and research polytechnic

Abstract- The Customer Interaction System (CIS) is a web-based application developed to enhance the interaction between users and service providers through a centralized digital platform. The primary objective of the system is to simplify user communication, manage service-related activities efficiently, and provide a seamless user experience through an intuitive interface. The system allows users to register, log in, and access a personalized dashboard where they can explore available services, submit requests, and track their interactions. It also includes an administrative module that enables administrators to manage user data, monitor system activities, and handle service requests effectively. The application is developed using modern web technologies such as HTML, CSS, and JavaScript for the front-end interface, along with backend integration for data processing and storage. The system ensures proper data handling, user authentication, and structured information management to maintain reliability and performance. By digitizing the interaction process, the Customer Interaction System reduces manual efforts, improves communication efficiency, and enhances overall system transparency. This project demonstrates the practical implementation of web development concepts and provides a scalable solution that can be further extended with advanced features in the future.

Keywords— Customer Interaction System (CIS) is a web-based platform focused on user registration, login, and personalized dashboards, enabling service browsing, request submission, and interaction tracking. It includes an admin module for user management and activity monitoring, built using HTML, CSS, JavaScript, and backend integration, ensuring secure data handling, efficient communication, reduced manual effort, improved transparency, and scalable system performance.

I. INTRODUCTION

In today's digital world, cybersecurity has become a critical concern due to the rapid increase in online threats such as phishing attacks, data breaches, and unauthorized access. Users often lack awareness and tools to monitor their digital security, which can lead to serious risks including data loss and identity theft. Therefore, there is a growing need for an integrated system that can help users analyze, monitor, and improve their cybersecurity status in a simple and effective way.

The Cyber Immunity Score (CIS) is a web-based application developed and app to provide users with a centralized platform for managing and enhancing their digital security. The system includes multiple modules such as user authentication, phishing detection, data breach analysis, OTP-based security features, and a personalized dashboard that displays the user's security status.

The application allows users to register and log in securely, after which they can access various cybersecurity tools. The phishing module helps users identify suspicious links or activities, while the data breach module checks whether user data has been exposed in known breaches. The CIS calculator module evaluates the user's overall security score based on different parameters and provides recommendations to improve their security posture.

Additionally, the system includes features like customer support for user assistance, profile management for handling personal data, and an

admin panel to monitor system activities and manage users. The change password functionality ensures secure account management, while OTP verification enhances authentication security.

The system is developed using modern web technologies such as React for the front-end interface and routing, ensuring a smooth and responsive user experience. The modular design of the application makes it scalable, efficient, and easy to maintain.

Overall, the Cyber Intelligence System aims to create awareness about cybersecurity while providing practical tools for users to protect their digital presence. It reduces dependency on multiple platforms by integrating various security features into a single user-friendly application.

II. LITERATURE REVIEW

The increasing dependence on digital platforms has significantly raised concerns related to cybersecurity threats such as phishing attacks, data breaches, and weak authentication mechanisms. Various research studies and existing systems have attempted to address these issues by providing specialized tools for threat detection, user authentication, and security monitoring. However, most of these systems are either standalone solutions or lack integration of multiple cybersecurity features into a single platform.

Existing phishing detection systems primarily focus on identifying malicious URLs or suspicious email patterns using predefined rules or machine learning techniques. While these systems are effective in detecting known threats, they often fail to provide a user-friendly interface for non-technical users. Similarly, data breach detection platforms allow users to check whether their credentials have been compromised, but they usually operate independently and do not offer additional security recommendations or preventive measures.

Authentication systems using One-Time Password (OTP) mechanisms have been widely adopted to enhance account security. Research indicates that multi-factor authentication significantly reduces the risk of unauthorized access. However, many applications implement OTP only during login processes and do not integrate it with broader security monitoring systems.

III. PROPOSED SYSTEM

The proposed system, Cyber Intelligence System (CIS), is designed as a comprehensive web-based application that provides users with an integrated platform to monitor, analyze, and improve their digital security. The system focuses on combining multiple cybersecurity features into a single, user-friendly interface, reducing the need for separate tools and enhancing overall user awareness.

- The system provides a secure authentication mechanism where users can register and log in to access personalized features. Additional security is ensured through OTP-based verification and password management functionalities.

- A centralized dashboard is implemented to give users an overview of their security status. It displays important information such as security scores, alerts, and recommendations in a structured and easy-to-understand format.

- The phishing detection module allows users to identify potentially harmful links or suspicious activities, helping them avoid online scams and malicious attacks.

- The data breach module enables users to check whether their personal information or credentials have been exposed in known data breaches, increasing awareness about potential risks. order records in real time.

- The CIS calculator module evaluates the user's overall cybersecurity strength by analyzing different parameters and generates a security score. This helps users understand their current security level.

- Based on the calculated security score and system analysis, the recommendation module provides personalized suggestions to improve the user's cybersecurity practices.

- The system includes a customer support module that allows users to raise queries or seek assistance, ensuring better user engagement and problem resolution.

- A profile management module is provided for users to manage their personal information securely, along with a change password feature to maintain account safety.

- An admin module is integrated to allow administrators to monitor system activities, manage users, and ensure smooth functioning of the platform.

- The system is developed using React for the front-end, utilizing routing for smooth navigation between modules, ensuring a responsive and dynamic user experience.

III. METHODOLOGY

The development of the Cyber Immunity Score (CIS) follows a structured and systematic approach to ensure efficient design, implementation, and performance of the application. The methodology focuses on understanding user requirements, designing system architecture, and implementing modular functionalities.

- Initially, system requirements were gathered by analyzing common cybersecurity issues faced by users, such as phishing attacks, data breaches, and weak authentication practices. Based on these challenges, the need for an integrated cybersecurity platform was identified.

- A detailed system design was prepared, including application flow, module structure, and routing architecture. The system was divided into multiple modules such as authentication, dashboard, phishing detection, data breach analysis, CIS score calculation, recommendations, admin panel, and customer support.

- The front-end of the application was developed using React.js, ensuring a dynamic and responsive user interface. Routing was implemented using React Router to enable smooth navigation between different modules like login, dashboard, profile, and security tools.

- Individual modules were developed separately to maintain modularity and scalability. Each module, such as phishing detection and data breach analysis, was designed to perform specific tasks while interacting with the overall system.

- User authentication and security features were implemented, including login, registration, OTP verification, and password management, to ensure secure access to the system.

- The CIS calculator module was developed to evaluate user security levels by processing different parameters and generating a security score. Based on this score, the recommendation module provides suggestions to improve cybersecurity practices.

- The system also includes an admin module for managing users and monitoring system activities, as well as a customer support module to handle user queries and issues.

- After development, the application was tested using functional testing methods to verify each module's performance, navigation flow, and data handling. Errors and bugs were identified and resolved to improve system stability.

- Finally, the system was optimized to ensure smooth performance, better user experience, and scalability for future enhancements.

V. SYSTEM ARCHITECTURE

The Cyber Immunity Score (CIS) follows a modular client–server architecture consisting of three main layers:

Front-End Layer:
Developed using React.js, it provides the user interface for login, dashboard, phishing detection, data breach checking, and other modules.

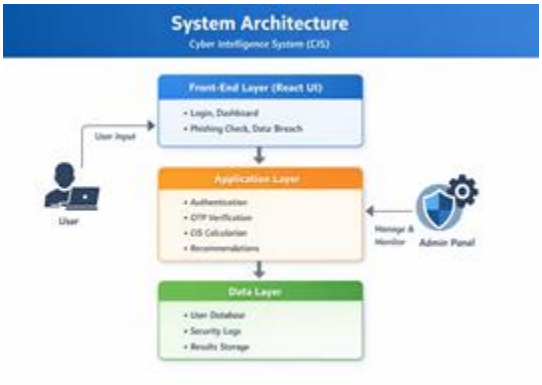
Application Layer:
Handles core functionalities such as authentication, OTP verification, CIS score calculation, recommendations, and module processing.

- **Data Layer:**

Responsible for storing and managing user data, security results, and system information.

Data Layer
The data layer is responsible for storing and managing application data such as user information, security analysis results, and system records. It ensures proper data handling and retrieval whenever required by the application.

If integrated with a backend or database (such as Firebase or other services), this layer supports real-time updates, secure data storage, and efficient data synchronization across modules.



Working Flow of the System
The user accesses the application through the front-end interface (React).

The user logs in or registers using authentication modules.

After login, the user is redirected to the dashboard.
The user can access different modules like phishing detection, data breach check, and CIS calculator.
The application logic processes user inputs and generates results.

Based on results, recommendations are provided to improve security.

Admin monitors system activities and manages users through the admin panel.

VI. APPLICATIONS

- Helps users to monitor and improve their cybersecurity status through a single platform.
- Useful for identifying phishing attacks and avoiding malicious links or websites.
- Enables users to check data breaches and secure their personal information.
- Provides a centralized dashboard to view security score and recommendations.
- Can be used by individuals and organizations to increase cybersecurity awareness.

VII. ADVANTAGES

- Combines multiple cybersecurity features into one system.
- Reduces dependency on different security tools and platforms.
- Simple and user-friendly interface for all types of users.
- Improves awareness about online threats and security practices.

- Enhances account security using OTP verification.

- Modular design makes the system scalable and easy to upgrade.

VIII. CHALLENGES AND LIMITATIONS

- Requires stable internet connection for proper functioning.

- Accuracy depends on available data sources for phishing and breach detection.

- New users may need time to understand all features.

- Limited real-time threat detection without advanced backend integration.

- Currently web-based; mobile application not available.

- System requires regular updates and maintenance for better performance.

IX. FUTURE SCOPE

- Integration of AI/ML for advanced threat detection.
- Real-time alerts for phishing and data breach activities.
- Development of mobile application for Android and iOS.
- Integration with external cybersecurity APIs.
- Advanced analytics and personalized security reports.
- Implementation of multi-factor authentication (MFA).

X. CONCLUSION

The Cyber Intelligence System (CIS) is an effective web-based application designed to improve user awareness and protection against cybersecurity threats. The system provides a centralized platform where users can access features such as phishing detection, data breach analysis, OTP-based authentication, and security score evaluation.

By integrating multiple cybersecurity modules into a single interface, the system reduces complexity and enhances user experience. The use of modern technologies like React ensures a smooth and responsive interface, while the modular design supports scalability and future improvements.
Overall, the CIS project demonstrates a practical approach to solving real-world cybersecurity problems. With further enhancements such as AI integration and real-time monitoring, the system has strong potential to evolve into a complete cybersecurity solution.

REFERENCES

1. React Documentation – https://react.dev
2. JavaScript Documentation – https://developer.mozilla.org
3. Cybersecurity Research Articles and Online Resources
4. Software Engineering – Pressman
5. Software Engineering – Sommerville