IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 8, March 2025

Virus Detection and Prevention Tool for Browser

Shubham Pisal[1], Nihar Patil[2], Vedant Naik[3],Sujata Gawade[4]
Students, Department of Computer Technology1,2,3
Lecturer, Department of Computer Technology4
Bharati Vidyapeeth Institute of Technology, Navi Mumbai, Maharashtra, India

Abstract: *Browsing speed, user experience, and privacy. Ads such as pop-ups, banners, and autoplay videos slow down webpages and consume bandwidth, while tracking technologies monitor user behavior without consent. Secure-Block is a browser extension designed to eliminate these issues by blocking intrusive ads and trackers, ensuring a cleaner, faster, and more private browsing experience. It utilizes content filtering, regularly updated block lists, and customizable filtering rules to effectively detect and remove unwanted ads. Additionally, users can whitelist trusted websites, balancing ad-free browsing with content support. Developed using JavaScript, JSON, HTML, and CSS, Secure-Block is open-source and prioritizes privacy by not collecting user data. This paper examines the technical framework, implementation, and impact of Secure-Block in enhancing online security and user satisfaction..*

Keywords: Ad blocking, tracker blocking, online privacy, content filtering, browser extension, web security, internet performance, open-source software

I. INTRODUCTION

In today's digital world, online advertisements have become a common yet intrusive part of web browsing. While ads help support free content, they often disrupt the user experience with pop-ups, banners, and autoplay videos that slow down page loading times and consume bandwidth. Additionally, many websites deploy trackers that collect user data without consent, raising privacy concerns. These factors have led to a growing demand for ad-blocking solutions that offer a cleaner, faster, and more private browsing experience.

Secure-Block is a browser extension designed to tackle these challenges by blocking intrusive ads and tracking technologies. It leverages content filtering, regularly updated block lists, and custom rule support to ensure effective ad detection. Users can customize their experience through whitelisting options, real-time blocking statistics, and personalized filter settings. Developed using JavaScript, JSON, HTML, and CSS, Secure-Block prioritizes user privacy by operating as an open-source, data-free solution. This paper explores the technical framework, functionality, and impact of Secure-Block in enhancing web browsing efficiency and security.

II. LITERATURE SURVEY

The growing presence of online advertisements and tracking technologies has led to extensive research on ad-blocking solutions and their impact on user experience, privacy, and web performance. Studies have shown that ad-heavy websites significantly slow down page loading times, increase bandwidth consumption, and degrade overall browsing efficiency. Ad-blocking technologies, such as browser extensions and script-based filtering methods, have been developed to address these issues. Popular solutions like uBlock Origin and Adblock Plus use predefined filter lists to remove intrusive ads, leading to faster load times and a smoother browsing experience. However, many websites implement anti-adblock mechanisms to bypass these solutions, forcing researchers to explore more adaptive and customizable blocking techniques.

Tracker blocking has also gained attention, as many websites deploy third-party tracking scripts to monitor user behavior and collect personal data without consent. Research highlights the risks associated with these practices, including targeted advertising, data breaches, and privacy violations. While several ad blockers incorporate tracker-blocking features, some have been criticized for collecting user data for monetization purposes. Secure-Block aims to

ISSN 2581-9429 IJARSCT
DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 8, March 2025

overcome these challenges by providing an open-source, privacy-focused browser extension that does not collect user data. By leveraging real-time content filtering, customizable blocking rules, and regularly updated block lists, Secure-Block enhances privacy protection and web performance while ensuring users have control over their browsing experience.

III. METHODOLOGY

The development of Secure-Block follows a structured approach to ensure efficient ad and tracker blocking while maintaining user privacy. The methodology consists of four key stages: requirement analysis, design and development, implementation, and testing.

In the requirement analysis phase, a detailed study of existing ad-blocking solutions was conducted to identify their strengths and limitations. Research was focused on improving ad detection accuracy, reducing resource consumption, and maintaining user privacy. Based on this analysis, the core functionalities of Secure-Block were defined, including ad blocking, tracker blocking, whitelisting options, and real-time statistics.

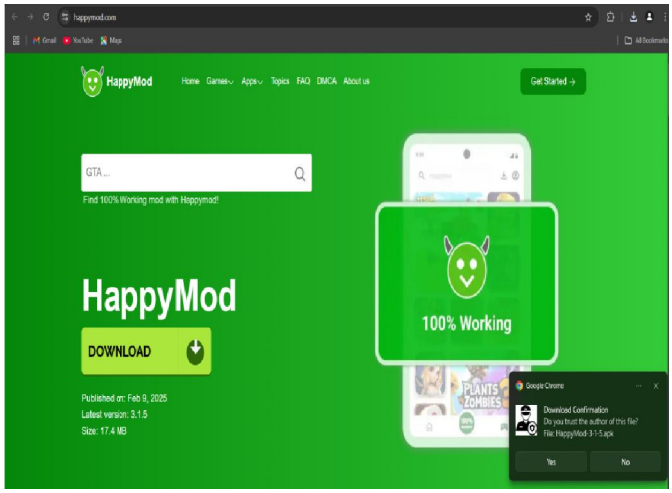
During the design and development phase, Secure-Block was built using JavaScript, JSON, HTML, and CSS. The extension's core logic relies on content filtering techniques to analyze web page elements in real time and block unwanted advertisements. A regularly updated block list is integrated to ensure comprehensive ad detection. Additionally, custom rule support allows users to define their own blocking preferences. The user interface was designed to provide a seamless experience with options for enabling or disabling blocking, managing whitelisted sites, and viewing real-time statistics of blocked ads.

The implementation phase involved integrating the extension with modern web browsers and ensuring compatibility across different platforms. Secure-Block was designed as a lightweight extension that minimizes CPU and memory usage, ensuring optimal performance without slowing down web browsing.

Finally, the testing phase included rigorous functional and performance testing to validate the extension’s effectiveness. Real-world browsing scenarios were used to measure ad-blocking accuracy, page loading speed improvements, and resource consumption. Usability testing was also conducted to refine the interface and enhance user experience. The extension was tested against various anti-adblock mechanisms to improve its resilience.

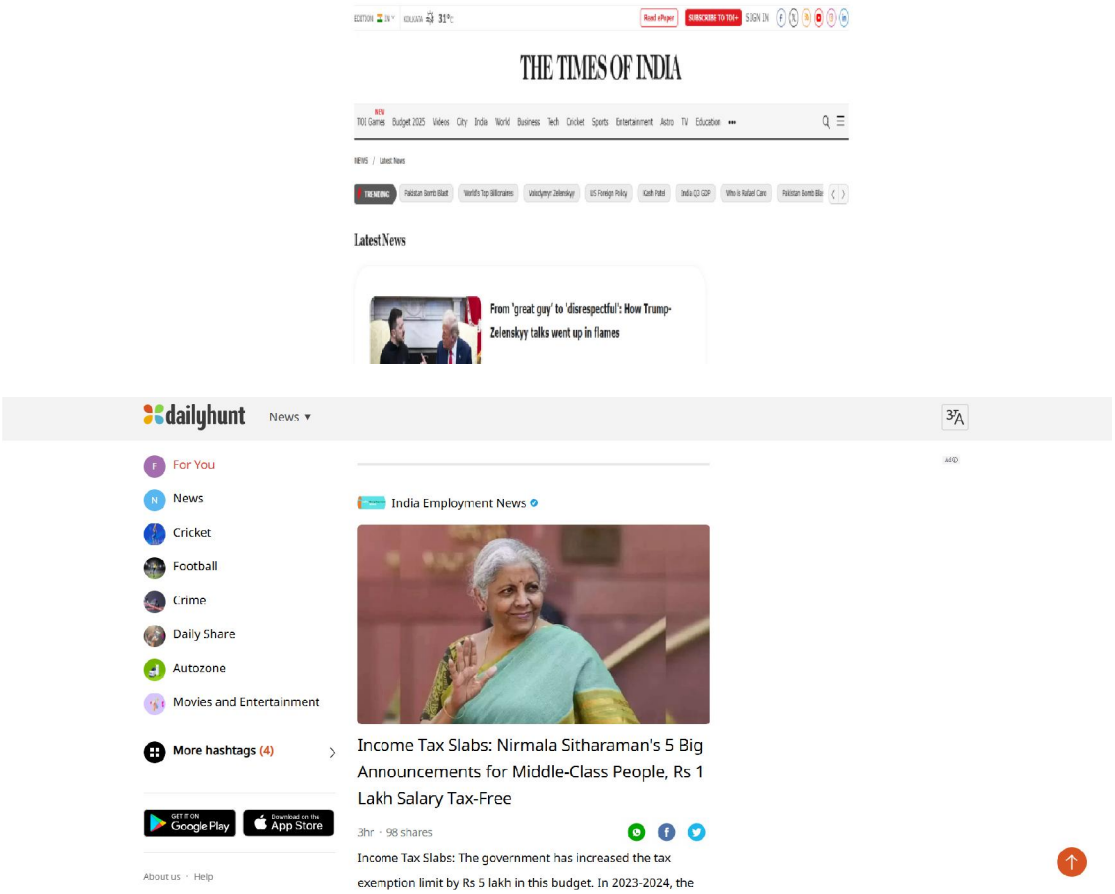
This structured methodology ensures that Secure-Block is an efficient, privacy-focused, and user-friendly solution for blocking intrusive ads and trackers while maintaining web performance.

IV. RESULT



ISSN 2581-9429 IJARSCT
DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 8, March 2025



V. CONCLUSION

Secure-Block addresses the growing concerns of intrusive advertisements and online tracking by providing an efficient and privacy-focused browser extension. By utilizing content filtering, regularly updated block lists, and customizable rules, it ensures a seamless and ad-free browsing experience without compromising performance. Unlike some ad blockers that collect user data, Secure-Block is designed as an open-source, lightweight solution that prioritizes user privacy. Testing has demonstrated its effectiveness in enhancing browsing speed, reducing bandwidth consumption, and improving security. As online advertising and tracking methods continue to evolve, future enhancements to Secure-Block will focus on adaptive filtering techniques and improved resistance against anti-adblock measures, ensuring a more secure and user-controlled browsing environment.

VI. ACKNOWLEDGEMENT

We would like to express our heartfelt gratitude to our mentors and professors for their invaluable guidance, constructive feedback, and continuous encouragement throughout this research on Secure-Block. Their expertise in web security and ad-blocking technologies has played a crucial role in shaping our understanding and refining our approach.

ISSN 2581-9429 IJARSCT
DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 8, March 2025

Their insights have helped us navigate challenges and develop a more effective and privacy-focused solution for blocking intrusive advertisements and trackers.

We also extend our appreciation to our peers and colleagues for their valuable suggestions and discussions, which contributed to improving the functionality and performance of Secure-Block. Additionally, we acknowledge the contributions of researchers and developers in the field of online privacy, whose work has provided a strong foundation for this study. Lastly, we are deeply grateful to our families and friends for their unwavering support and motivation, which have been instrumental in completing this research successfully.

REFERENCES

[1]. Barth, S., & de Jong, M. D. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior. *Telematics and Informatics, 34*(7), 1038-1058.

[2]. Englehardt, S., & Narayanan, A. (2016). Online tracking: A 1-million-site measurement and analysis. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*, 1388-1401.

[3]. Ikram, M., Kaafar, M. A., Berkovsky, S., & Buyukkayhan, B. (2017). The anatomy of browser-based ad-blocking. *Proceedings of the Web Conference 2017*, 1-10.

[4]. Pujol, E., Hohlfeld, O., & Feldmann, A. (2015). Annoyed users: Ads and ad-block usage in the wild. *Proceedings of the 2015 Internet Measurement Conference*, 93-106.

[5]. Gervais, R., Shokri, R., Singla, A., & Lenders, V. (2016). Quantifying web adblocker privacy. *Proceedings on Privacy Enhancing Technologies, 2016*(1), 41-60.

[6]. Lerner, A., Simpson, A., Kohno, T., & Roesner, F. (2016). Internet Jones and the Raiders of the Lost Trackers: Analyzing and defending against browser fingerprinting. *25th USENIX Security Symposium*, 513-530.

[7]. Merzdovnik, G., Buhov, D., Neuner, S., Huber, M., Schrittwieser, S., & Weippl, E. (2017). Block me if you can: A large-scale study of tracker-blocking tools. *IEEE European Symposium on Security and Privacy (EuroS&P)*, 319-333.

[8]. Nithyanand, R., Khattak, S., & Gill, P. (2016). A measurement study of tracking in paid and free apps. *Proceedings of the 2016 Network and Distributed System Security Symposium (NDSS 2016)*, 1-15.

[9]. Roesner, F., Kohno, T., & Wetherall, D. (2012). Detecting and defending against third-party tracking on the web. *USENIX Symposium on Networked Systems Design and Implementation (NSDI '12)*, 155-168.

[10]. Zhang, X., Ruan, Y., Komanduri, S., Acquisti, A., Cranor, L. F., & Gummadi, K. P. (2013). Measuring and analyzing the impact of anti-tracking browser extensions. *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security*, 1-13.

ISSN 2581-9429 IJARSCT

DOI: 10.48175/568