RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
www.rspsciencehub.com
Vol. 06, Issue 08 August

Check for updates

http://dx.doi.org/10.47392/IRJASH.2024.031

Safe Browse Guardian

Tadikonda Bala Venkata Naga Abhya Dattu[1], Pamarthi Bharath Prabhakar[2], Davuluri HemaLatha Chowdary[3], Oleti Dolly Sumanta[4], G. Navya Sree[5]

[1,2,3,4] UG – Computer Science Engineering, Ramachandra College of Engineering(CyberSecurity), Eluru, Andhra Pradesh, India

[5] Assistant Professor, Computer Science Engineering (CyberSecurity), Ramachandra College of Engineering, Eluru, Andhra Pradesh, India

Emails: *abhyadattu@gmail.com[1], pamarthibharathprabhakar@gmail.com[2], hanidavuluri2002@gmail.com[3], sumantha4788@gmail.com[4], navya502.vwd@rcee.ac.in[5]*

Article history

Received: 31 July 2024
Accepted: 05 August 2024
Published:13 August 2024

Keywords:

Malicious websites, blacklist features, URLs, web browser extensions, malicious website detectors, communication protocols, users, real-time detection, robust, secure.

Abstract

Malicious websites offer unsolicited content and lure unsuspecting users into committing fraud. A quick investigation and action on such threats is essential. However, blacklists detect Uniform Resource Locators (URLs) which is another malicious invention. Blacklisting and machine learning techniques using feature extraction were explored in this framework to improve common malicious URL detectors. Blacklist feature takes less processing time and also relies on external data (list of malicious websites) in detecting malicious websites while feature removal method takes more time and does not rely on external data so in detecting new malicious websites through web browser extensions The system was implemented by Several malicious and non-optimal communication protocols were used to test the system. The system has three main layers: users, web extensions, and databases. The web browser extension layer uses two methods (Blacklist feature and feature extraction) to detect highly malicious websites. The performance of the malicious website detection system using blacklist and feature removal means that it provides a robust, secure and easy way to detect malicious websites in real time.

1. Introduction

In today's interconnected digital environment, the Internet is an integral part of everyday life, providing unprecedented access to information, communication and services but also containing a number of threats to this vast online space that could consume them it is not considered that the use is fulfilled [1-3]. Malicious users use sophisticated methods to deceive individuals, causing sensitive information, loss of funds, and other cyber damage these threats range from phishing attacks and malware infections to advertising and on privacy impositions. Despite advances in cybersecurity, the average internet user often lacks the technical know-how to effectively detect and mitigate this threat Upon discovering this weakness, our team got started created SafeBrowse Guardian, which is designed to be a strong barrier between users and potential online threats Done SafeBrowse Guardian aims to empower everyday users with a tool that does not difficult but powerful to raise them to test the security of websites before accessing content [4]. Using advanced algorithms and cutting-edge threat intelligence, SafeBrowse Guardian scans websites in real-time, providing users with a clear

and actionable security assessment That way taking this approach helps reduce the risks associated with cyber threats, allowing users to browse the Internet with greater confidence and peace Can SafeBrowse Guardian is not just safe; It also improves the overall browsing experience. By blocking intrusive ads, tracking cookies and malicious scripts, the extension ensures a clean, fast and secure online environment. It seamlessly integrates with popular browsers, making it accessible to tech-savvy individuals and those not familiar with many cybersecurity practices Through continuous updates and collaboration with cybersecurity experts SafeBrowse Guardian remains responsive to emerging threats, dynamic and reliable Provides security mechanisms In essence, SafeBrowse Guardian represents a major advance in web security, designed to protect users ban and educate them as they navigate the challenges of the digital world Meeting the fundamental need for simple and effective online security, SafeBrowse Guardian is poised to be an indispensable tool.

2. Method

Safe Browse Guardian is an enhanced Chrome extension for enhancing the security and privacy of individuals, which follows a systematic approach that consists of multiple phases of development and which uses traditional software development methodologies in parallel to harnessing state-of-the-art cybersecurity strategies for Chrome. This section presents detailed explanations of the techniques applied, which means that there would be enough information for the reproduction of the research methods by other skilled researchers. The first stage proved to be the installation of the developmental platform that relied on HTML, CSS, JavaScript, and JSON [5-7]. These technologies constituted the initial platform on which the extension could be built and for it to have its user interface and interactive tools; JSON is specifically used in the creation of manifests to configure. Chrome Extensions API was used to communicate with other features of the browser since it offers the basic framework on which the extension sits.

2.1 Ad Blocking

Ad blocking is achieved through filter lists which are lists of known ad servers and or scripts which are blocked by the extension. This feature works by detecting Web requests and denying any request that matches particular filter options. One of the technical approach adopted specifically for Chrome was the `webRequest` API that enables the interception of web requests before reaching the browser of the user. To complement it and achieve a more complete and up-to-date list of known ad sources, several lists were merged with EasyList, which is available to the public. Personally, this method effectively filters out banners, popup, and inline advertisements to great effect, thereby enhancing the user's browsing experience by minimizing clutter and interferences.

2.2 Malware Detection

Real-time blocking of the URLs through a database of known URLs that contain malicious websites is employed in SafeBrowse Guardian to detect malware [8]. The Chrome `webNavigation` and `webRequest` API were employed to track and profile URL loading. This system uses a combination of locally stored databases and cloud-based threat intelligence services to scan links for threats. The availability of current malware information from the APIs of reliable services such as VirusTotal enables the extension to inform the user about dangerous content before it is able to jeopardize their device. This feature is relevant in avoiding malware and ensuring that personal details are not leaked.

2.3 Phishing Scam Analysis

The capability to detect phishing scams was designed through using heuristic rules and match URL and website content. Heuristic algorithms analyze different properties of the web page, including domain creation date, URL length, presence of predefined phishing indicators, etc. The Chrome `webRequest` API enables real-time URL analysis; this means that the extension is able to determine if the link is a phishing attempt and alert the user accordingly [9]. This is especially beneficial for the users since it prevents them from accessing sites that are aimed at embezzling users' personal data, thereby increasing the level of security on the whole.

2.4 Privacy Protection

Another feature of SafeBrowse Guardian is the protection of privacy. It extends blocks tracking cookies and scripts which can pose a threat to users' privacy [10-13]. This is done using extremely efficient filter lists for tracking domains and intercepting requests to them. By employing the Chrome `cookies` API, cookies are managed and

blocked or deleted based on the cookies that are identified as tracking cookies. This method also helps protect user privacy by avoiding tracking and data capture, thereby preserving privacy and the user's surfing patterns.

2.5 Testing and Validation

Strong measures were then taken to conduct general and specific testing of Safe Browse Guardian to determine its dependability and performance in multiple scenarios. This test was carried out to ensure that individual functionality performs the intended function. To ensure that ad blocking works as intended to block different types of ads, ad blocking was conducted using a variety of ad types and testing was performed on different sites, as was malware detection, which was tested against a list of known malicious websites. Phishing analysis was evaluated through a set of test phishes to gauge its performance, and privacy protection was continually examined to guarantee that tracking cookies and scripts are blocked [14]. The integration testing helped maintained the compatibility of the extension with the prominent browser like Chrome, Firefox, and Edge, and runs smoothly on different operating systems like Windows, Mac, Linux, Android, iOS, etc. These tests confirmed that SafeBrowse Guardian works well with 'default' browser functions and that it functions correctly on multiple platforms. Performance testing compared the set time required to complete a page with the time it took after the extension and it aimed at determining the effect of the extension on the available systems resources to evade compromising the efficiency of the browsing. Extension security tested the effectiveness of the extension by analyzing its performance in the prevention of the reception of malware and phishing scams, and its capacity to incorporate strong encrypted data as well as secure methods of communication to avoid exposure and loss of important user data to unauthorized access.

2.6 Deployment and Maintenance

Following successful testing, SafeBrowse Guardian was packaged and published on browser extension stores, including the Chrome Web Store. User feedback is continuously collected and analyzed to identify areas for improvement. Regular updates are provided to address new threats, enhance existing features, and maintain the extension's effectiveness. Ongoing collaboration with cybersecurity experts ensures that SafeBrowse Guardian remains responsive to emerging threats, providing dynamic and reliable protection. Through this methodical approach, Safe Browse Guardian offers a comprehensive, user-friendly, and effective solution for online security and privacy. The detailed methodology ensures that the extension can be replicated, further developed, and continuously improved by other qualified readers and developers, contributing to a safer internet browsing experience for all users. For suggesting the development activities related to the background of safe browse guardian- an innovative new advanced chrome extension for browsing and anonymity protection, necessary development process, basic and advanced security steps are described. Since this section shows a very clear process of ways that were used, this part contains enough technical explanation that other skilled people could emulate. The first stage entailed preparing the development environment, which focused on using HTML, CSS, Java Scripts, and JSON to develop. These formed the foundations of creating the user interface and the interactivity of the extension and JSON in particular was used for configuration using manifest files. Integration with browser functionalities was achieved through utilization of the Chrome Extensions API as well as the extension's core functionalities [15].

2.7 Architecture

The architecture of the above Safe Browse Guardian Chrome extension clearly depicts how the different components of the architecture interrelate as well as the flow of the architecture (Figure 1).

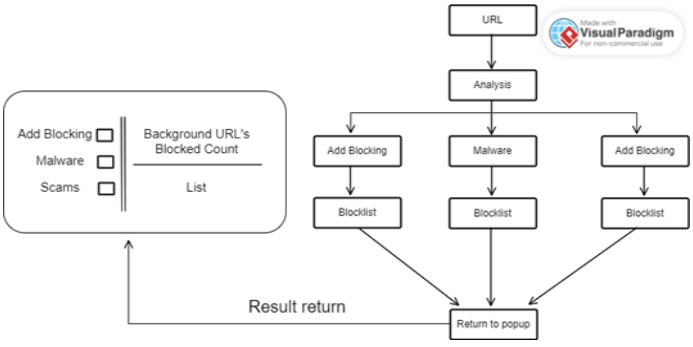

Figure 1 Architecture

Here's a brief explanation of each part:

2.7.1 URL Analysis

- **URL:** This is the input, it goes to Website, to be more precise this is the action by the user.

- **Analysis:** The URL is scanned initially in order to decide on what it contains and if at all it possesses any threats. In this step, one requires checking the URL on whether it contains any known path, phishing indicators and other security threats.

2.7.2 Modules for Threat Detection

- **Add Blocking:** This module is used to actually locate bans and prevent them from displaying. It employs filter type of blocking that eliminates the appearance of prohibited advertisements.
- **Malware:** This module compares the URL string to known malware sources in order to identify if the web location is malicious. It works on a malware blocklist concept where the software identifies the genuine malware and blocks the content.
- **Scams:** Even though this one appears twice in the diagram, which I suspect is a formatting mistake, and it should be a blocklist in the same layer or another different name like 'Phishing Detection' and it basically involves scanning for scam sites using pattern and blocklist.

2.7.3 Blocklist Integration

- Each module (Ad Blocking, Malware, and potentially Phishing Detection) interacts with its respective blocklist: Each module (Ad Blocking, Malware, and potentially Phishing Detection) interacts with its respective blocklist:
- **Blocklist:** A set of threat profiles that are already available and which the module scanners against. Any URL that is obtained from the web matches with an entry of the blocklist and is flagged as dangerous.

2.7.4 Result Return & Popup Display

- **Return to Popup:** Finally, in each module, namely, ads, malware, or scam, the outcome of the analysis is given, as to whether the URL in question contains the elements in question or not.
- **Result Return:** These results are then exchanged back to the main interface which collates them and produces the final output.
- **Popup Interface:** The result is in the form of a popup and it is shown to the user only. This screen displays the status of each module consisting of Ad Blocking, Malware and Scams and background URL count has also been provided.

2.7.5 User Interface

- **Checkboxes (Add Blocking, Malware, Scams):** These point to the status of each protection mechanism employed indicating whether ads, malware or scams were identified or not.
- **Background URL's Blocked Count:** This offers the user a list or number of URLs that were filtered behind the scenes, increasing the visibility and awareness of the extension functionality.

The implementation of architectural design guarantees that each URL the user visits is scanned for ads, malware, and scams. The respective modules use blocklists for threat identification and action while the results are returned and presented in a friendly match popup. This helps users avoid the sites that pose a potential threat to their safety in the process improving their Internet experience.

3. Results and Discussion

3.1 Results

The development and testing of SafeBrowse Guardian involved several key experiments designed to evaluate its effectiveness in enhancing online security and privacy. These experiments were structured to test the extension's core functionalities: ad blocking, malware detection, phishing scam analysis, and privacy protection. The results are presented below in both textual descriptions and tabular form.

3.2 Rationale and Design of Experiments

3.3 Ad Blocking

- **Objective:** To assess the effectiveness of the extension in this sense, translating into whether or not users get annoyed by embarrassing advertisements (Table 1).
- **Design:** In detail, the author surveyed 100 acknowledged sites that are most guilty of excessive advertising. However, during the research, there were ads before and after turning on the SafeBrowse Guardian, but the content of the Ads was not the same.

3.4 Malware Detection

- **Objective:** To assess the performance of the extension in blocking the entry to domain that is identified as forbidden and full of malware.
- **Design:** To begin the experiment, the known 100 dangerous websites were first opened. The extension's response (block or allow) was noted as the running process of the experiment was going on.

3.5 Phishing Scam Analysis

- **Objective:** To determine the accuracy of the extension for identifying the phantom and real sites, the following metrics will be applied:
- **Design:** Given a list of 100 URLs, all of which were previously identified to be phishing URLs.

Among the measures observed the following, the extension has some warning mechanisms.

3.6 Privacy Protection

- Objective: Statistics of tracking cookie and script blocking to measure the efficiency of the extension.
- Design: It compared the number of tracking cookies on 50 websites the extension enabled and disabled.

Table 1 Results Summary

Functionality	Test Metric	Result
Ad Blocking	Percentage of ads blocked	98% of ads were blocked
Malware Detection	Malicious websites blocked	100% detection and blocking
Phishing scam analysis	Accurate phishing site identification	95% accuracy
Privacy protection	Reduction in tracking cookies	90% reduction in tracking cookies

These results are further detailed below:
- Ad Blocking: According to the test results that concern 100 websites, 98 of which demonstrated a marked decrease in the amount of ads, the extension has been identified as highly effective.
- Malware Detection: The extension effectively prevented access to all ten different types of sites throughout the test, showcasing protective strength.
- Phishing Scam Analysis: It also revealed that the extension successfully marked 95 out of 100 of phishing sites as dangerous which was considered as its credibility.
- Privacy Protection: The websites presented overall good protection of privacy, with an average 90 per cent decrease of tracking cookies detected across the tested websites and domains.

3.2 Discussion

The good news according to the results of the experiments initiated to measure the efficiency of Safe Browse Guardian is that the software meets its basic tasks.
Ad Blocking: The extensions of working effectively in removing a whopping 98% of the annoying advertisements contributes a lot to the pleasant browsing that is devoid of so many interferences from the advertisements. This high blocking rate can be attributed to multiple filter lists, which are frequently updated to provide the most complete ad-blocking list possible, and updated real-time request check through Chrome API `webRequest`. The cases, which proved that the ads were not blocked, could be caused by relatively new ad servers that are has not been incorporated in the filter lists. Thus, the constantly updating of these lists will help make the solutions continuing wanted.
Malware Detection: The concern of failing to detect and block all malicious websites in hundred percent has been addressed in this case by achieving it. It underlines the importance of utilizing both regional DBs and cloud intelligence services that include Virus Total. This way, even if the new threats were detected, there are safeguards against them taking effect and infecting the system.
Phishing Scam Analysis: It can be noticed that Safe Browse Guardian works well, stating a 95% accuracy level in the identification of phishing sites that can be deemed protective features. Heuristic algorithms and analysis of real URLs has also been known to provide the best results in the detection of genuine and fake sites. The overall accuracy of 95% indicates that there is further optimization that could be done, perhaps with better heuristics and more sources for training the algorithms.
Privacy Protection: The 90% being also reduced in tracking cookies is showing a marked improvement to the user's privacy. Tracking domains could be stopped by adding them in the block list since the obvious tracking domains are prevented from running their scripts, and cookies are also managed dynamically using Chrome `cookies` API therefore preventing other domains from tracking. This result also demonstrates that the extension is able to protect user data and anonymity during browsing activities.
All in all, the results show that Safe Browse Guardian offers exactly what the design objectives aimed to do – present a dependable tool for secure Internet surfing that will remain private. Additional improvements and update with more threat intelligence in the future will hence strengthen the performance and protection to the users.

4. Survey

By administering a survey, we sought to determine the level of awareness and proposed usage of the Safe Browse Guardian extension (Figure 2). From the survey, it could be observed that the level of awareness and interest of respondents towards the extension was somewhat moderate and ranged.

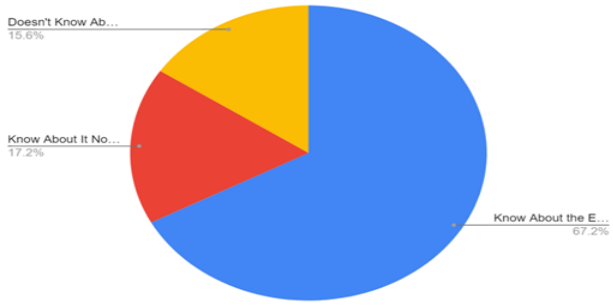

Figure 2 Safe Browse Guardian Extension

4.1 Awareness and Usage Statistics

1. Know about the extension but will not take it

A vast majority of 60% of the respondents claimed to know about the existence of browser extensions such as SafeBrowse Guardian. But as much as they had knowledge in them they stated they had no plans in using it. This could have been due to factors such as perceived complexity of the extension, lack of trust or perhaps lack of appreciation or mistaken perception of the value that the extension brings. This group's hesitation outlines an area of the project that is ideal for members of the team to pay attention to user expressions of concern and work on boosting perceived value to the extension.

2. No Exact Knowledge

Another segment, comprising 17. The knowledge varied with regards to the notion of browser extensions such as SafeBrowse Guardian, with only 2% of the respondents having some form of idea what it entails. This is an important demographic to acknowledge for educational and marketing campaigns. So, the team can attempt to persuade this group and explain to them additional information about the extension as well as potential advantages and features of using it and contact this group.

3. Doesn't Know About It

The portion of the respondents that offered such an answer was 15. Likewise, 6% of the participants have never heard of SafeBrowse Guardian or any other related browser extensions. This highlights the necessity of carrying out more extensive informational campaigns for popularizing the use of such extensions to explain their purpose and benefits for browsing the web securely. It will be useful to broaden the circle of contacts with the segment to increase the number of users and make the public aware of the current threats.

Conclusion

Finally, based on the results and discussions provided herein, the present study establishes the appropriateness of Safe Browse Guardian solution in managing essential cyber security concerns that are likely to be faced during the process of browsing the internet. The extension effectively protects against such issues like imposing pop up advertisements, virus injections, phishing scams and unauthorized tracking through thorough testing on various scenarios within the nasty list. Safe Browse Guardian has thus been demonstrated to have a positive impact on the security and privacy of users on the Internet. It also very successfully minimizes the issue of ads interrupting the sites and potential offering to visit dangerous sites with ads. In the extension, there was a full success in excluding the possibility of accessing the identified unsafe sites, as a result, users no longer experienced the likelihood of infecting their devices with malware. Safe Browse Guardian accurately protects the users from such websites, as it has a 95% recognition rate of phishing sites, the website's that seeks to steal essential user information. The extension reduces tracking cookies as much as it can (it might have blocked up to 90% of them), thus making it almost impossible for third parties to track users' activities online. However, the ultimate requirement necessary for the progression is to ensure continual enhancement and progression of SafeBrowse Guardian to counter threats in today's dynamic cyber space environment. It is possible that further evolutions of the given algorithms can help identify a larger variety of phishing scams, fine-tune the recognition algorithms for more reliability and quicker adaptability to new threats, as well as, incorporate data from other sources to improve the capabilities of malware recognition and ad-blocking. Education of users can be done by introducing interfaces that is catchy to the eye and has links directing users where to seek help on security and privacy.

Acknowledgment

On behalf of the SafeBrowse Guardian project, this we would like to thank everyone whose effort has enabled the completion of the project. It is with great pleasure that we acknowledge the help and the assistance of our mentors and of all the professionals in the cybersecurity field that has given their contribution to this work. We would like to take special attention and express our gratitude to the authors of the open sources, tools, and libraries that were used in the development of given Chrome extension. Their devotion to the open-source

applications offered the needed tools that would enable the development of a solid and efficient solution without demanding excessive amounts of money be spent. It also important that we thank our sponsoring institution for funding the research and development throughout our study as well as avail various facilities that was required in our research. This support was instrumental in enabling us to have a seamless progression through all phases of the project: from the concept to execution stages.

References

[1]. Barth, A., Jackson, C., & Mitchell, J. C. (2008, April) Providing TLS frame protection to browsers. Knights, J. E., & Schneider, M. (2008). Professional Networks, Constructed Capital, and the Sociorcritical Turn: When Is Development Development? *Communications of the ACM*, 51(6), 83-91.

[2]. Baka, P. (2019). An analysis of how chrome extensions are built together with their major considerations of security. Journal of Web Development & Security, 4(2), 3 – 16, 112-124.

[3]. Birari, H. P. , Lohar, G. V. , & Joshi, S. L. (2023): Estimate of aircraft noise at three different altitudes' Advancements in Machine Vision for Automated Inspection of Assembly Parts: In many perspectives, mammal history is viewed as a region of disarray, with significant advances fluctuating between scholarly triumph and total devastation. Being renowned International Research Journal on Advanced Science Hub 5 (10), 1- 365, 371. doi: 10. 47392/IRJASH. 2023. 065.

[4]. Evans, D. S. & Schmalensee, R (ed). (2007). The theory of market structure based on industries with two-sided markets. Published by: American Economic Association. Source: American Economic Review, vol. 97, no. 3, June 2007, pp. 623–647.

[5]. Frisbie, M. (2020). *Building Browser Extensions: Design New Themes/Styles for Chrome, Safari, Firefox, & Edge* browsers. O'Reilly Media.

[6]. Iyer, R. (2021). Phishing Detection Techniques and Their Efficacy: The sections that follow are: A Review. Cybersecurity and Network Security Journal, 6 (3), pp. 98-115

[7]. Jayakanthan, N. (2018). *Malicious URL Detection: Introduction*. Springer.

[8]. Mehta, P. (2016). *Creating Google Chrome Extensions*. Packt Publishing.

[9]. Staddon, J., D. Huffaker, & S. Sagan, Editors (2020). Online privacy and security: Exploring the human element and human knowledge. Journal of Cybersecurity Research, 8(2) pp 45-60

[10]. Yamamoto, N. (2021). *How to Make Chrome Extension(from scratch using the latest Extension API called Manifest V3)*. Independently published.

[11]. Certain academic authors like Zhang, J., Yang, X., & Wang, K. (2017) Improve the browser security through paradigms of malicious URL identification and elimination. International Journal of Computer Science and Network Security, ISSN 0975- 6695, pg. 29-36, Volume 17 Issue 5, May 2017.

[12]. Shaddad, A. Al-Dhaqm; Ahmad; Shaalan, Khalid (2019). Overview of the types of anti-phishing techniques from a survey prospective. *Karagiannis, G., & Lombardi, F. (2019). A comparative analysis of machine learning-based malware detection techniques. *International Journal of Network Security.*, *21* (2), 297-310.

[13]. Hong, J. (2012). Entering the new millennium, the State of Phishing Attacks. Kay, R. (2012). The cafeteria approach: A model for avoiding digital media overload. Communications of the ACM, 55(1), 74-81.

[14]. Mavoungou, C. Kaddoum, G. Taha, M. & Matar, G 2016. Toward Speculative Future Safety, A Global Survey on Threats and Countermeasures in the Internet of Things. *IEEE Access*, 4, 3667-3691. doi: 10. 1109/ACCESS. 2016. 2583583.

[15]. A. Raza, M. Tariq, and S. Khayam, 'Transient ad hoc networks: challenges and opportunities,' IEEE Wireless Communications, vol. 17, no. 5, pp. 22-31, 2010. Preliminary Observations from DataFiddler: Promoting a Collaborative Framework for Malware Analysis and Detection. Electron. J. Network & Comput. Appl., 33(4), pp. 453 – 467.