WebArmor Extension: One-Stop Solution to Secure Net Surfing

Vaishnavi Ramkumar[1], Supriya Dhebe[2], Harshita Patil[3], Prof. Sujata Kullur[4]
Usha Mittal Institute of Technology SNDT Women's University Mumbai, India 400049.

***Abstract*—Ensuring a secure browsing experience has become essential due to the increase in sophisticated cyber threats. By combining several security features, such as phishing detection, malware scanning for downloaded files, ad and tracker blocking, content filtering for explicit material, and keylogger detection, WebArmour is a complete browser extension that improves online safety. To precisely identify malicious websites, the extension uses a hybrid phishing detection system that combines structured analysis and unstructured analysis using machine learning. Furthermore, WebArmour uses structural and behavioral characteristics to check downloaded files for malware, blocks trackers and intrusive ads to enhance user privacy, and stops keyloggers from obtaining private data. WebArmour seeks to give users a comprehensive solution for safer browsing by combining these security features into a single, lightweight extension. This document outlines the architecture, methodologies, and implementation details of WebArmour, evaluates its effectiveness against existing security solutions, and discusses potential enhancements for future development.**

***Index Terms*—Browser Security, Phishing Detection, Malware Scanning, Ad Blocking, Tracker Blocking, Keylogger Detection, Web Privacy, Content Filtering, Cybersecurity, Web Threats, Ma- chine Learning in Security.**

I. INTRODUCTION

Internet has become an essential part of modern life, enabling seamless access to information, communication, and financial transactions. However, with their widespread adoption, they have also become prime targets for cyber threats. Studies have shown that web-based attacks are among the most common cyber threats, with phishing, malware distribution, and intrusive tracking accounting for a significant portion of security incidents [1] [2]. Phishing remains one of the most prevalent threats, with reports indicating that phishing attacks account for more than 36% of data breaches globally, often leading to financial losses and identity theft [3]. Furthermore, malware attacks, including ransomware and spyware, continue to evolve, with polymorphic malware making signature-based detection less effective [4].

Adversaries continually refine their techniques to evade detection, using sophisticated tactics such as domain obfuscation, adversarial machine learning, and runtime script embedding [5]. Studies have shown that traditional security mechanisms, including antivirus software and browser-based defenses, often do not provide comprehensive protection due to their dependence on static rules or outdated heuristics [6]. Many existing solutions also function in isolation, leaving gaps that attackers exploit.

Another growing concern is online tracking and the invasion of user privacy. Research indicates that more than 90% of websites embed third-party trackers, collecting user data with- out explicit consent [7]. These trackers not only compromise privacy, but also expose users to targeted attacks, including cross-site scripting (XSS) and session hijacking. Furthermore, malicious advertisements, or malvertising, have emerged as a significant threat, with attackers injecting harmful scripts into legitimate ad networks to distribute malware [8].

The existing literature highlights the limitations of standalone security measures. URL-based phishing detection, for example, is based on predefined heuristics that adversaries can easily bypass by manipulating domain structures and using lookalike characters [1]. Similarly, traditional antivirus solutions are based on signature-based methods, which are ineffective against zero-day threats and polymorphic malware [4]. Studies also indicate that ad blockers and tracker blockers, while effective to some extent, often struggle to differentiate between essential and intrusive scripts, leading to functionality issues on legitimate websites [9].

Despite the increasing sophistication of cyber threats, there's a gap in an integrated approach that combines multiple security techniques into a single, real-time solution. The need for such an approach is made

evident by by the growing frequency of attacks, with phishing and malware-related breaches increasing by more than 20% annually [3]. Research has also pointed out the importance of real-time behavioral analysis as a more effective strategy [5].

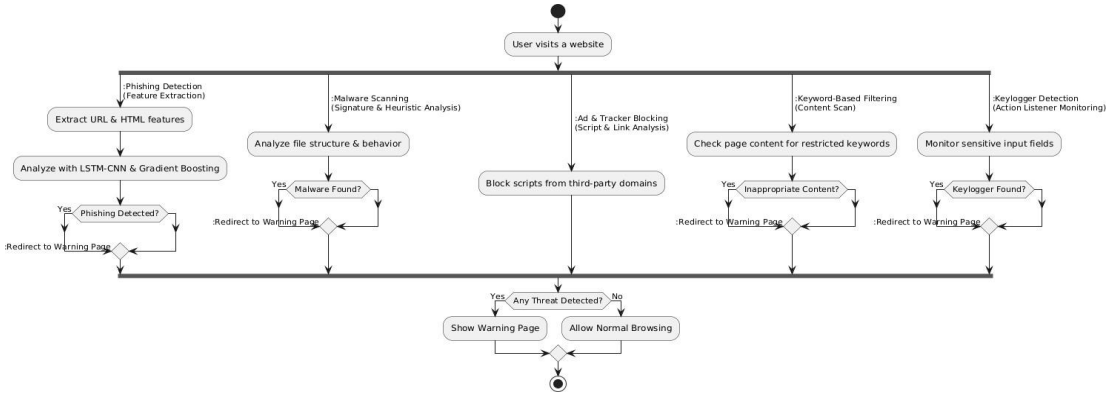

Fig. 1. WebArmour System Flowchart

II. METHODOLOGY

WebArmour is created to provide a seamless and efficient browsing experience while ensuring total protection against major online threats. The extension integrates multiple security features, including phishing detection, malware scanning, ad and tracker blocking, keyword-based content filtering, and keylogger detection, all working in real time with minimal impact on performance. Each module is carefully designed to identify and neutralize threats using a mix of machine learning, rule-based filtering, and script analysis techniques.

For phishing detection, WebArmour takes a hybrid approach by analyzing both structured and unstructured data. The dataset, sourced from Kaggle, contains key features like URL length, presence of special characters, subdomain count, and domain age, as well as webpage content and network traffic patterns. To process this data, the system combines a Gradient Boosting model for structured data, which achieved an accuracy of 98.65%, and a CNN-LSTM model for unstructured data, which reached 95.32%. When these models were integrated into an ensemble approach, the accuracy improved to 99.62%, making it highly effective in detecting phishing attempts, even when attackers manipulate website structures or content to evade detection.

Malware scanning focuses on preventing users from down- loading harmful files by employing both signature-based and behavioral analysis. The dataset used for training was com- piled from real-world malware and Trojan samples avail- able on GitHub. A Random Forest classifier was trained on extracted features and achieved an accuracy of 95%. The signature-based method allows for quick detection of known threats by checking file hashes against a malware database, while the behavioral analysis component observes suspicious file execution patterns, such as unauthorized system modifications or unusual network activity. This combination ensures that even newly developed malware strains can be detected and neutralized.

WebArmour's ad and tracker blocking feature enhances privacy by analyzing the scripts embedded in web pages. Instead of relying on predefined blocklists, the system actively scans <script>tags and flags those that originate from third- party domains unless they are part of a trusted exception list (e.g., Bootstrap, jQuery). By preventing the execution of these scripts, WebArmour effectively blocks intrusive ads, prevents third-party tracking, and ensures a smoother browsing experience.

To further improve security, WebArmour includes a keyword-based content filtering module that prevents access to websites containing explicit or harmful content. A predefined set of restricted keywords is used to scan web pages in real time, and if a match is found, the user is redirected to a warning page. This feature is particularly useful in parental control settings or workplace environments where content restrictions are necessary.

Keylogger detection adds another layer of protection by safeguarding sensitive input fields from unauthorized keystroke logging. Many malicious websites embed JavaScript keyloggers that monitor user input in login forms or payment sections. WebArmour combats this by scanning for add Event Listener functions linked to keylogging

activity. If such a script is detected near a sensitive input field, the extension alerts the user, helping to prevent credential theft and unauthorized data collection.

A system flowchart, shown in Figure 1, illustrates how WebArmour's modules interact to provide multi-layered pro- tection. Each detection module operates simultaneously, and if a threat is identified, the user is redirected to a secure warning page to prevent further risk.

III. RESULTS AND DISCUSSIONS

WebArmour was put to the test against various online threats, including phishing, malware, adware, tracking, explicit content, and keyloggers. Each security feature was evaluated

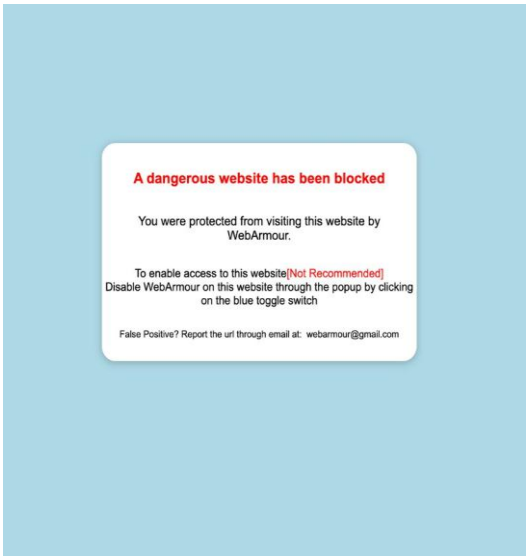

Fig. 2. WebArmour Warning users about a threat

both individually and in real-world browsing scenarios to measure its effectiveness and impact. The phishing detection system, which was trained on structured and unstructured showed remarkable accuracy. The Gradient Boosting model alone achieved 98.65% accuracy, while the CNN-LSTM model, reached 95.32% accuracy. When both approaches were combined, accuracy increased to an impressive 99.62%, proving that blending structured and unstructured data results in a more robust phishing detection system. During live tests, WebArmour successfully identified phishing attempts, even on websites that frequently changed their content to bypass traditional detection methods.

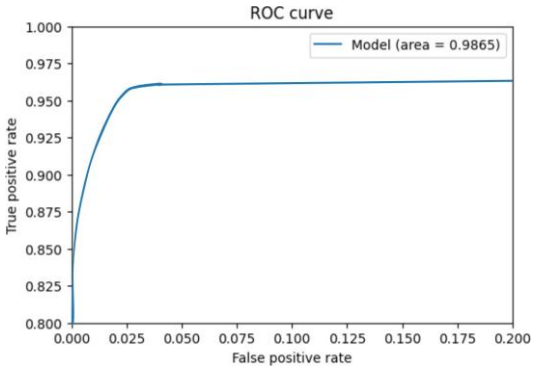

Fig. 3. Error Graph for Phishing Detection using Gradient Boosting

The malware detection module performed well, reaching

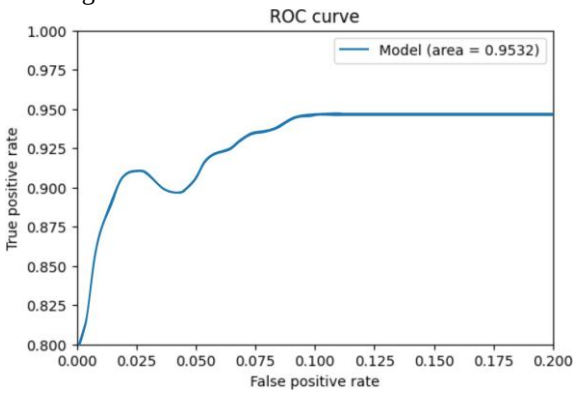

Fig. 4. Error Graph for Phishing Detection using CNN-LSTM

95% accuracy with a Random Forest classifier. When tested in real-world conditions, WebArmour effectively blocked malicious downloads disguised as common file types like PDFs and images. However, some highly obfuscated malware samples managed to slip through, suggesting that integrating advanced behavioral analysis could further strengthen this module.

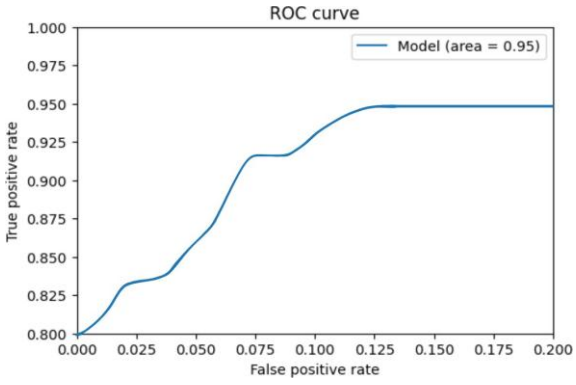

Fig. 5. Error Graph for Malware Detection

The adware and tracker blocking system In testing, successfully blocked all ads and trackers 10 out of

10 times, preventing intrusive pop-ups and improving page load speeds. This approach not only kept annoying ads at bay but also enhanced user privacy by stopping websites from tracking user behavior.

For keyword-based content filtering, WebArmour relied on a predefined list of restricted words to block explicit or harmful content. While this method worked well in most cases, it occasionally flagged non-offensive content that happened to contain a restricted word. A more context-aware filtering system, possibly using NLP (Natural Language Processing), could help reduce these false positives in the future.

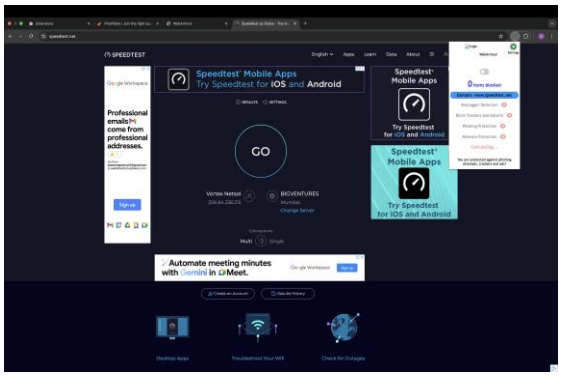

Fig. 6. Webpage with ads and tracker

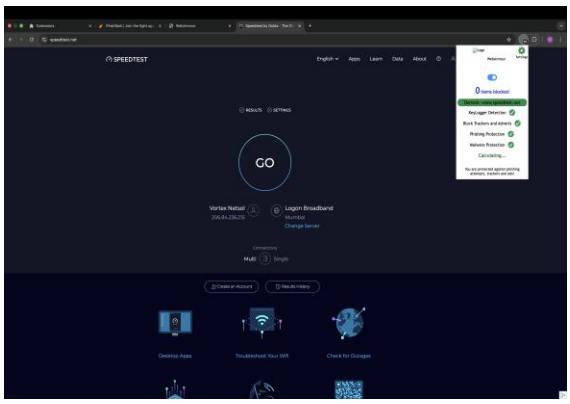

Fig. 7. Clean page with ads blocked

The keylogger detection module monitored login forms and other sensitive input fields, In most cases, this system was effective, but more advanced keyloggers embedded within seemingly legitimate scripts were harder to detect. A behavior- based anomaly detection system could improve accuracy and catch more sophisticated keyloggers in future iterations.

IV. CONCLUSIONS

WebArmour brings together a complete set of security features in a lightweight, easy-to-use browser extension, ensuring users stay protected from online threats without sacrificing browsing speed or experience. By covering key areas of cybersecurity—such as network security, data protection, and privacy—it provides a well-rounded defense against phishing, malware, intrusive tracking, and unauthorized data collection. Of course, no security system is perfect. As cyber threats become more advanced, attackers may find new ways to bypass existing defenses. While WebArmour is designed to adapt and improve over time, ongoing updates and smarter threat detection will be crucial to staying ahead. Addition- ally, balancing strong security with performance remains a challenge, as more advanced protections could slightly impact browser speed.

That said, WebArmour stands as a reliable and proactive security solution, offering a seamless blend of protection and usability. With future improvements like AI-driven detection and smarter filtering, it has the potential to become an even more powerful tool in the fight against cyber threats. As the digital landscape continues to evolve, WebArmour ensures that users can browse with confidence, knowing they have a strong layer of security on their side.

V. ACKNOWLEDGMENT

We would like to express our sincere gratitude to our Principal, Dr. Yogesh Nerkar, for their unwavering support and encouragement throughout this research. We extend our heartfelt thanks to our Head of Department, Dr. Sanjay Shitole, for their valuable guidance and constructive criticism, which significantly contributed to the improvement of our work. We also appreciate the efforts of our esteemed faculty members and the teaching and non-teaching staff for their constant support and assistance, creating an environment conducive to research and learning. Lastly, we are grateful to our peers, friends, and family for their encouragement and motivation throughout this journey.

REFERENCES

[1] A. K. Dutta, “Detecting phishing websites using machine learning technique,” *PloS one*, vol. 16, no. 10, p. e0258361, 2021.

[2] Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, Q. E.

U. Haq, K. Saleem, and M. H. Faheem, "A deep learning-based phishing detection system using cnn, lstm, and lstm-cnn," *Electronics*, vol. 12, no. 1, p. 232, 2023.

[3] "2023 data breach investigations report," 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[4] S. Alnemari and M. Alshammari, "Detecting phishing domains using machine learning," *Applied Sciences*, vol. 13, no. 8, p. 4649, 2023.

[5] J. Shen, "On the power of localized perceptron for label-optimal learning of halfspaces with adversarial noise," in *Proceedings of the 38th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, M. Meila and T. Zhang, Eds., vol.

139. PMLR, July 18–24 2021, pp. 9503–9514. [Online]. Available: https://proceedings.mlr.press/v139/shen21a.html

[6] X. Zou, R. Zhuang, A. D. Kent, S. Samtani, M. L. Shue, and M. Gupta, "Security risk assessment of machine learning-based systems: A quan- titative approach," *IEEE Security & Privacy*, vol. 17, no. 2, pp. 40–48, 2019.

[7] M. Muzamil, A. Khan, S. Hussain, M. Z. Jhandir, R. Kazmi, and I. S. Bajwa, "Analysis of tracker-blockers performance," *Pakistan Journal of Engineering and Technology*, vol. 4, no. 1, pp. 184–190, 2021.

[8] M. S. Team, "Microsoft's warning on malvertising campaigns," *The Hacker News*, 2025, accessed: 2025-03-16. [Online]. Available: https: //thehackernews.com/2025/03/microsoft-warns-of-malvertising.html

[9] X. Zhou, Y. Liu, and X. Wang, "The effectiveness of ad-blocking: A measurement study," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2345–2358, 2020.

[10] D. K. McGrath and K. Gupta, "Behind phishing: An examination of phisher subdomains," *eCrime Researchers Summit*, pp. 1–8, 2008.

[11] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Beyond blacklists: Learning to detect phishing sites from the webpage structure," in *Proceedings of the 17th International Conference on World Wide Web*. ACM, 2009, p. 449–458.

[12] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs, "Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, p. 373–382, 2010.

[13] T.-C. Lin, C.-H. Lai, and Y.-L. Chen, "Malware behavioral analysis based on sandboxing," *Journal of Information Science and Engineering*, vol. 29, no. 1, pp. 73–89, 2013.

[14] L. Huang, A. D. Joseph, B. Nelson, B. I. Rubinstein, and J. D. Tygar, "Adversarial machine learning," in *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*, 2018, pp. 43–58.

[15] H. Zhang, W. Wang, Y. Li, and G. Jiang, "An end-to-end deep learning model for web threat detection," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2300–2312, 2021.

[16] C. Kruegel and G. Vigna, "Anomaly detection of web-based attacks," in *Proceedings of the 10th ACM Conference on Computer and Communi- cations Security*. ACM, 2003, pp. 251–261.

[17] N. Hardy, S. Creese, and M. Goldsmith, "A survey of keylogger detection techniques," *Journal of Cyber Security and Mobility*, vol. 6, no. 2, pp. 183–212, 2017.

[18] Y. Jia, X. Wang, Y. Chen, and W. Lee, "Web tracking and user privacy: Perception, behavior, and barriers," *Proceedings of the 26th USENIX Security Symposium*, pp. 1339–1356, 2017.

[19] R. Gandhi, M. Mahoney, N. Sharma, and A. Selim, "Detecting malicious javascript with static and dynamic analysis," in *Proceedings of the 5th International Conference on Cyber Security and Information Assurance*, 2011, pp. 78–85.