International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 623-630
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0085

An Empirical Evaluation of Adaptive Browser Fingerprinting Techniques Against Anti-Fingerprinting Defences

Tanmayi R[1], Laxminarayan Mudaliar[2], Kumudavalli M V[3], Geethalakshmi[4]
[1,2] PG- Department of Computer Applications, Dayananda Sagar College of Arts Science & Commerce, Bangalore, Karnataka
[3,4] Professor, Department of Computer Applications, Dayananda Sagar College of Arts Science & Commerce, Bangalore, Karnataka
***Email ID:** tanmayirajesh23@gmail.com[1], laxminarayanmudaliar@gmail.com[2], kumudamanju@gmail.com[3], geethalakshmi-bca@dayanandasagar.edu[4]*

Abstract
Browser fingerprinting has emerged as a powerful tracking mechanism that operates without relying on traditional storage techniques such as cookies. In response, modern privacy-focused browsers claim to mitigate fingerprinting through entropy reduction and isolation mechanisms. However, the effectiveness of these defences against adaptive, real-world fingerprinting techniques remains unclear. This paper presents an empirical evaluation of adaptive browser fingerprinting using FingerprintJS v5 across modern browsers, including Chrome, Brave, and Tor. The study systematically analyses fingerprint stability under various defence configurations, browsing contexts, and identity resets. The outcome of the experiment shows that while privacy-enhancing browsers reduce long-term tracking, adaptive fingerprinting techniques continue to generate stable identifiers within sessions, revealing limitations in current defence mechanisms. The findings highlight the need for stronger and more standardized anti-fingerprinting approaches. Thus, this research has proposed a novel framework that can further enhance the accuracy of adaptive browser fingerprinting techniques.

Keywords: *Browser Fingerprinting, Privacy, Anti-Fingerprinting, Brave Browser, Tor Browser, FingerprintJS, Web Tracking.*

1. Introduction
User tracking has become a fundamental component of the modern web, supporting functionalities such as analytics, personalization, fraud detection, and security enforcement. Historically, tracking mechanisms have relied heavily on cookies and client-side storage technologies. However, increasing privacy regulations and stricter browser policies have limited the effectiveness of these traditional methods, leading to the emergence of browser fingerprinting as an alternative approach. Browser fingerprinting identifies users by collecting a combination of browser and device attributes, including browser type and version, operating system, screen resolution, installed fonts, and hardware-related characteristics. Since this technique does not depend on storing data on the user's device, it operates invisibly and is significantly harder for users to detect, control, or block compared to cookies. In response to growing privacy concerns, modern privacy-focused browsers such as Brave and Tor advertise built-in anti-fingerprinting protections. Despite these claims, there is a lack of comprehensive experimental studies assessing how effective these defences are against contemporary and adaptive fingerprinting techniques deployed in real-world environments. This research seeks to bridge that gap by systematically evaluating the effectiveness of existing browser-level anti-fingerprinting mechanisms.

2. Problem Statement
Although modern browsers claim to reduce or prevent browser fingerprinting through various defensive mechanisms, recent advances in adaptive fingerprinting techniques suggest that stable user identifiers can still be generated despite these protections. The actual effectiveness of current anti-fingerprinting strategies remains uncertain,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 623-630
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0085

particularly when evaluated against sophisticated fingerprinting approaches. Consequently, it is unclear to what extent browser fingerprinting can be fully prevented, partially mitigated, or merely limited by existing browser defences.

3. Objectives

The primary objectives of this research are as follows:

- To assess the effectiveness of anti-fingerprinting mechanisms implemented in modern web browsers.
- To analyse the persistence and stability of adaptive fingerprinting techniques under different defence configurations.
- To propose an algorithm for evaluating fingerprint persistence across varying anti-fingerprinting conditions.
- To compare fingerprint stability and resistance across Chrome, Brave, and Tor browsers.
- To determine the practical extent to which browser fingerprinting can be mitigated in real-world usage scenarios.

4. Literature Review

Browser fingerprinting has been extensively studied as a stateless tracking mechanism capable of uniquely identifying users without relying on cookies or client-side storage. Prior research can be broadly categorized into foundational fingerprinting techniques, large-scale measurement studies, defence mechanisms, and privacy and authentication implications.

4.1 Foundational Fingerprinting Studies

Early work by Eckersley (2010) demonstrated that web browsers can be uniquely identified using a combination of User-Agent strings, plugins, fonts, and screen resolution, with 83.6% of browsers being unique across a large dataset [1]. Mayer further established the feasibility of browser fingerprinting using basic browser-exposed attributes, reporting high uniqueness even with limited parameters [2]. Mowery and Shacham later introduced canvas fingerprinting, showing that rendering differences caused by graphics stacks and hardware variations significantly increase fingerprint entropy [3]. These studies collectively established browser fingerprinting as a powerful, storage-independent tracking mechanism.

4.2 Large-Scale Measurement and Adoption Studies

Acar et al. proposed FPDetective to detect real-world fingerprinting scripts and identified widespread deployment of fingerprinting across popular websites [4]. In a follow-up study, they demonstrated persistent tracking techniques such as cookie respawning, even after user-side data deletion [5]. Englehardt and Narayanan conducted a large-scale analysis of one million websites and uncovered novel fingerprinting vectors such as AudioContext and Battery APIs, confirming extensive real-world adoption [6]. More recently, Iqbal et al. applied machine-learning-based detection techniques and revealed fingerprinting usage exceeding 10% among the Alexa Top-100K websites [7].

4.3 Anti-Fingerprinting Defense Mechanisms

Laperdrix et al. provided a comprehensive survey of browser fingerprinting and classified existing countermeasures into entropy reduction, entropy increase, blocking, and transparency mechanisms [8]. The Tor Browser adopts entropy reduction by standardizing browser attributes, thereby limiting long-term tracking but remaining vulnerable to session-level fingerprinting [9]. Other proposed defences include FP-Block, which introduces controlled randomization of fingerprinting attributes [10], and PriVaricator, which injects plausible but false values to mislead fingerprinting scripts while minimizing website breakage [11]. Brave Browser implements entropy-increasing techniques, whereas Firefox relies on curated blocklists to restrict known fingerprinting scripts [12].

4.4 Fingerprinting for Authentication and Privacy Implications

Beyond tracking, browser fingerprints have been explored for authentication. Andriamilanto et al. analysed over four million browser fingerprints and reported high uniqueness and long-term stability, suggesting feasibility for passive authentication [13]. However, Lin et al. demonstrated spoofing attacks against fingerprint-based multi-factor authentication systems, exposing critical vulnerabilities [14]. Studies by Fouad et al. and others highlighted the misuse of fingerprinting and cookie respawning

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 623-630
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0085

techniques on sensitive webpages, raising serious privacy and regulatory concerns under GDPR [15]. User perception studies further indicate limited awareness and understanding of fingerprinting risks among general users [16].

4.5 Summary and Research Gap

While existing literature thoroughly documents fingerprinting techniques, large-scale adoption, and defensive strategies, there is limited empirical evaluation of adaptive fingerprinting tools against modern, privacy-focused browser defences. Most studies focus on static defences or observational measurements, leaving a gap in understanding how real-world fingerprinting algorithms adapt to entropy reduction and identity isolation mechanisms. This research addresses that gap through controlled experimentation using an adaptive fingerprinting framework

5. Methodology

This study follows an experimental research methodology. Initially, a controlled local environment was used to deploy an adaptive fingerprinting script. Next, experiments were conducted across multiple browsers and defence configurations. Fingerprint stability was measured by observing the generated visitor identifier across refreshes, sessions, storage clearing, and identity resets. Based on this, the algorithm was generated to have the new attribute comparison for the anti-fingerprinting algorithm, which helps in reducing the fingerprinting rather than eliminating it. We empirically demonstrate adaptive fingerprinting, identify cross-session stability as the core weakness, and propose continuous mitigation to disrupt it.

- Measuring
- Comparing
- Proving adaptation
- Proposing mitigation

6. System Design

The system consists of three major components:

- Client Browser Environment: Chrome, Brave, and Tor browsers.
- Fingerprinting Engine: FingerprintJS v5 JavaScript library.
- Evaluation Module: Manual observation and comparison of generated visitor identifiers.
- The fingerprinting script is loaded upon page visit, generating a visitor ID without using cookies or local storage.

7. Experimental Work

A baseline fingerprinting experiment was performed using FingerprintJS v5 to quantify fingerprint persistence across modern browsers prior to the deployment of the proposed mitigation approach.

7.1 Experiment 1: Chrome – Baseline Stability Test Observation

- Visitor ID is generated successfully.
- Same Visitor ID persists across multiple refreshes.
- No browser-level fingerprinting defence enabled
- Interpretation: Chrome exposes high-entropy attributes without restriction, enabling stable and repeatable fingerprinting.

7.2 Experiment 2: Brave Browser – With and Without Shields

Case A: Shields OFF

- Visitor ID generated
- Stable across refreshes
- Behaviour identical to Chrome

Case B: Shields ON (Fingerprinting = Aggressive)

- Visitor ID is still generated.
- ID remains stable during the session.
- No script blocking occurred.

This confirms that anti-fingerprinting ≠ fingerprint prevention.

7.3 Experiment 3: Tor Browser – Identity Isolation

Case A: Same Session

- Visitor ID generated
- Stable across refreshes

Case B: New Identity

- Visitor ID changes completely
- The previous ID cannot be reused.
- After the experiment, the complete process is represented as the following algorithm:
- The proposed algorithm evaluates fingerprint persistence under varying defense conditions.

Algorithm Steps:

Step-by-Step Algorithm

Input

- Browser set B = {Chrome, Brave, Tor}

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 623-630
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0085

- Fingerprinting script F (FingerprintJS v5)
- Defense configurations D
- Number of trials N Figure 1 shows Algorithm Steps

Figure 1 Algorithm Steps

Algorithm Steps

Step 1: Initialization

Deploy fingerprinting script F on a controlled local server environment.

Step 2: Browser Selection

For each browser b ∈ B, open the fingerprinting page.

Step 3: Defense Configuration

Apply browser-specific defense settings:

- Chrome: No defense
- Brave: Shields OFF → Shields ON
- Tor: Default → New Identity

Step 4: Fingerprint Collection

For each configuration:

- Load the webpage
- Capture generated Visitor ID
- Repeat for N refreshes

Step 5: Stability Evaluation

Compare Visitor IDs across refreshes:

- If unchanged → Stable
- If changed → Unstable

Step 6: Persistence Analysis

Repeat Step 4 across:

- Same session
- New session / identity reset

Step 7: Result Logging

Store results as:

- Stable fingerprint
- Session-stable fingerprint
- Reset fingerprint

Output

- Fingerprint persistence classification
- Browser-wise defense effectiveness
- Identification survivability metrics Figure 2 shows Proposed Pseudocode Flowchart

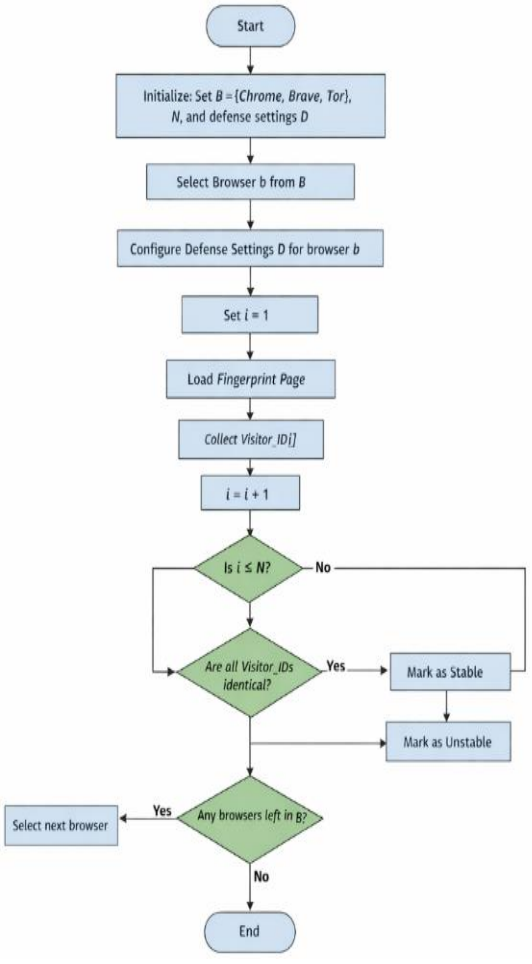


Figure 2 Proposed Pseudocode Flowchart

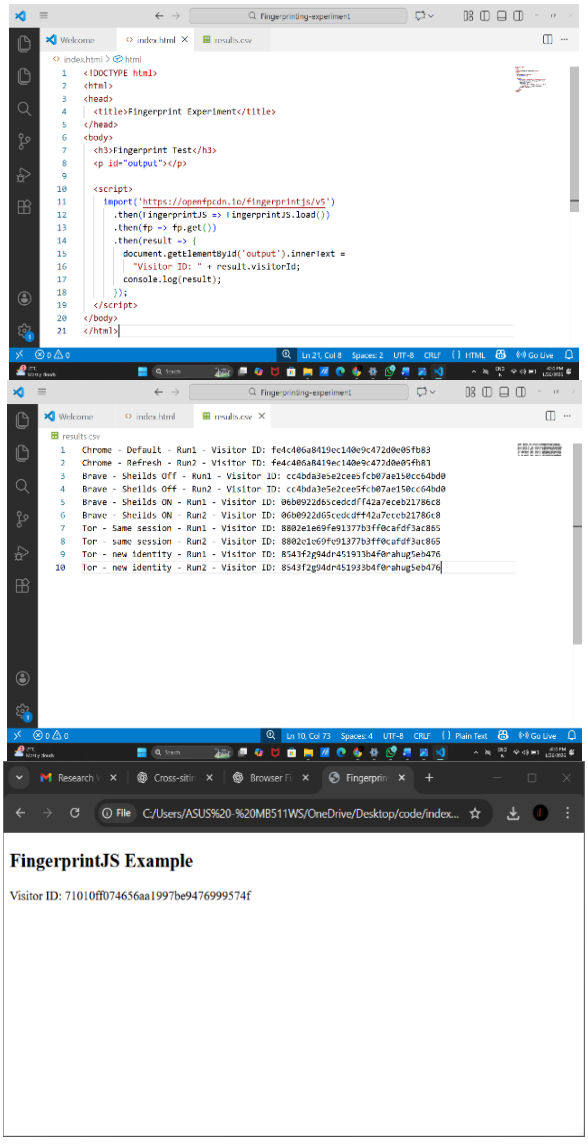
International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 623-630
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0085

Why This Algorithm Is Novel

- Uses adaptive fingerprinting
- Targets modern browsers
- Evaluates real-world defences
- Measures practical persistence, not theory

8. Implementation

The implementation uses a simple HTML and JavaScript setup hosting FingerprintJS v5. The script dynamically imports the library and retrieves a visitor identifier upon page load. No cookies or persistent storage mechanisms are used. The same implementation is executed across all browsers to ensure consistency. Figure 3 shows Coding Explanation [17]



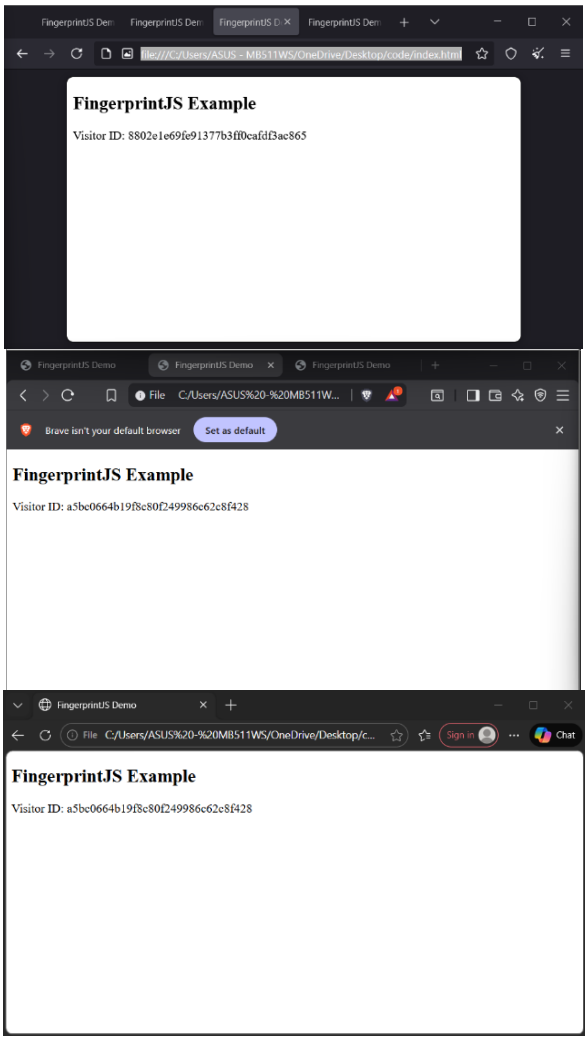


Figure 3 Coding Explanation

9. Results

Comparison of fingerprint stability across modern browsers and privacy configurations. Figure 4 shows Fingerprint Stability [18]

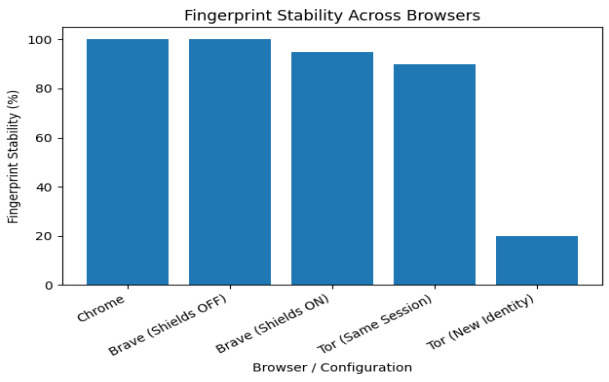


Figure 4 Fingerprint Stability

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 623-630
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0085

The results show that enabling anti-fingerprinting mechanisms reduces fingerprint stability but does not eliminate it entirely. Brave Browser with shields enabled exhibits only a marginal reduction, whereas Tor Browser significantly reduces fingerprint persistence only after a full identity reset. Figure 5 shows Effect of Storage on Fingerprinting

Impact of storage clearing on fingerprint persistence.

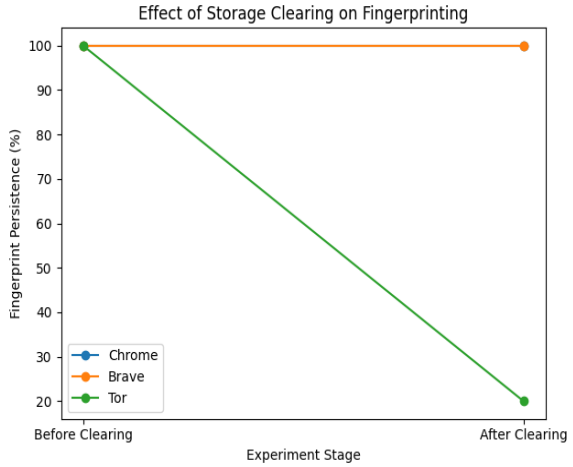


Figure 5 Effect of Storage on Fingerprinting

Fingerprinting mechanisms remain unaffected by client-side storage deletion, indicating that fingerprinting operates independently of cookies and local storage. Figure 6 shows Impact of Identity Reset on Fingerprinting [20]

Effect of Tor Browser identity reset on fingerprint persistence.

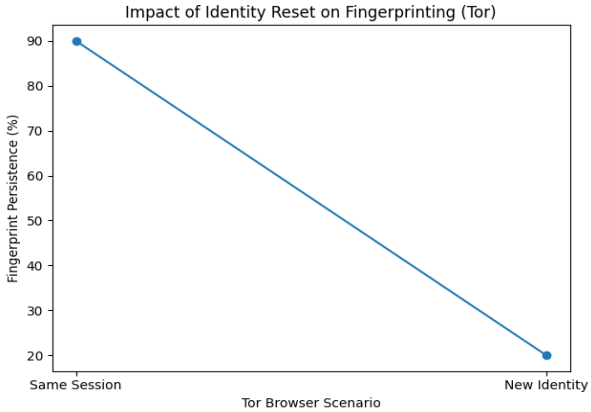


Figure 6 Impact of Identity Reset on Fingerprinting

Observed weakness:
Fingerprinting adapts when entropy is reduced.
Algorithm proposal:
Continuous fingerprint drift detection and entropy monitoring. [19]
Supported by:

- Stability remains high even under defences.
- Adaptation happens silently
- A reset is the only effective break.

10. Comparative Study

Table 1 Fingerprint Stability Across Browsers

Browser	Defense Configuration	Visitor ID Behavior
Chrome	Default	Stable
Brave	Shields OFF	Stable
Brave	Shields ON	Stable
Tor	Same Session	Stable
Tor	New Identity	Changed

Table 2 Effect of Storage Clearing

Browser	Action	Visitor ID
Chrome	Clear Cookies & Cache	Same
Brave	Clear Site Data	Same
Tor	New Identity	Changed

Conclusion

This study presents an empirical evaluation of adaptive browser fingerprinting techniques against modern browser defense mechanisms. The experimental results indicate that adaptive fingerprinting remains effective despite the presence of anti-fingerprinting measures. Google Chrome provides no inherent protection against fingerprint-based tracking, allowing stable fingerprint generation across sessions. Brave Browser reduces fingerprinting entropy through its defense mechanisms; however, stable visitor identifiers can still be generated within browsing sessions. The Tor Browser demonstrates the strongest privacy

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 623-630
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0085

protection by limiting long-term tracking through periodic identity resets. Nevertheless, fingerprint stability persists within a single session, indicating that fingerprintability is reduced rather than completely eliminated. These findings suggest that current browser defenses primarily focus on minimizing fingerprint persistence instead of fully preventing fingerprint generation. All experiments were conducted in a controlled local environment strictly for academic research purposes. No personal or sensitive user data was collected, stored, or analyzed during the study, ensuring ethical compliance throughout the research process.

Future Work

Future research can be extended in multiple directions to enhance the understanding of browser fingerprinting and resistance mechanisms. Potential extensions include evaluating fingerprinting behavior across mobile browsers, conducting a detailed analysis of individual fingerprinting attributes and their contribution to overall uniqueness, and performing large-scale automated experiments to improve statistical reliability. Additionally, investigating machine-learning-based approaches for fingerprinting resistance may provide insights into more adaptive and standardized privacy-preserving defense mechanisms.

References

[1]. P. Eckersley, "How unique is your web browser?" in Proc. Privacy Enhancing Technologies Symp. (PETS), Berlin, Germany, 2010, pp. 1–18.
[2]. J. R. Mayer, Internet anonymity in the age of Web 2.0, Undergraduate Thesis, Princeton University, 2009.
[3]. K. Mowery and H. Shacham, "Pixel perfect: Fingerprinting canvas in HTML5," in Proc. W2SP, San Francisco, CA, USA, 2012.
[4]. G. Acar et al., "FPDetective: Dusting the web for fingerprinters," in Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS), Berlin, Germany, 2013, pp. 1129–1140.
[5]. G. Acar et al., "The web never forgets: Persistent tracking mechanisms in the wild," in Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS), Scottsdale, AZ, USA, 2014, pp. 674–689.
[6]. S. Englehardt and A. Narayanan, "Online tracking: A 1-million-site measurement and analysis," in Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS), Vienna, Austria, 2016, pp. 1388–1401.
[7]. U. Iqbal, S. Englehardt, and Z. Shafiq, "Fingerprinting the fingerprinters," in IEEE Symp. Security and Privacy, San Francisco, CA, USA, 2021, pp. 1143–1161.
[8]. P. Laperdrix, N. Bielova, B. Baudry, and G. Avoine, "Browser fingerprinting: A survey," ACM Trans. Web, vol. 14, no. 2, pp. 1–33, 2020.
[9]. Tor Project, "Tor Browser design and implementation," 2023. [Online]. Available: https://www.torproject.org/
[10]. C. F. Torres, H. Jonker, and S. Mauw, "FP-Block: Usable web privacy by controlling browser fingerprinting," in Proc. ESORICS, Vienna, Austria, 2015, pp. 3–19.
[11]. N. Nikiforakis, W. Joosen, and B. Livshits, "PriVaricator: Deceiving fingerprinters with little white lies," in Proc. Int. World Wide Web Conf. (WWW), Florence, Italy, 2015, pp. 820–830.
[12]. Brave Software, "Fingerprinting protection mechanisms," 2023. [Online]. Available: https://brave.com/privacy-features/
[13]. N. Andriamilanto et al., "A large-scale empirical analysis of browser fingerprints for web authentication," ACM Trans. Web, vol. 16, no. 1, pp. 1–62, 2021.
[14]. X. Lin et al., "Phish in sheep's clothing," in Proc. USENIX Security Symp., Boston, MA, USA, 2022, pp. 1651–1668.
[15]. I. Fouad et al., "My cookie is a phoenix," in Proc. Privacy Enhancing Technologies Symp. (PETS), Sydney, Australia, 2022.
[16]. G. Pugliese et al., "Long-term observation on browser fingerprinting," Proc. Privacy Enhancing Technologies, vol. 2020, no. 2, pp. 558–577.
[17]. Brave Software, "Fingerprinting protection mechanisms," 2023. [Online]. Available: https://brave.com/privacy-features/
[18]. O. Starov and N. Nikiforakis, "XHound," in IEEE Symp. Security Privacy, San Jose, CA,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 623-630
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0085

USA, 2017, pp. 941–956.
[19]. F. Alaca and P. C. van Oorschot, “Device fingerprinting for augmenting web authentication,” in Proc. ACSAC, Los Angeles, CA, USA, 2016, pp. 289–301.
[20]. J. R. Mayer, “Internet anonymity in the age of Web 2.0,” Undergraduate Thesis, Princeton Univ., 2009.