# Article information:

Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors | IEEE Conference Publication | IEEE Xplore
<https://ieeexplore.ieee.org/document/9519502>

# Article summary:

1. Browser fingerprinting is an invasive and opaque stateless tracking technique that is becoming more prevalent on the web.

2. FP-Inspector is a machine learning based approach to accurately detect browser fingerprinting, which detects 26% more fingerprinting scripts than the state-of-the-art.

3. FP-Inspector helps significantly reduce website breakage caused by countermeasures against browser fingerprinting and can be used to perform a measurement study of browser fingerprinting on top-100K websites.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article "Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors" presents a machine learning-based approach to detect browser fingerprinting, which is an invasive and opaque stateless tracking technique. The authors propose FP-Inspector, which uses a combination of static and dynamic analysis to extract syntactic and semantic features and accurately detect fingerprinting scripts. The evaluation shows that FP-Inspector detects 26% more fingerprinting scripts than manually designed heuristics and significantly reduces website breakage.

The article provides a comprehensive overview of browser fingerprinting, its origins, prevalence, and countermeasures. It also highlights the limitations of existing countermeasures such as randomization, normalization, and heuristic-based approaches. However, the article does not provide a balanced view of the potential risks associated with browser fingerprinting. While it acknowledges concerns about cross-site tracking using browser fingerprints, it also mentions legitimate uses such as bot detection and web authentication.

One potential bias in the article is its focus on detecting fingerprinting scripts rather than addressing the root cause of browser fingerprinting. The article acknowledges that mainstream browsers have started to explore mitigations for browser fingerprinting but does not discuss the effectiveness or feasibility of these mitigations. Instead, it proposes FP-Inspector as a solution to detect fingerprinting scripts without considering other approaches such as API restrictions or user education.

Another potential bias is the use of Alexa top-100K websites as a representative sample for measuring the prevalence of browser fingerprinting. While Alexa rankings are widely used as a proxy for website popularity, they may not be representative of all websites on the internet. Moreover, measuring only the presence of fingerprinting scripts may not capture their actual impact on user privacy or security.

The article also lacks discussion on ethical considerations related to detecting and blocking fingerprinting scripts. While protecting user privacy is important, indiscriminate blocking of network requests or restricting APIs can have unintended consequences such as breaking website functionality or hindering legitimate uses of JavaScript APIs.

In conclusion, while "Fingerprinting the Fingerprinters" presents an innovative approach to detect browser fingerprinting behaviors using machine learning techniques, it falls short in providing a balanced view of potential risks associated with browser fingerprinting and alternative solutions to address them. The article's focus on detecting fingerprints rather than addressing their root cause may lead to unintended consequences such as breaking website functionality or hindering legitimate uses of JavaScript APIs.

# Topics for further research:

* Limitations and effectiveness of browser fingerprinting mitigations in mainstream browsers
* Ethical considerations of indiscriminate blocking of network requests or restricting APIs
* Potential impact of browser fingerprinting on user privacy and security beyond the presence of fingerprinting scripts
* Alternative solutions to address the root cause of browser fingerprinting
* Prevalence of browser fingerprinting on websites beyond the Alexa top-100K sample
* Legitimate uses of browser fingerprinting beyond bot detection and web authentication

# Report location:

<https://www.fullpicture.app/item/bb583ed694c60b7b62a137ee08cac1fb>