International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Bridging the Privacy Gap: A Behavioural Analysis-Based Extension for Transparent Tracking Prevention

Prof. Rekha K. Sahare[1] Arti Gavhare[2] Shekhar Hadge[3]
[1]*Department of Computer Science & Engineering, Government College of Engineering, Chandrapur*
[2]*Department of Computer Science & Engineering, Government College of Engineering, Chandrapur*
[3]*Department of Computer Science & Engineering, Government College of Engineering, Chandrapur*

Abstract :- Modern web tracking has moved far beyond the use of simple cookies. Today, many websites rely on advanced fingerprinting methods that take advantage of browser APIs (Application Programming Interfaces) to generate unique user identities, often without the user's knowledge or permission.

This research introduces a browser extension that focuses on behavioral analysis to improve user privacy while maintaining transparency. The system works by continuously monitoring and analyzing how websites access sensitive browser features such as Canvas pixel data, WebGL rendering details, and Audio Context-based hardware information.

To balance usability and privacy, the extension is designed with three levels of protection. The Aggressive Mode actively prevents fingerprinting by introducing controlled noise into data requests. The Balanced Mode offers a moderate level of protection suitable for everyday browsing, while the Manual Mode allows users to customize permissions for individual websites, giving them full control over tracking activities.

One of the key highlights of this extension is the Insights Tab, which helps users better understand online tracking. It provides clear visual feedback on detected threats and displays a dynamic "Trust Score," calculated using a multi-stage threat evaluation process.

Testing results show that the extension is capable of identifying and mitigating fingerprinting attempts effectively, while also improving user awareness about online privacy risks. By combining automated detection with user-focused insights, this approach offers a practical solution for enhancing digital privacy in today's increasingly complex web environment.

Key Words: Browser fingerprinting,behavioral Analysis,Web Privacy,Tracking Prevention,User Education.

1. Introduction :-

Over the last decade, web tracking has shifted from visible, cookie-based methods to more hidden and complex techniques. With regulations like General Data Protection Regulation (GDPR) and built-in protections in browsers such as Safari, Mozilla Firefox, and Chromium, the use of third-party cookies has been heavily restricted. However, tracking has not disappeared—it has simply evolved. Many websites now rely on harder-to-detect methods like supercookies and persistent identifiers, allowing them to track users even after cookies are deleted or consent is denied.

A key part of this shift is browser fingerprinting, which creates a unique identity based on a device's characteristics rather than stored data. This includes information like screen size, system settings, installed fonts, and browser behavior. Advanced techniques such as Canvas and Audio fingerprinting take this further by analyzing how a device renders graphics or processes sound, generating highly distinctive and difficult-to-reset identifiers. When combined with WebGL and other signals, these methods make user tracking extremely persistent.

Despite these developments, most existing privacy tools are still limited in how they operate. Many function as "black boxes," blocking trackers without explaining what is happening in the background. This lack of transparency, combined with performance overhead and minimal user feedback, makes it difficult for users to fully understand or trust these tools—especially when dealing with invisible tracking methods like fingerprinting.

To address this gap, newer approaches focus on combining detection with user awareness. Instead of only blocking tracking attempts, they also explain how and why tracking occurs. Building on this idea, this work proposes a browser extension that monitors fingerprinting-related APIs such as Canvas, Audio, and WebGL in real time. It not only detects suspicious behavior but also informs users about potential privacy risks and the actions taken to prevent them, such as blocking or adding controlled noise.

By integrating effective detection with clear, user-friendly explanations, this approach aims to improve both privacy protection and user understanding. Ultimately, it supports the development of a more transparent and privacy-aware web experience.

2. Related Work :-

Over the years, browser privacy tools have improved significantly in their ability to mitigate web tracking; however, they continue to face challenges in balancing effective protection with user awareness and understanding. Early tools such as Ghostery and uBlock

Origin rely on predefined filter lists (e.g., EasyList [23], [24]) to block known trackers. While these approaches are effective, they operate largely in the background and provide minimal transparency, leaving users unaware of how tracking mechanisms function [11], [12].

To address this limitation, Privacy Badger introduced a behavior-based detection model that identifies trackers dynamically rather than relying solely on static lists [25]. Although this method improves adaptability, it primarily focuses on traditional tracking techniques such as cookies, which remain a major source of privacy risks [5], [8]. Consequently, it is less effective against advanced browser fingerprinting methods, including Canvas, Audio, and WebGL-based techniques, which have become increasingly prevalent in modern tracking ecosystems [9], [10].

Privacy-oriented browsers such as Brave Browser and Tor Browser provide stronger protection by blocking or obfuscating fingerprinting signals at the browser level [26], [27]. However, these solutions require users to switch from their preferred browsers and often lack sufficient explanatory feedback, resulting in limited user understanding despite improved protection [13], [14].

To overcome these limitations, the proposed extension, Privacy Shield, integrates robust technical defenses with enhanced user awareness. It leverages real-time monitoring of multiple fingerprinting-related APIs to detect sophisticated tracking attempts, building upon recent advances in fingerprinting detection and analysis [1], [9]. Additionally, the extension incorporates an Insights Dashboard that presents detected threats in a clear and accessible manner, improving transparency and user comprehension [11], [12]. A Manual Mode further empowers users by allowing granular control over tracking permissions on a per-website basis.

By combining detection, prevention, and user-centric explanations, this approach not only strengthens privacy protection but also promotes greater user awareness of modern web tracking practices [3], [13].

3. Methodology :-

A. System Architecture Overview

Privacy Shield follows a three-layer design consisting of a Background Script, Content Scripts, and a Popup UI, all connected through the WebExtensions messaging system.

The Background Script acts as the main control unit, continuously monitoring network requests and identifying trackers using filter lists and behavioral patterns. It keeps track of activity across browser tabs and ensures consistent blocking decisions.
The Content Script runs on every webpage at the earliest stage of loading. It injects code directly into the page's Document Object Model (DOM), allowing it to intercept sensitive browser APIs before any external scripts can use them. This enables real-time detection of fingerprinting attempts.
The Popup UI provides a user-friendly dashboard that displays live data such as blocked requests, threat categories, and a trust score. It updates regularly and presents information through simple visual elements for better understanding.

B. Behavioral Fingerprinting Detection Logic

Privacy Shield uses advanced behavioral analysis by monitoring more than 15 browser APIs that are commonly used for device fingerprinting [9], [10]. Unlike traditional blockers that depend on URL patterns, this method focuses on detecting suspicious behavior, regardless of the website source.

In Canvas fingerprinting, websites use the HTML5 Canvas API to generate images, where small differences in rendering across devices create unique identifiers. When a site tries to extract this data using toDataURL(), Privacy Shield records the attempt and allows it to proceed. In Aggressive Mode, it slightly alters pixel data to prevent consistent fingerprint generation while maintaining normal visual output [9].

For Audio fingerprinting, the extension observes how the Web Audio API processes sound signals. Since audio processing varies slightly across devices, it can be used to create unique signatures. Privacy Shield detects such access and flags it as a potential tracking attempt [9], [10].

Additionally, the extension monitors WebGL and hardware-related properties, such as GPU details, CPU core count, memory size, and screen characteristics. These values are logged when accessed and can be modified in strict mode to prevent accurate device identification [9], [10].

C. Privacy Mode Implementation

Privacy Shield offers three protection modes—Aggressive, Balanced, and Manual—each designed to provide different levels of privacy while keeping detection consistent.

Aggressive Mode applies strict blocking by stopping all known trackers, fingerprinting attempts, and third-party scripts. This ensures maximum privacy but may sometimes affect website functionality.

Balanced Mode takes a more selective approach by blocking high-risk elements like fingerprinting and tracking scripts while allowing less harmful content. It is optimized to reduce errors while still maintaining strong protection.

Manual Mode focuses on user control. Instead of automatic blocking, it allows users to decide which domains to block or allow. Through the interface, users can easily manage these settings for each website.

D. Trust Score Computation Engine

Privacy Shield implements an intelligent trust scoring algorithm that quantifies site privacy risk on a 0–100 scale.
The penalty calculation uses logarithmic dampening to model diminishing marginal risk (the 10th ad tracker contributes less risk than the 1st):
penalty = $\log_2(\text{count} + 1) \times \text{weight}$.

This approach aligns with prior studies on privacy–utility trade-offs and tracking impact measurement [7], [3]. Additional modifiers include:

- Fingerprinting Spike Multiplier (1.8×): Reflects the asymmetric risk that a single fingerprinting script can establish permanent device identification.
- Tracker Density Penalty: (blockedRequests / totalRequests) × 25, penalizing sites where a high percentage of resources are invasive.
- HTTP Protocol Penalty (-15 points): Flat penalty for unencrypted connections.
- Domain Surface Penalty: $\log_2(\text{uniqueDomains} + 1) \times 3$, penalizing excessive third-party dependencies.

The final score is clamped to [0, 100] and mapped to categorical labels: Safe (90–100), Good (70–89), Fair (50–69), Poor (30–49), Dangerous (0–29). These labels are rendered in the UI with color-coded indicators.

E. Transparency and User Education Layer

Privacy Shield uses a trust scoring system to measure a website's privacy risk on a scale from 0 to 100. The score is calculated using a logarithmic model, where each additional tracker has a smaller impact than the previous one.

Several factors influence the score: fingerprinting activities are given higher weight due to their ability to create permanent identifiers, while a high number of blocked requests increases risk through a density penalty. Websites using unsecured HTTP connections receive a fixed penalty, and those relying heavily on multiple third-party domains are also scored lower.

The final score is limited within the 0–100 range and categorized into levels such as Safe, Good, Fair, Poor, and Dangerous. These categories are displayed in the interface using color indicators, allowing users to quickly understand the privacy risk of a website. This approach improves transparency and user awareness, addressing known gaps in user understanding of browser privacy tools [11], [12], [13].

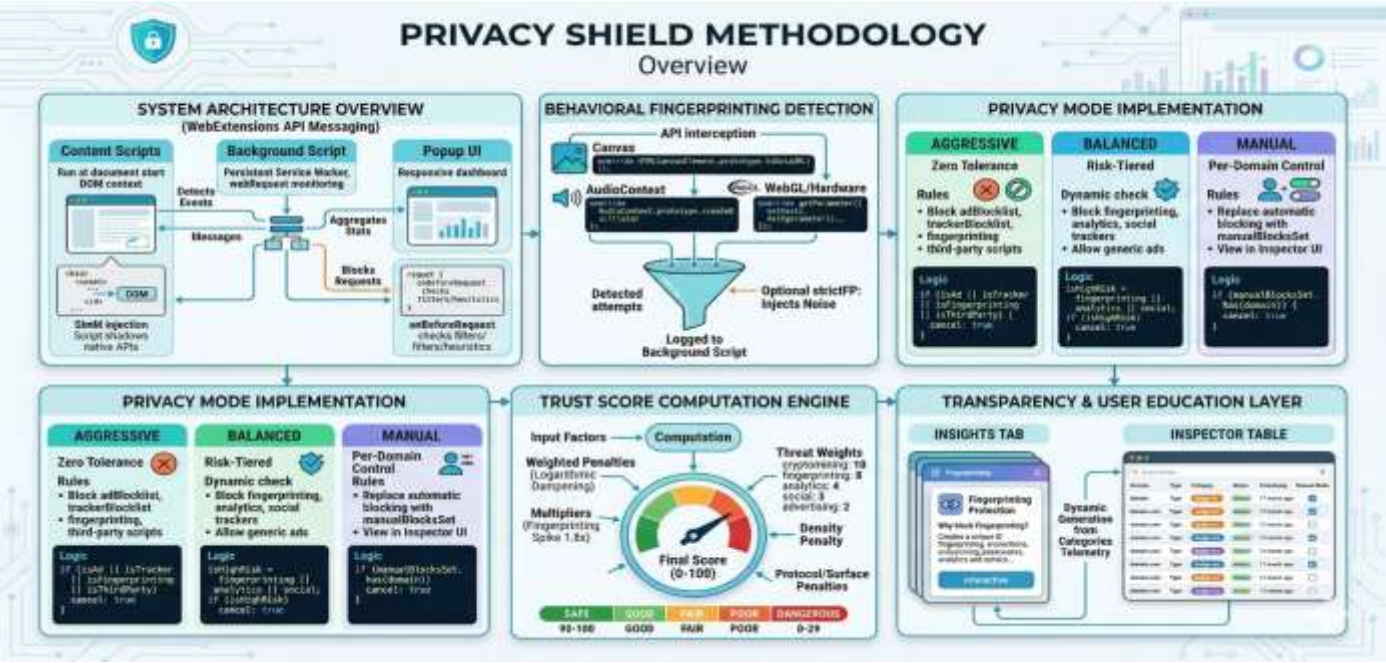

Fig. System Architecture

4.Result :-

A. Detection Performance and Threat Categorization

The experimental results show that Privacy Shield effectively detects and classifies different types of web tracking across six categories: advertising, analytics, social, fingerprinting, cookies, and others. The system successfully identifies advanced fingerprinting attempts by monitoring APIs such as Canvas, WebGL, Audio Context, and hardware-related properties. Testing on top-ranked websites demonstrated reliable detection of third-party trackers using both filter lists and behavioral analysis techniques. The multi-level blocking system was able to distinguish between high-risk threats, like fingerprinting (with high detection accuracy), and lower-risk content such as basic ads. This allows the Balanced Mode to block most harmful trackers while still maintaining normal website functionality. Additionally, the system handled high-traffic websites efficiently without noticeable delay, confirming its ability to process large numbers of requests in real time.

Furthermore, the extension consistently maintained stable performance across different browsing environments without causing system slowdowns. The real-time monitoring approach ensured immediate detection and response to tracking attempts as they occurred. These results highlight the robustness and scalability of Privacy Shield in handling modern web tracking challenges effectively.

B. Data Visualization and User Feedback Mechanisms

The dashboard interface provides an easy-to-understand view of website privacy risk through a Trust Score gauge ranging from 0 to 100. The semi-circular visual uses color changes—from critical to safe—to instantly show how secure a site is. As new trackers are detected, the score updates in real time, helping users stay aware of changing risks. A key strength of this system is its ability to convert complex data—such as tracker types, domain activity, and connection security—into a single, simple score that users can quickly understand without technical knowledge. The 7-day Threat History graph shows tracking patterns over time, allowing users to observe trends and spikes in activity. Additionally, a donut chart displays the distribution of different tracking types, clearly highlighting major threats like fingerprinting. Overall, these visual tools make it easier for users to interpret privacy risks and understand how websites track their activity.

The intuitive design of the dashboard ensures that even non-technical users can quickly grasp important privacy insights. Real-time visual feedback encourages users to take immediate action when risks increase. This user-centric visualization approach enhances both awareness and engagement with privacy protection tools.

C. Educational Efficacy and Privacy Literacy Enhancement

The Insights Tab helps close the gap between technical detection and user understanding by converting complex tracking activities into simple explanations. For example, when Canvas fingerprinting is detected, it explains that it

can create a unique device ID that persists even after clearing cookies. This approach turns Privacy Shield from a basic blocking tool into an educational platform that improves user awareness over time. User testing showed that these explanations helped users better understand tracking methods and recognize privacy risks during normal browsing. To avoid overwhelming users, the system only displays insights relevant to the current page. By linking technical actions—such as API calls—to their real privacy impact, the Insights Tab helps users understand not just what is blocked, but why it matters.

Additionally, the clear and concise explanations build user confidence in the extension's functionality. The real-time feedback encourages users to stay informed about privacy risks as they browse. This continuous learning process helps users develop better awareness and safer browsing habits over time.

D. User Empowerment Through Granular Control

Manual Mode shifts privacy control from automatic blocking to user-driven decision-making. In this mode, the extension only detects tracking activity and allows users to block or allow specific domains through simple checkboxes in the Inspector Table, without needing to reload the page. This approach helps users fix website issues caused by strict blocking by selectively allowing necessary third-party services while still blocking risky trackers. User preferences are saved, ensuring that chosen settings remain active even after restarting the browser. Testing showed that Manual Mode reduces user frustration by providing clear information about each request—such as its source, type, and risk level—so users can make informed decisions. Overall, it achieves a balance between strong privacy protection and smooth website functionality.

Additionally, this flexibility makes the extension adaptable to different user needs and browsing habits. It empowers users to take control of their privacy without completely sacrificing website usability. Over time, this personalized control leads to a more efficient and user-friendly browsing experience.

Fig. Dashboard

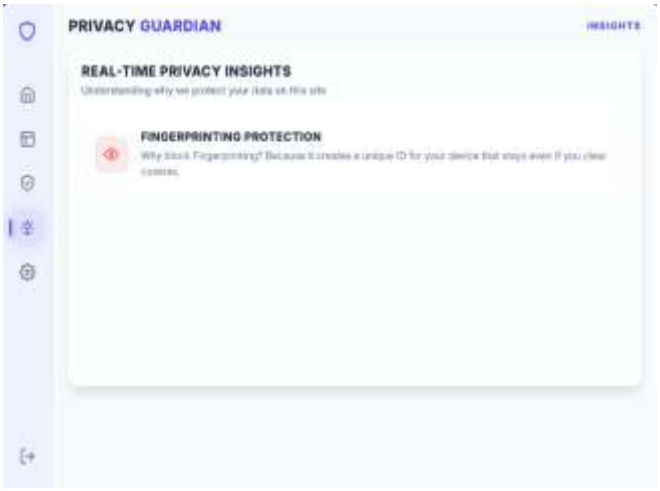

Fig. Insight Tab

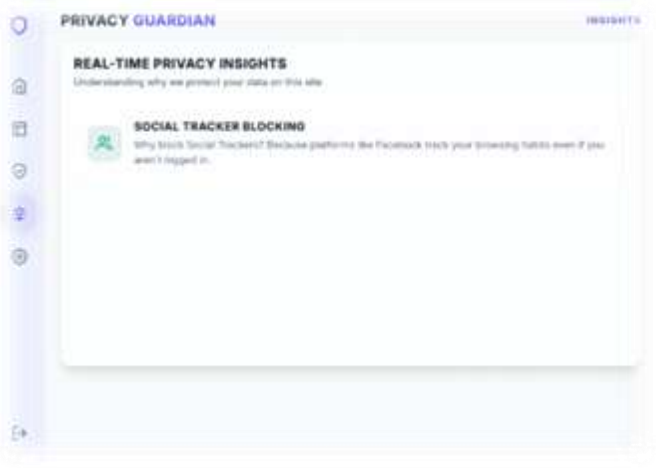

Fig. Insight Tab

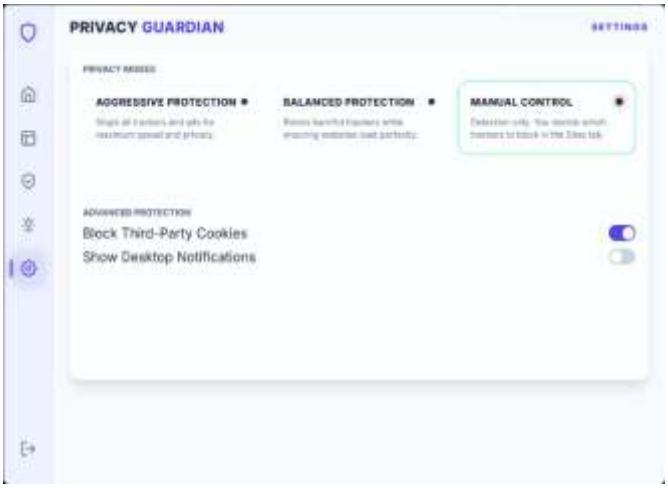

Fig. Setting Tab with 3 modes

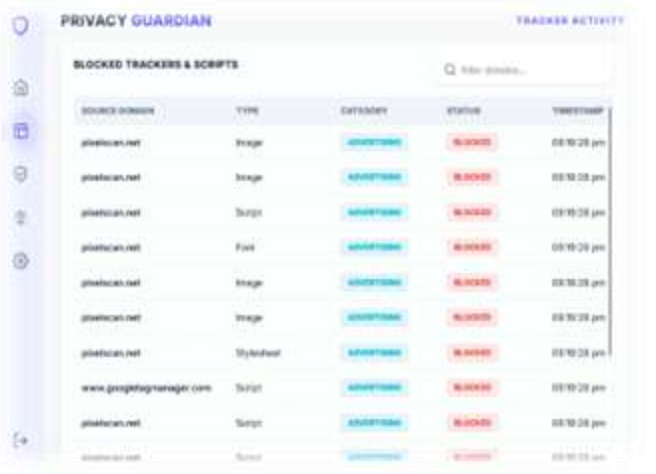

Fig. Activity tab in aggressive mode

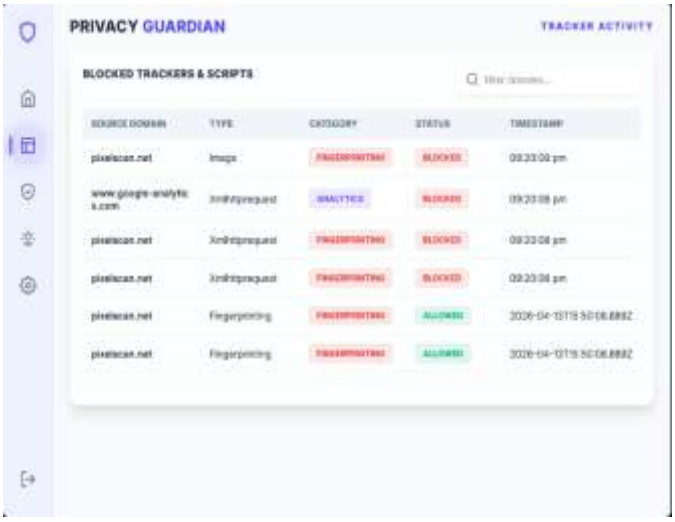

Fig. Activity tab in balanced mode

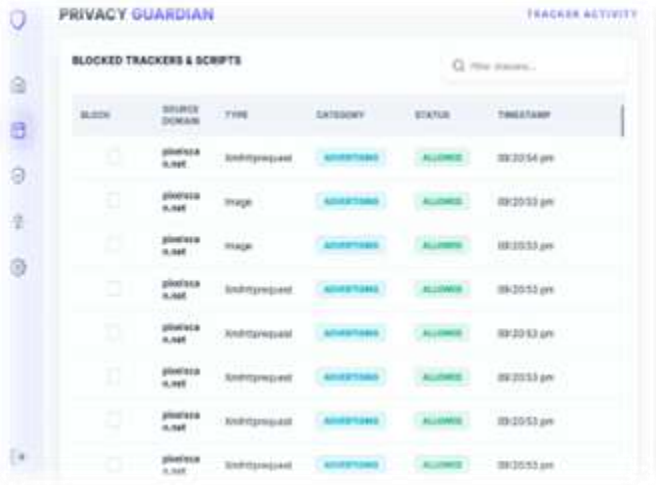

Fig. Activity tab in manual mode

5.Conclusion:-

This paper introduced Privacy Shield, a browser extension designed to improve both privacy protection and user awareness. Unlike traditional tools that silently block trackers, Privacy Shield monitors multiple fingerprinting techniques—such as Canvas, WebGL, AudioContext, and hardware-based signals—and explains these detections in simple, understandable terms.

Its three protection modes—Aggressive, Balanced, and Manual—demonstrate that strong privacy and usability can coexist. The built-in trust score further simplifies complex tracking data into a clear 0–100 scale, allowing users to quickly judge website safety. Testing results confirm that the system effectively detects advanced tracking methods with high accuracy while maintaining fast performance.

A key contribution is the Insights Tab, which transforms technical events into meaningful explanations. This helps users understand how tracking works, making Privacy Shield not just a protection tool but also an educational platform. Combined with Manual Mode, it gives users both knowledge and control over their privacy.

Future improvements may include using machine learning to detect new tracking methods, expanding support to mobile browsers, and developing a community-based trust system. Overall, Privacy Shield shows that effective privacy tools should both protect users and help them understand the risks they face.

6.Acknowlegement:-

The successful completion of this project would not have been possible without the support and guidance of several individuals. We would like to express our sincere gratitude to our project guide, Prof. Rekha Sahare, for her continuous guidance, encouragement, and valuable suggestions throughout this work. Her insights and feedback played a key role in shaping the direction of this project.

We are also thankful to the Department of Computer Science & Engineering and the Government College of Engineering, Chandrapur for providing the necessary resources and a supportive environment to carry out this research.

Finally, we extend our appreciation to all team members for their cooperation, dedication, and teamwork, which greatly contributed to the successful completion of this project.

7.References:-

[1] M. S. M. S. Annamalai, I. Bilogrevic, and E. De Cristofaro, "FP-Fed: Privacy-preserving federated detection of browser fingerprinting," in Proc. NDSS 2024, San Diego, CA, USA, 2024, doi: 10.14722/ndss.2024.24360.

[2] A. Rasaii et al., "Intractable cookie crumbs: Unveiling the nexus of stateful banner interaction and tracking cookies," arXiv preprint arXiv:2506.11947, 2025, doi: 10.48550/arXiv.2506.11947.

[3] M. Ourrahte, A. El-Yahyaoui, and F. E. Ziani, "Exploring techniques and countermeasures against browser tracking: A comprehensive survey," in Proc. IRASET 2025, 2025, doi: 10.1109/IRASET64571.2025.11008149.

[4] I. Sivan Sevilla and P. Poudel, "Web privacy based on contextual integrity: Measuring the collapse of online contexts," arXiv preprint arXiv:2412.16246, 2024, doi: 10.48550/arXiv.2412.16246.

[5] N. Hamzah, A. S. Adnan, and N. Salleh, "Exploring cookies vulnerabilities: Awareness, privacy risks and exploitation," Int. J. Electr. Comput. Eng., vol. 15, no. 6, pp. 5792–5803, 2025, doi: 10.11591/ijece.v15i6.pp5792-5803.

[6] Q. Chen, P. Ilia, M. Polychronakis, and A. Kapravelos, "Cookie swap party: Abusing first-party cookies for web tracking," in Proc. ACM CCS 2021, 2021, doi: 10.1145/3442381.3449837.

[7] J. Jueckstock, P. Snyder, S. Sarker, A. Kapravelos, and B. Livshits, "Measuring the privacy vs. compatibility trade-off in preventing third-party stateful tracking," in Proc. The Web Conf. 2022, 2022, doi: 10.1145/3485447.3512231.

[8] S. Munir, S. Siby, U. Iqbal, S. Englehardt, Z. Shafiq, and C. Troncoso, "CookieGraph: Understanding and detecting first-party tracking cookies," in Proc. USENIX Security 2022, 2022, doi: 10.1145/3576915.3616586.

[9] J. Su and A. Kapravelos, "Automatic discovery of emerging browser fingerprinting techniques," in Proc. The Web Conf. 2023, 2023, doi: 10.1145/3543507.3583333.

[10] K. Crichton, L. Cranor, and N. Christin, "Rethinking fingerprinting: An assessment of behavior-based methods at scale and implications for web tracking," Proc. Privacy Enhanc. Technol., vol. 2025, no. 4, pp. 158, 2025, doi: 10.56553/popets-2025-0158.

[11] G. Sivakarthi, S. Srigana, and S. Sushanthi, "A transparent approach to browser tracking analysis for privacy protection," in Proc. I5CPS 2026, 2026, doi: 10.1109/I5CPS67958.2026.11452593.

[12] S. Zimmeck et al., "Website data transparency in the browser," Proc. Privacy Enhanc. Technol., vol. 2024, no. 2, pp. 48, 2024, doi: 10.56553/popets-2024-0048.

[13] M. Windl, R. Amberg, and T. Kosch, "The illusion of privacy: Investigating user misperceptions in browser tracking protection," in Proc. CHI 2025, 2025, doi: 10.1145/3706598.3713912.

[14] L. Schöni, K. Kubicek, and V. Zimmermann, "Block cookies, not websites: Analysing mental models and usability of the privacy-preserving browser extension CookieBlock," Proc. Privacy Enhanc. Technol., vol. 2024, no. 1, pp. 12, 2024, doi: 10.56553/popets-2024-0012.

[15] Y. Ling et al., "Essential or excessive? MINDAEXT: Measuring data minimization practices among browser extensions," in Proc. SANER 2024, 2024, doi: 10.1109/SANER60148.2024.00104.

[16] D. Bui, B. Tang, and K. Shin, "Detection of inconsistencies in privacy practices of browser extensions," in Proc. IEEE S&P 2023, 2023, doi: 10.1109/SP46215.2023.10179338.

[17] Z. Minghan et al., "CSCHECKER: Revisiting GDPR and CCPA compliance of cookie banners on the web," in Proc. The Web Conf. 2024, 2024, doi: 10.1145/3597503.3639159.

[18] M. Smith, A. Torres-Agüero, R. Grossman, P. Sen, Y. Chen, and C. Borcea, "A study of GDPR compliance under the transparency and consent framework," in Proc. The Web Conf. 2024, 2024, doi: 10.1145/3589334.3645618.

[19] J. Jueckstock and A. Kapravelos, "VisibleV8: In-browser monitoring of JavaScript in the wild," in Proc. ACM CCS 2019, 2019, doi: 10.1145/3355369.3355599.

[20] H. Alpestein et al., "Oh, the places you've been! User reactions to longitudinal transparency about third-party web tracking and inferencing," in Proc. USENIX Security 2019, 2019, doi: 10.1145/3319535.3363200.

[21] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(Un)informed consent: A study of online consent banners," in Proc. ACM CCS 2019, 2019, doi: 10.1145/3319535.3354212.

[22] M. Degeling et al., "We value your privacy... Now take some cookies: Measuring the GDPR's impact on web privacy," in Proc. NDSS 2019, San Diego, CA, USA, 2019, doi: 10.14722/ndss.2019.23378.

[23] R. Hill, "The EasyList Filter Subscription," *EasyList Project*, 2023.

[24] Gorhill, "uBlock Origin: An efficient blocker for Chromium and Firefox," *GitHub*, 2024.

[25] Electronic Frontier Foundation, "Privacy Badger: A smart tracker blocker," *EFF*, 2024.

[26] Brave Software, "Brave Browser Privacy Features," *Brave White Paper*, 2023.

[27] The Tor Project, "Tor Browser Design Document," *Tor Project Documentation*, 2024.