Secure Flow AI-Powered Redirection Blocker for Safe Browsing

Ashwin Biju, Bachelor of Technology in CSE, NCERC
Abijith K, Bachelor of Technology in CSE, NCERC
Azin Raja, Bachelor of Technology in CSE, NCERC
Athul krishna K S, Bachelor of Technology in CSE, NCERC
Mrs. Sajitha A S, Assisstant Professor,Department of CSE(AI AND ML) ,NCERC

1.Abstract

SecureFlow is a browser extension developed to enhance online security by preventing malicious redirections, phishing attempts, and tracking scripts. The system ensures safe browsing by using AI-powered threat analysis and third-party security APIs, including Google Safe Browsing. It provides real-time notifications, maintains a comprehensive history of blocked threats, and supports user customization through whitelisting and history management. The Admin Panel monitors browsing activities and maintains system settings. The Security Engine handles detection and prevention of harmful URLs using machine learning with TensorFlow.js. The User Panel allows users to review history, manage blocked sites, and adjust preferences. By integrating these components, SecureFlow delivers a streamlined, transparent, and secure browsing experience, empowering users to manage their digital safety effectively.

2 .INTRODUCTION

The internet has become an essential part of everyday life, offering convenience, connectivity, and access to an endless array of information and services. However, as users navigate the web, they are increasingly exposed to various security threats that can compromise their personal data, privacy, and overall browsing experience. Among the most persistent and dangerous challenges faced by internet users today are malicious redirections, deceptive advertisements, and unauthorized tracking. SecureFlow is a browser extension specifically designed to address these issues by blocking unwanted redirections and malicious ads in real time, ensuring a safer and more seamless browsing experience. With the rapid evolution of cyber threats, many users unknowingly fall victim to phishing attacks, malware infections, and intrusive tracking mechanisms that exploit weaknesses in traditional browser security features. SecureFlow mitigates these risks by intelligently analyzing and preventing suspicious redirections before they can expose users to harm, empowering individuals with greater control over their online interactions while significantly reducing their vulnerability to cyber threats.

One of the most pressing concerns for online security is the prevalence of phishing and malware threats. Cybercriminals use deceptive techniques to redirect users to fraudulent websites that mimic legitimate platforms, tricking them into revealing sensitive information such as login credentials, banking details, or personal data. These malicious sites often employ sophisticated social engineering tactics to gain the trust of unsuspecting users, leading to severe consequences such as identity theft, financial loss, or unauthorized access to personal accounts. Furthermore, malware-laden websites can automatically download harmful software onto a user' s device without their knowledge, infecting systems with ransomware, spyware, or trojans. SecureFlow addresses these threats by actively monitoring and intercepting redirections to known or suspicious malicious domains, preventing users from falling into these cyber traps.A significant challenge in the fight against malicious redirections is the lack of effective prevention mechanisms in traditional browser security features. While modern browsers implement certain safeguards, they often fail to detect dynamically loaded or obfuscated redirections that bypass built-in security protocols.

Malicious actors continually refine their techniques to evade detection, using complex scripting methods and rapid domain switching to execute attacks before security measures can respond. SecureFlow utilizes AI-driven analysis and third-party security databases to recognize these evolving threats, offering a proactive defense against even the most sophisticated redirection schemes.

Beyond security risks, many redirections serve as tools for unwanted tracking and privacy violations Large advertising networks, data brokers, and even some legitimate websites use redirections as a method to track user activity without explicit consent. These tracking techniques allow advertisers to build extensive profiles on users, gathering data on their interests, behaviors, and browsing habits. In some cases, this data is sold to third parties, raising serious privacy concerns. SecureFlow helps users reclaim their digital privacy by blocking redirections associated with tracking mechanisms, thereby limiting exposure to surveillance-driven advertising and unauthorized data collection.

Finally, one of the most common complaints among internet users is the frustration caused by constant redirections. Whether browsing news articles, shopping online, or accessing social media, users frequently encounter disruptive page redirections that make navigation difficult and unpleasant. Websites that employ excessive redirections create a frustrating experience where users struggle to find the content they were initially searching for. SecureFlow enhances the browsing experience by eliminating these distractions, allowing users to move freely across the web without being unexpectedly redirected to unrelated or unwanted pages.By tackling these critical issues, SecureFlow provides a comprehensive solution for safer and more user-friendly browsing. With its advanced AI-powered detection, real-time blocking, and customizable security features, it empowers users to take control of their online experience. Whether protecting against cyber threats, preserving privacy, or improving website navigation, SecureFlow serves as a vital tool in the ongoing battle against online threats and disruptions.

3. LITERATURE SURVEY

3.1 Author: Dr. Latesh G. Malik, Rohini Shambharkar, Shivam Morey, Shubhlak Kanpate, Vedika Raut

Title: Browser Extension for Fake URL Detection

Contribution:

This paper introduces a browser extension that leverages machine learning to enhance online security. It integrates three key functionalities: malicious URL detection, spam email detection, and network log analysis. The extension uses the LGBM classifier for phishing website detection, achieving 96.5% accuracy.

3.2 Author: Dr. V. R. Kanagavalli, Aarthi B, Pavithra S

Title: College Bus Locator and Tracker

·Contribution:

This paper presents a mobile application, College Bus Locator and Tracker (CBLT), designed for students of Sri Sairam Institutions to track their buses in real time using GPS technology. The app aims to improve transportation efficiency by providing secure and instant updates on bus locations and arrival times.

3.3 Author: Rahul Ganpatrao Sonkamble, Anupkumar M. ongale, Shraddha Phansalkar, Deepak Sudhakar Dharrao

Title: A Secure Interoperable Method for Electronic Health Records Exchange on Cross Platform Blockchain Network

Contribution:

This article proposes a secure, patient-centric method for exchanging Electronic Health Records (EHRs) across different blockchain platforms— specifically Ethereum and Hyperledger Fabric. The method addresses the need for interoperability between distinct blockchain networks, which often operate in isolated environments despite their varying strengths.

4. Technolgy used in Secure Flow :

Software Requirements:

- VS Code: A lightweight but powerful source code editor developed by Microsoft. It supports multiple programming languages and offers extensions, debugging tools, and version control integration.
- Java Script: A versatile, high-level programming language primarily used to create interactive and dynamic content on websites. In this system, it powers the core functionality of the browser extension.

Packages Used :

- TensorFlow: It is an open-source machine learning framework developed by Google, widely used for building and training AI models. It supports both deep learning and traditional machine learning algorithms, making it versatile for a range of applications. With TensorFlow.js, developers can run machine learning models directly in the browser using JavaScript, enabling real- time AI-powered features on the web. It is commonly used in tasks such as image recognition, natural language processing, and predictive analytics.
- Browser-native APIs: are built-in interfaces provided by web browsers that allow developers to interact directly with browser features and system resources. These APIs enable functionalities like accessing the camera and microphone, storing data locally, detecting network status, and manipulating the DOM. They help create rich, interactive web applications without relying on external plugins or tools. These APIs give access to functionality like DOM manipulation, storage, networking, graphics, and hardware access.

5. Proposed System

Improvements Over the Existing System:

intelligence to detect and block online threats in real time.

- Malicious Redirection Blocking: It prevents users from being redirected to harmful or suspicious websites, ensuring a safer browsing experience.
- Phishing Attempt Detection: SecureFlow actively scans for and blocks phishing sites that try to steal user credentials or personal information.
- Script Filtering: It detects and blocks tracking and malicious scripts that compromise user privacy.
- Integration with Trusted APIs: SecureFlow uses trusted third-party services like Google Safe Browsing and VirusTotal for enhanced threat detection.
- Real-Time Alerts: Users receive instant notifications whenever a threat is detected, helping them stay informed and protected.
- User-Friendly Interface: The extension features a clean and intuitive UI that makes it easy for users to navigate and customize settings.
- Activity and Threat History: SecureFlow logs past incidents and alerts, allowing users to view and manage their security history easily

User interface functions:

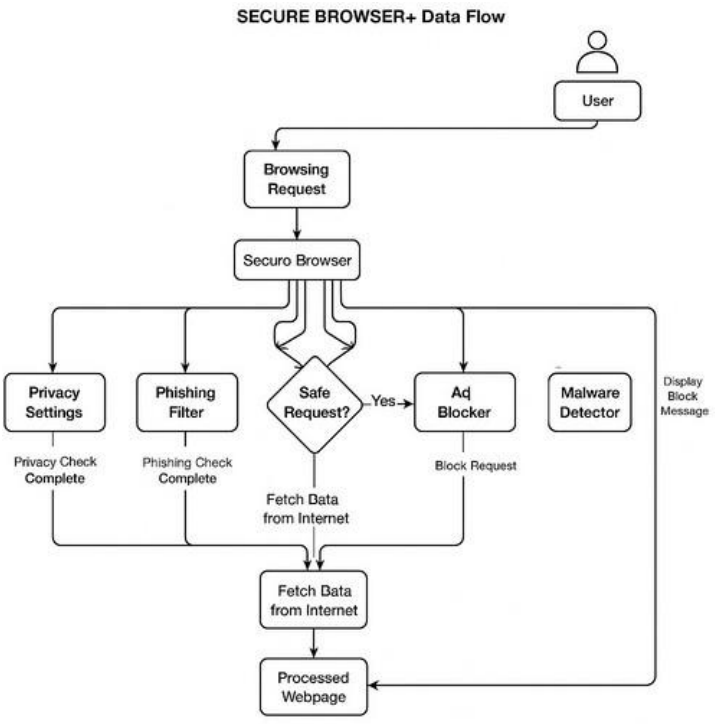
- Block Current Tab – Blocks the website in the current tab.
- Blocked Sites – Shows/manage the list of blocked websites.
- Blocked History – Shows what's been blocked or hides browsing history.

6. Challenges Faced During Implementation

- **TensorFlow.js Integration**:Manifest V3 restricted direct module imports; required offscreen documents and script injection.
- **Content Security Policy (CSP)**: Blocked inline scripts and CDN usage, so all libraries had to be locally hosted.
- **API Rate Limits:** Frequent requests to VirusTotal and Safe Browsing caused throttling; implemented caching to avoid repeat checks.
- **Service Worker Lifecycle**: Automatic termination disrupted model loading; used keep-alive techniques like port connections and storage pings.
- **Redirect Detection:** Some JavaScript/meta redirects bypassed APIs; handled via content scripts and DOM observers

7. System Design

7.1 Architechture of the System



7.2.Module include:

1. **tensorflow/tfjs & tfjs-backend-wasm –** for AI-based redirect detection.
2. **VirusTotal & Google Safe Browsing APIs –** for URL safety checks.
3. **Chrome Extension APIs –** for tab control,storage,notifications, background tasks.
4. **Declarative Net Request API –** for blocking gambling and ad domains.
5. **Offscreen API –** to run AI model securely in the background.

8. Implementation and Results

8.1 System Development

- The project was developed as a Chrome Extension using JavaScript, HTML, and CSS, with integra
- tion of AI and third-party security APIs. The implementation is modular and includes the following components:
- Background Script: Core logic for monitoring URL changes, handling redirection detection, and API communication.
- Content Script: Detects and blocks JavaScript and meta-based redirection at the page level.
- Offscreen Document: Executes the TensorFlow.js AI model in a background thread using WebAssembly (WASM).
- Popup Interface: User-friendly dashboard to view blocked URLs and manually manage site access.
- AI Module: Trained on redirect URL patterns, this model predicts the likelihood of a URL being suspicious using extracted URL features.
- Security APIs Used:
- Google Safe Browsing API to detect phishing and malware.
- VirusTotal API to check URLs against multiple antivirus engines.

- Additional features include:
- Manual blocking/unblocking. Notification
- system with user controls. History tracking
- of all blocked URLs

8.2 System Testing :

1. Environment:
Tested on Google Chrome (Manifest V3) in Windows 10/11.
Simulated both stable and unstable network conditions.
2. Functional Testing:
Verified redirection blocking, AI prediction accuracy, and API responses (VirusTotal & Google Safe Browsing).
Ensured manual block/unblock and history logging work correctly.
3. Integration Testing:
Checked smooth communication between background script, content script, offscreen AI model, and popup UI.
4. Performance Testing:
Measured delay from detection to blocking (minimal latency).
Confirmed low resource usage even under high browsing activity.
5. Security Testing:
Confirmed compliance with Chrome's Content Security Policy.
Ensured no unauthorized script execution or data exposure.
6. User Acceptance:
Tested by users in real-world scenarios.

Results:
SecureFlow successfully detects and blocks malicious redirects, gambling sites, and ad domains in real-time using AI and security APIs. It notifies users instantly, logs blocked URLs, and provides options to manually manage access. The extension runs smoothly on Chrome with accurate threat detection and minimal performance impact

8.3.Results:

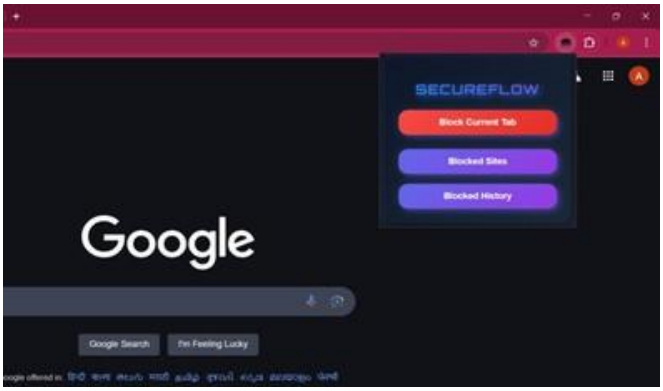


Fig 1. user interface

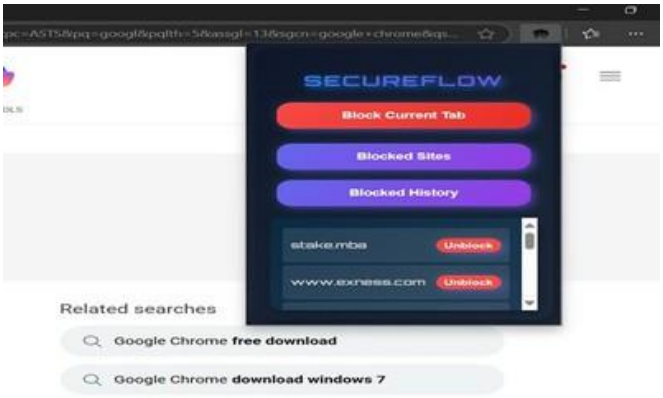


Fig 2. blocked site details

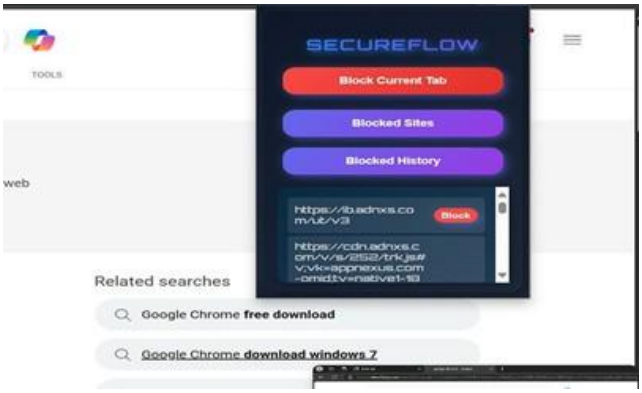


Fig 3.blocked site history

Fig 4.pop up notification

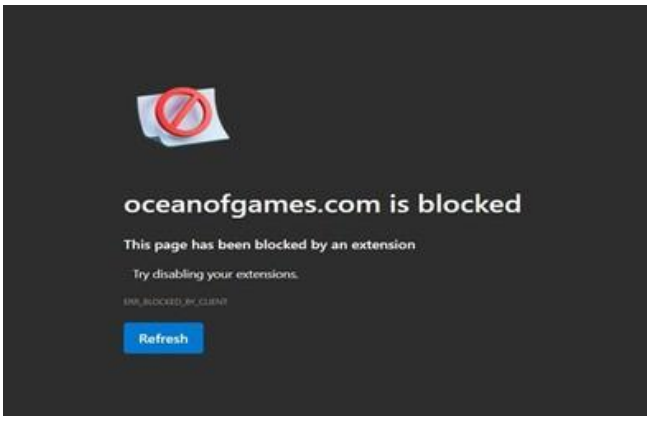


Fig 4. malware detection

9. DISCUSSION AND ANALYSIS

9.1 Advantages of SecureFlow:

- Blocks malicious redirects and phishing links in real-time.
- Integrates AI with trusted security APIs for enhanced detection.
- Provides user control with manual block/unblock options.
- Logs blocked URLs for easy review and tracking.Lightweight and runs efficiently as a browser extension.

9.2 Future Work

- Add support for image-based phishing detection using CLIP or Vision AI.
- Extend compatibility to other browsers like Firefox and Edge.
- Enable auto-updating of AI models via cloud services.Introduce a real-time threat analytics dashboard.
- Implement customizable filters and domain blocklists

10. ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my Mentor Mrs. Soumya T for their invaluable guidance, encouragement, and continuous support throughout the development of this project. Their expertise and insightful feedback played a crucial role in enhancing my understanding and improving the project's quality. I extend my heartfelt thanks to my team members for their dedication, teamwork, and commitment, which were instrumental in successfully implementing the Procurement Management System. Their contributions in various aspects of design, development, and testing greatly enriched the project. I am also thankful to Nehru College of Engineering and Research Centre, Thiruvillamala for providing the necessary resources and a conducive learning environment, enabling me to explore and apply my technical knowledge effectively. Finally, I deeply appreciate the unwavering support and encouragement from my family and friends, whose motivation kept me inspired through out this journey. This project has been a

DDsignificant learning experience, and I am truly grateful to everyone who contributed to its successful completion.

11. CONCLUSION

The SecureFlow project successfully demonstrates the design and development of an AI-powered browser extension focused on enhancing user safety by detecting and blocking malicious redirections in real-time. With the increasing number of phishing attacks and deceptive links on the internet, this tool provides a crucial layer of protection for users, especially those unaware of underlying web threats.By integrating modern technologies such as React for the front-end, Node.js for development support, and various JavaScript libraries for API handling and UI enhancement, the system achieves both functionality and usability. The AI module intelligently evaluates suspicious links and takes immediate action to prevent potential harm, thereby creating a safer browsing experience.The project not only addresses a real-world problem but also showcases the effective application of system analysis and design principles. Overall, SecureFlow contributes to the growing need for proactive cybersecurity solutions and stands as a reliable tool for safe and secure web navigation.

12. REFERENCES

1. "Next Generation of Phishing Attacks using AI powered Browsers"
Author : Akshaya Arun
https://arxiv.org/pdf/2406.12547
2. "Prevention of phishing attacks using AI-based Cybersecurity Awarenes Training,"
Author : M. F. Ansari, P. K. Sharma, and B. Dash
https://www.researchgate.net/publication/362112009_Prevention_of_Phishing_Attacks_Using_AI-Based_Cybersecurity_Awareness_Training
3. "Phishing website detection based on supervised machine learning with wrapper features selection,"
Author : W. Ali https://www.researchgate.net/publication/320131222_Phishing_Website_Detection_based_on_Supervised_Machine_Learning_with_Wrapper_Features_Selecti on
4. "A novel approach for phishing urls detection using lexical based machine learning in a real-time environment," Author : B. B. Gupta et al
https://www.sciencedirect.com/science/article/abs/pii/S0140366421001675
5. "Phishing URL detection using machine learing methods,"
Author : S. H. Ahammad et al
https://www.researchgate.net/publication/365790574_Phishing_URL_detection_using_machine_learning_methods