International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Infra-Armor - Chrome Extension for Information Infrastructure Security

Papani Dhanush[1], Samarth V Murthy[2], Shrikanta[3], Vishakha Kashyap[4]

Department of Data Science, MVJ College of Engineering, Bengaluru, Karnataka 560067 India

ABSTRACT

With the advent of digitalisation, online security is constantly facing threats from various kinds of cyber-attacks. Cyber-attacks tend to target people, organisations and nations through their various malicious techniques. To combat this, a chrome extension namely Infra-Armor was proposed and developed. This extension acts as a defence mechanism to provide users with five essential functionalities that protect against various web threats prevalent in the digital landscape.

The first functionality, being called Secure Snooze, offers users a dynamic auto-logout mechanism. The second functionality ID Shield protects against fake IDs in social media. While, the third functionality Fraud Guard identifies Fake Forms and Sites, providing users with a vigilant guard against deceptive websites. The fourth functionality Privacy Sentinel focuses on the detection and prevention of data leakage, safeguarding sensitive information from unauthorized exfiltration. The last functionality Vigilance Sheild has a mechanism to detect threats over Anonymous Networks, acknowledging the evolving landscape where anonymity becomes a breeding ground for potential hazards.

Keywords: Online security, cyber-attacks, Chrome extension, Infra-Armor, Machine Learning, Secure Snooze, ID Shield, Fraud Guard, Privacy Sentinel, Vigilance Shield, auto-logout, fake IDs, fake forms, deceptive websites, data leakage prevention, anonymous networks, web threats.

1. Introduction

The introduction highlights the meaning of Information Infrastructure security, while also emphasizing its need in the present cyber era. It further discusses the proposed Chrome Extension and its various useful functionalities and their architecture.

The safeguard of information infrastructure is critical for individuals, businesses, and governments. The evolution of online interactions, data storage, and communication mediums has exposed our information systems to increasingly sophisticated cyber threats. Cyber incidents can be costly, further leading to loss of revenue, recovery expenses, and legal liabilities to businesses. IIS aims to reduce such risks, saving organizations significant revenues by preventing or reducing the impact of such attacks.

As technology continues to proliferate and more systems become interconnected, information infrastructure security becomes imperative to protect data, maintain trust, and ensure the resilience of important services. Advancing in IIS helps safeguard both organizational assets and the broader digital ecosystem, contributing to a more secure and safe digital environment.

The primary objective of this proposed system is to design, develop, and deploy a Chrome extension that seamlessly integrates into the browsing experience, empowering users with real-time threat detection, secure browsing measures, and proactive measures to protect their information assets. The extension combines advanced security algorithms, threat intelligence, and user-friendly interfaces to create a robust defence mechanism that functions transparently, ensuring a secure online environment without compromising user experience.

This paper outlines the architecture, implementation details, and evaluation of Infra-Armor, showcasing its effectiveness in mitigating various web security threats. With its comprehensive functionalities, Infra-Armor aims to be a crucial tool in bolstering web security and preventing any potential cyber-attacks. It offers an inclusive approach to information infrastructure security, protecting users from identity fraud, phishing attacks, data leaks, and network threats. This tool is significant for maintaining privacy, data integrity, and security in today’s digital environment, especially for those who handle sensitive data regularly.

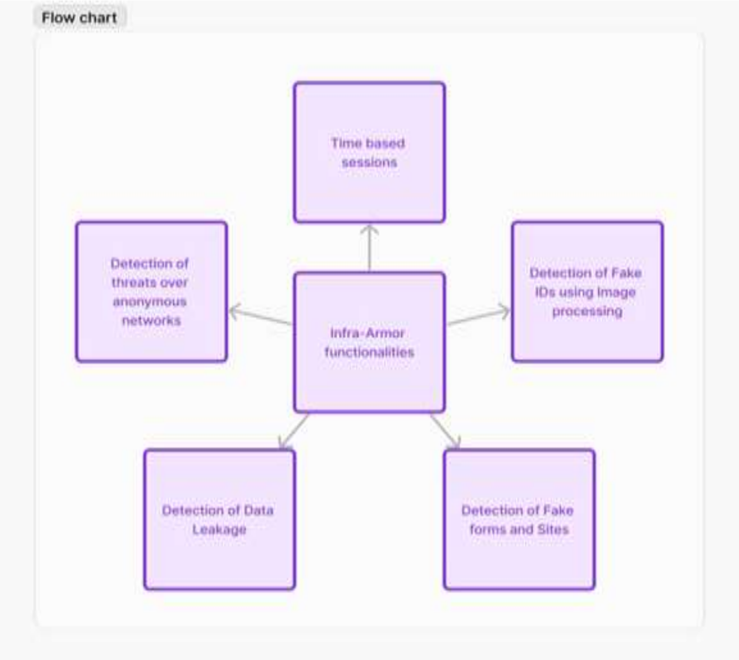

Flow chart
Time based sessions
Detection of threats over anonymous networks
Infra-Armor functionalities
Detection of Fake IDs using Image processing
Detection of Data Leakage
Detection of Fake forms and Sites

Fig. 1 - Functionalities of Infra-Armor

2. Methodology and Analysis

Infra-Armor's methodology follows a structured approach, integrating real-time data processing, user interaction monitoring, and cybersecurity protocols. It details the systematic approach taken to develop its security functionalities and ensure effective protection against cyber threats. Here’s an outline of the methodology, including two data flow diagrams and one operational flow diagram. The data flow diagrams illustrate how Infra-Armor processes user activity data, validates identities, and identifies threats in real time. The operational flow diagram further establishes the seamless integration of these functionalities, ensuring continuous monitoring and prompt user alerts in response to any detected anomalie**s.** These diagrams detail the sequential stages of user authentication, data validation, and the operational flow of threat detection and response, providing a structured framework that focuses on Infra-Armor’s functionality and responsiveness.

Infra-Armor’s methodology combines user-centric design with robust backend processing to ensure security. Through two data flow diagrams, we examined both user authentication and threat detection stages, while the operational flow diagram illustrated the end-to-end process of real-time threat detection and user response. Together, these diagrams highlight the core processes and ensure Infra-Armor remains resilient and responsive to various cyber threats.

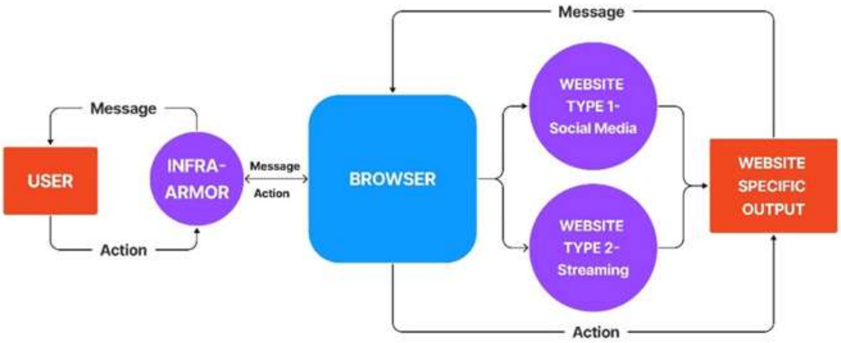


Fig. 2 - Data flow Diagram 1

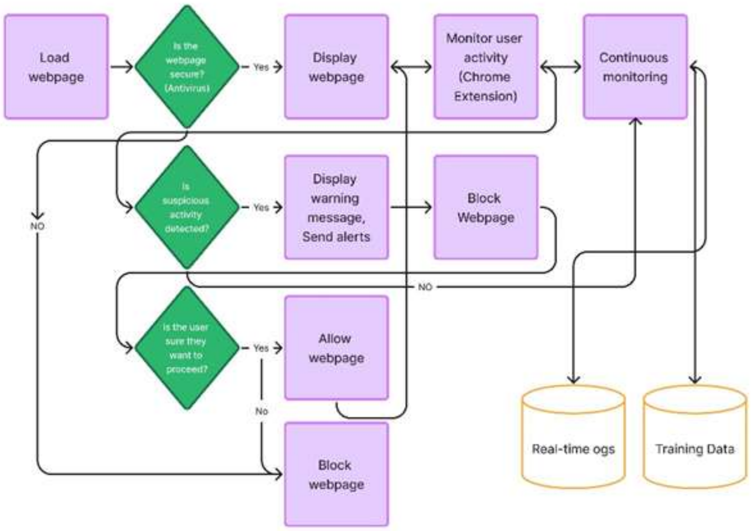

Load webpage
Is the webpage secure? (Antivirus)
Yes
Display webpage
Monitor user activity (Chrome Extension)
Continuous monitoring
NO
Is suspicious activity detected?
Yes
Display warning message, Send alerts
Block Webpage
NO
Is the user sure they want to proceed?
Yes
Allow webpage
No
Block webpage
Real-time ogs
Training Data

Fig. 3 - Data flow Diagram 2

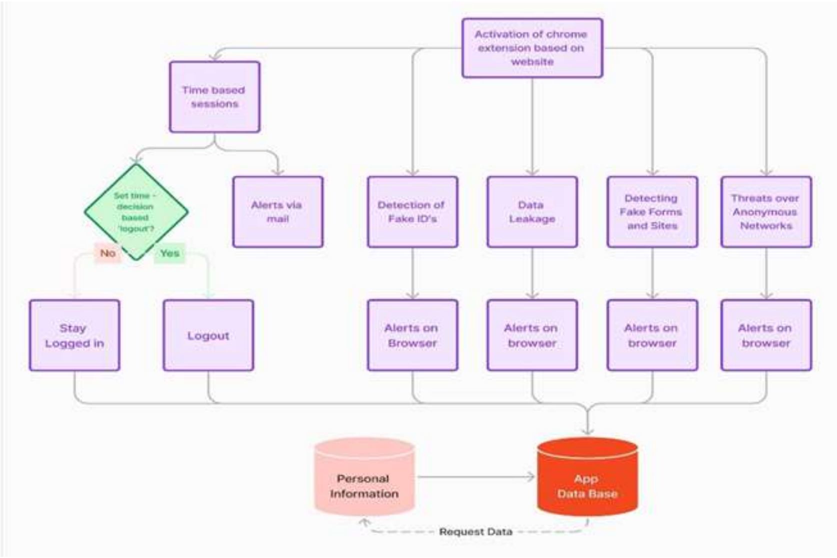


Fig. 4 - Operational flow diagram

Objectives

Develop an Auto logout Feature: Design and implement an auto logout functionality to enhance security by automatically logging users out of online accounts after a specified period of inactivity, preventing unauthorized access.

Identify and Prevent ID Theft on social media: Create a mechanism to monitor and identify potential identity theft on social media platforms, using machine learning and behavioural analysis to detect unauthorized account access and impersonation.

Detect and Mitigate Data Leakage Risks: Design a system to identify, prevent, and mitigate instances of data leakage within online platforms, incorporating monitoring, alerting, and containment strategies to protect sensitive information.

Develop Mechanisms to Protect Against Fake Websites: Build and integrate methods to detect and block access to phishing or fraudulent websites, leveraging domain reputation scoring, visual similarity algorithms, and user alerts.

Secure Data Transmission Over VPN Networks: Enhance data security by implementing advanced encryption and monitoring techniques for data transmitted over VPN networks, ensuring data integrity and confidentiality across network communications.

Evaluate the System’s Overall Security Effectiveness: Conduct comprehensive testing to assess the effectiveness of the combined security features, identifying potential vulnerabilities and areas for improvement to bolster overall online security.

Results

The journey began with a vision to develop an insightful security tool that could protect users not only from conventional risks but also from sophisticated cyber threats that exploit identity vulnerabilities, network weaknesses, and unmonitored sessions. Through extensive research, testing, and leveraging advanced machine learning and behavioral analysis, Infra-Armor was developed to evolve into a cutting-edge browser extension experience, designed to give users control, visibility, and peace of mind in their day to day digital. Each of its functionalities aims to reflect a specific need identified through rigorous analysis of the cyber threat landscape, offering a multi-layered approach to secure the user's digital surrounding in real time. From secure session management to anonymous network monitoring, Infra-Armor represents the commitment to creating a safer and more resilient cyberspace. While arriving at each functionality, we understood the potential risks users face in their mundane web activities. Be it stumbling upon malicious websites or forms or interacting with fake IDs, all the functionalities were built on the basis of a real-life digital situation and designed to provide a real time situation.

Functionality 1: Secure Snooze

The Infra-Armor extension uses a timer to prevent unauthorized access and allows users to set their session time. Users can adjust the time limit using a drop-down menu. An option is provided to keep users signed in until they manually log out. A JavaScript function communicates with the website's session data for a dynamic user experience.

Functionality 2: ID Shield

Infra-Armor searches for similar accounts based on your ID and analyzes their activity for suspicious behavior. It alerts you if it detects a potentially fake or duplicate account and constantly improves its algorithms based on feedback and patterns.

Functionality 3: Fraud Guard

Infra-Armor integrates with IP Address Reputation Services to evaluate website servers and identify malicious IP addresses. Using Recurrent Neural Networks (RNN), it analyzes user activity, detects anomalies, and alerts users promptly. Infra-Armor scans websites for suspicious elements and generates browser pop-up alerts if it identifies any. Users can report false positives and provide feedback to enhance detection accuracy.

Functionality 4: Privacy Sentinel

Infra-Armor uses autoencoder machine learning to analyze user behavior and web interactions. It adapts to changing user behaviors and web structures, monitoring content to address data leakage. It distinguishes between normal and malicious user input, analyzing data transmission patterns in real-time to alert users of potential breaches. Users can customize alerts and trust websites. Incidents are securely logged in encrypted storage to protect privacy and comply with regulations.

Functionality 5: Vigilance Sheild

Infra-Armor is a network monitoring system for anonymous networks. It uses behavioral analysis and recurrent neural networks to identify potential malicious activities and trigger real-time alerts to network administrators or users. The alerts provide comprehensive details on the nature of the threat, affected network nodes, and suggested mitigation strategies. Infra-Armor is a vigilant guardian that fortifies anonymity networks against diverse security risks.

Results from the evaluation of the "Chrome Extension for Information Infrastructure Security" demonstrate its effectiveness in enhancing web security and user experience across various dimensions.

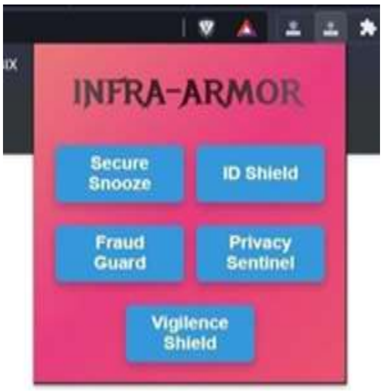
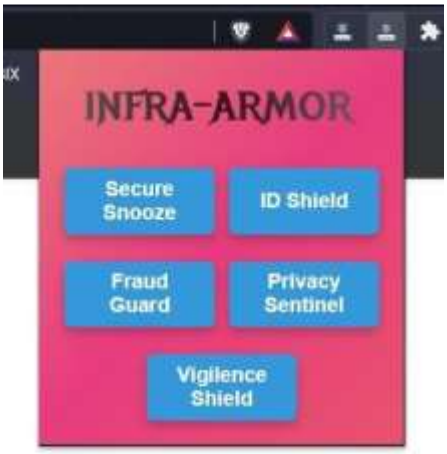
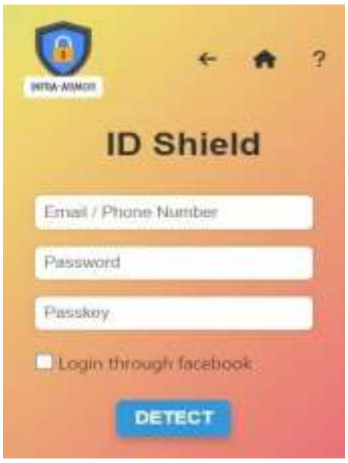
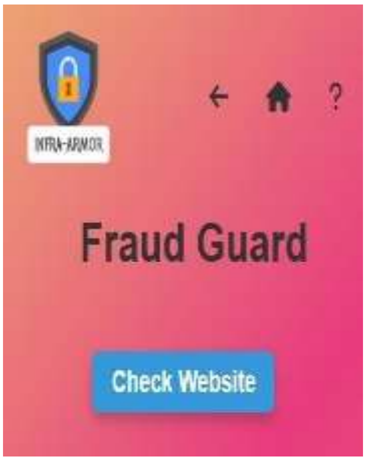
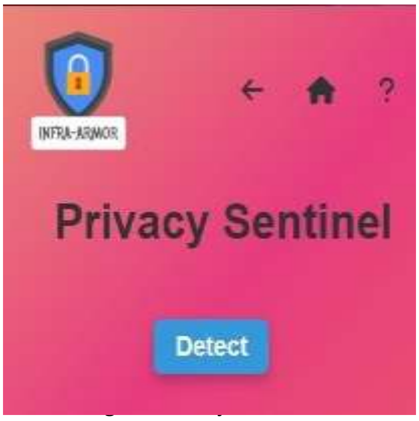


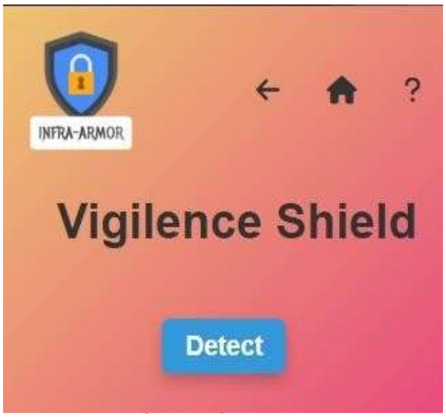
Fig. 5 – Infra-Armor Chrome Extension











Conclusion

This proposed system presents **Infra-Armor**, an advanced Chrome extension designed to strengthen **Information Infrastructure Security** by delivering a suite of protective functionalities targeted at common yet essential cybersecurity vulnerabilities. Infra-Armor's focus on usability and real-time responsiveness accentuates its potential to significantly mitigate cybersecurity risks across a wide range of applications—from personal browsing to organizational security

This research concludes that by providing an intuitive and effective security solution, Infra-Armor serves as a vital tool for individuals and organizations alike, contributing to a safer digital ecosystem and promoting greater user confidence in their online interactions. The findings validate Infra-Armor's design as a robust and scalable security extension, paving the way for future developments and enhancements in the landscape of information infrastructure security. In conclusion, this research substantiates the effectiveness of Infra-Armor as a resilient and adaptable security solution, determining its potential to contribute considerably to the field of cybersecurity.

References

1. Bhrugumalla L.V.S Aditya, Sachi Nandan Mohanty (2023) "Heterogenous Social Media Analysis for Efficient Deep Learning Fake-Profile Identification".

2. Muzzamil Ahmed, Ahmed B. Altamimi, Wilayat Khan, Mohammad Alsaffar, Aakash Ahmad, Zawar Hussain Khan, Abdul Rahman Alreshidi (2023) "PhishCatcher: Client-Side Defense Against Web Spoofing Attacks Using Machine Learning".

3. Lizhen Tang, Qusay H. Mahmoud (2021) "A survey of Machine Learning – Based solutions for Phishing Website Detection".

4. Rasa Bruzgiene and Konstantinas Jurgilas.(2021)"Securing Remote Access to Information Systems of Critical Infrastructure Using Two-Factor Authentication"..