Pakistan Journal of Engineering and Technology, PakJET
Multidisciplinary & Peer Reviewed
Volume: 04, Number: 01, Pages: 184- 190, Year: 2021

Analysis of Tracker-Blockers Performance

Muhammad Muzamil[1], Akmal Khan[2], Shabir Hussain[1,3], M. Zeeshan Jhandir[2], Rafaqat Kazmi[2], Imran Sarwar Bajwa[2]

[1]National College of Business Administration & Economics Rahim Yar Khan
[2]Department of Computer Science, The Islamia University of Bahawalpur, Pakistan
[3]School of Information Engineering, Zhengzhou University, Henan, China

Corresponding author: Akmal Khan (e-mail: akmal.shahbaz@iub.edu.pk).

***Abstract*-The Users are increasingly worried and conscious about privacy issues that appear during browsing the web. Web extensions such as anti-tracking, Ad-blockers, anonymity, and privacy plug-ins ensure protecting users and their privacy from third-party tracking systems. We introduce the experimental campaign to benchmarking well-known plug-ins for web privacy protection to date in this work. We set up a testbed to automatically browse usual website pages and exploit five freeware plugins. We assessed the collected data to evaluate each plug-in, considering both performance and privacy-protection angles. We found mainly famous tracker-blockers are relatively efficient in detecting as well as blocking third-party trackers. Specifically, by default, Ghostery does not provide protection; if appropriately set enabled, it offers the best protection from third-party trackers (93.99% of third-party trackers blocked). We also assessed the tracker-blockers effectiveness on client web QoE and bandwidth usage. Up to 30% bandwidth usage decreases by enabling tracker-blockers. For example, Ghostery decreases data to download by 40% and Disconnect with a 36.45% reduction. Ghostery is also faster than the baseline, with page loading 32.37% acceleration. Privacy Badger shows a negative effect on load time, with only 4.53% improvement Disconnect and Ghostery provide the best trade-off among web page quality and protection. However, Ghostery requires a manual configuration step to get the best protection from third-party tracking domains, which is difficult for users. Our study allows developers and researchers to better understand the Internet's privacy threats, possibly better performing privacy-preserving tools.**

***Index Terms*-- Ad-Blockers, Tracking Techniques, Web tracking, Web privacy.**

I. INTRODUCTION

People contact servers to obtain web pages by web browsers; many web pages contain advertisements, images, and videos. Others gather information about users' browsing activities on the web page. The website is almost funded by ads shown to users [1-8]. While the web page content is being served, it can give clues as to the significance of website ad organizations additionally depend on instruments to track and uniquely identify client activities eventually. These systems are known as third-party trackers and can uniquely identify users through different types of methods [7, 9]. These systems track users across other website pages and collect enough information about users and build their unique profiles to serve personalized advertisements. A considerable number of services are referred to as tracking systems; however, unluckily, it is tough to get a complete list due to their hidden nature.

Users are increasingly worrying regarding their online privacy reports by many surveys [10, 11]. This worry demand users to install tracker-blockers tools to protect their privacy during browsing. The latest years have seen an expansion of tracker-blockers. Adblock Plus [1], AdGuard Blocker [2], and Ghostery [3] are very famous. The latest work reported that these extensions, jointly more than 20 million users account [12]. In equivalent other systems emerged to block advertisement content, with AdBlock Plus [1] being among the most popular ones and installed by about 20% of Internet users in their browsers. AdBlock Plus detects trackers by filter requests via a set of rules crowdsourced. Regardless of the tracker-blockers impetus, modest is recognized regarding tracker-blockers and tracker-blockers efficiency. Several strategies have been introduced to detect and defend against trackers (see Section 3 for detail) by the research community. Significant effort has been spent on studying countermeasures to detect and defeat third-party trackers. However, our work has paid attention to thoroughly evaluating the efficiency of tracker-blockers.

We analyzed five notable freeware plug-ins performances in this study. Our ambition is to evaluate the utilization of the average internet client. From this end, for our benchmark, we develop a custom setup that utilizes dynamic assessments. Designing benchmarking tools needs some creativity because of the complex associations between objects and web pages' dynamic nature. Each page must be visited several times to ensure statistical significance in data. The tool must handle unpredictable events such as page timeouts and crashes, which may halt the browsing emulation. In turn, this inflates the testing time; therefore, the right balance must be considered.

We assess the effectiveness of each plug-in from a different angle to preserve users' privacy. We also validated the assertion regarding enhancing the QoE (Quality of Experience), such as decreasing bandwidth utilization and web page loading time speed up. Furthermore, to monitor the effect of the "Cookie Policy," we run experiments notification and when a user accessed for the first-time web sites present acceptance banner. Our analyses demonstrate unpredictable and surprising results. In the initial, there is a significant variation in the effectiveness of each tracker-blocker.

Ghostery [3] provides the best protection from third-party trackers, followed by Disconnect [6], AdGuard Blocker [2], and AdBlock Plus [1] offers adequate protection; however, they unable to block the least number of third-party trackers. Moreover, the Electronic Frontier Foundation (EFF) supported Privacy Badger [5] provides the least number of third-party trackers, its algorithm work with client browsing history.

We also analyzed page loading performance; data being downloaded with any tracker-blockers usually reduces because the browser fetched few contents. Despite this, the page loading time might decrease (Ghostery, Disconnect) or increase (Privacy Badger). It is because of the additional difficulty of executing the plug-in code and the different anti-tracking approaches. We have confidence that the average Internet client's existing work results help make the knowledgeable selection on tracker-blockers. Our results are useful for researchers and developers to design better tracker-blocking technologies.

A. CONTRIBUTIONS

- We build a testbed to systematically compare five (AdBlock Plus, AdGuard Blocker, Privacy Badger, Disconnect, and Ghostery famous) well-known freeware plug-ins by analyzing their performance through a setup that automatically browses the web pages.
- We perform the measurement campaign in February lasted seven days. We highlight the comparison of the tracker-blocker impact on the webpage quality. We also analyze page loading performance; data being downloaded by tracker-blockers.
- Our results are useful for researchers and developers to design better tracker-blocking technologies.
- We simulate the typical Internet client's utilization that appreciates the protection that plug-ins offer by installing one's of these web extensions.

II. LITERATURE REVIEW

Several studies [8, 13-22] have evaluated a third-party tracking system's diffusion and occurrence. Craig et al. [13] give a third-party tracking preview, demonstrating that the most significant tracking organizations domain had multiplied their affair in websites from 2005 to 2008. This paper examined the dispersion of private information at the level of website access. The present study provides details about the existing techniques used by third-party tracking systems to track users browsing history and build their profiles. There are specialized companies that track user's online activities across all friendly websites. Beyond the website's user's visit, clients supply much private information to several different websites.

A. TRACKING ON WEB

When users access the first-party site, then they are tracked by multiple entities. However, this study also focuses on the existing protection techniques available in the web market that protect third parties and such technique limitations. Furthermore, secondary privacy leakage information about users is also highlighted.

At the beginning of the website, contents were created and facilitated through a single party, organization, and group. Web pages are progressively made out of substance as numerous distinct "third-party" sites in analytics, ads, and SNS websites. In any case, a third party comes at a protection cost: researchers, policymakers have progressively pointed out how a user's browsing activities can track by third parties across websites, [8] shows technology and policy problems within the outsider tracking domain.

Utilized a passive measurement point of view, Hassan et al. [7] demonstrate that a few trackers are so unavoidable to have the capability to observe the movement of 89% of the experiential client populace. Over 80% of clients get in touch with the first tracker within 1 second after starting navigating. These days' sites are embedded in over 40 to 99 outsider tracking domains and combined individual data.

Much more worryingly, trackers are contacted when clients switch on their tablets or cell phones. Adam et al. [15] demonstrate how Web tracking has additionally significantly grown in complexity. This paper presents the longitudinal measurement of third-party web tracking behaviors from 1996 to 2016. Nowadays, the most popular websites are being tracks by the most familiar web trackers. Web trackers increase the complexity and pervasiveness to track users browsing activities.

B. WEB TRACKING MEASUREMENT TECHNIQUES

Third-party tracking services use broad fingerprinting list methods on the web to distinguish the clients [16]. The research moment branch has concentrated on determining the tracking domain. Research highlights 15 types of measurements on each site, including stateful (cookie-based) and stateless (fingerprinting-based) tracking, the effect of browser privacy tools, and the exchange of tracking data between different websites ("cookie syncing"). Open WPM and open-source tools are utilized to perfume these different types of measurements. They also demonstrate how WebRTC's capability to find neighborhood IPs without client authorization or connection is used only to track clients. They break down another fingerprinting procedure using Audio Context found during experiments. This paper mostly focuses on the fingerprinting techniques that are used to track the users.

Specifically, several studies concentrate on characterizing automatic methodologies to distinguish tracking domains [22]. Jason et al. [17] show a mechanized machine learning-based way to identify users, in which machine learning could enable tracking countermeasures that are effective and easy to use. Franziska et al. [18] develop a client-side method for detecting and classifying five kinds of third-party trackers based on how they manipulate browser state.

Generally, business sites are followed via numerous tracking domains. Multiple parties track most commercial pages, trackers vary widely in their coverage, with a small number being widely deployed, and many trackers exhibit a combination of tracking behaviors. The number of trackers can track over 20% of a client's browsing behavior. There is no current browser tool available to protect privacy from social media tracking. Simultaneously, web-based social networking sites are still allowed to track users and achieve their objectives.

III. METHODOLOGY

This section describes the methodology for the data collection and the datasets we obtain and compares tracker-blocker plug-ins' performance. Point A covers all the testbed settings that are used for data collection. Point B focuses on the websites which are used for measurements. List of trackers and types covered trackers by Point C.

A. TESTBED SETUP

To run our benchmark and setup of our dataset, we use active measurement. We build the platform on a predefined set of web pages by automatically visiting. We make a testing tool that takes the URL list as input, shown in Fig. 1; we build a browser configuration that determines the tracker blocker to test, instruments a Chrome browser to automatically visit a set of web pages, and then collect navigation data and elaborate statistics. We rely on Selenium HQ [19], a toolset for web browsers, an automation instrument Chrome browser within python scripts, and a connector for all popular web browsers (such as Mozilla Firefox, Safari, Mobile browser, and Edge).

URLs visited by configuring Chrome browser, dump statistics through HTTP Archive files (HAR [20]). In short, web pages visited of given set, and profiles set, the profile loads by Selenium, runs Chrome browser, gives it a chance to visit apiece web page and return with the Onload event wait for the browser. We discard the visit and undertake some specialized technical issues when the event is not triggered within a 100s timeout. We embed a latency time of 6s between consecutive visits. The HAR extract from the navigation of the browser created data at the end of each visit.

The HTTP Archive file is a JSON-formatted container for HTTPS tracing data recording. The HTTP Archive file encompasses an entry for every website page object request. This section incorporates data, for example, statistics about the content (e.g., download time, size) and timings (e.g., get a URL, time to fetch DNS info). After each visit, we look out to remove the browser cache and enhance the experiment's reliability; each webpage visited five times.

B. DATA COLLECTION

We deliberate the situation in which a client is browsing the website on his device. We characterize the arrangement of web pages to visit with well-known top 40 sites. We collect these websites by using Google search. For more points of interest, we select four categories of site pages; also, for every class and discretionarily choose ten different well-known websites in Pakistan. Specifically, Google Search first returned for every class. The whole list of web pages we report, assembled by category Table 1.

We initially start with no plug-in installed to build a baseline; in the remainder of the work, we call it Plain, as a set of profiles. At that point, for every tracker-blocker, we manually install the comparing plug-in through which make a new Chrome profile. Therefore, in all-out, we acquire six diverse browser profiles. From the official Chrome add-on page, we install each plug-in. Except for Ghostery [3] utilizes the default setup for every one of them. Surprisingly, we found that it does not empower any filtering ability by default Ghostery to protect web pages from web tracking. While it requires the client to manually set the setting of Ghostery to develop protection from web tracking, such as a client first needs to create an account on Ghostery, second sign into Ghostery account, then choose propelled options web pages turn on protect. We follow all these steps to save web pages from web trackers and to test our experiment.

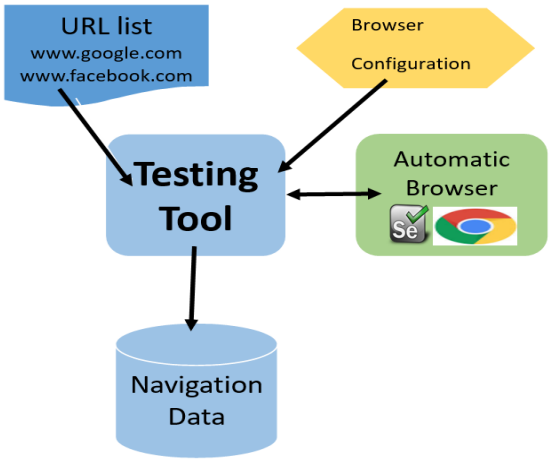

FIGURE 1. A Framework of Tracker-Blocker Measurement.

To assess the effect of the cookie's regulations, we make two settings of the browser (along these lines multiplying the number of profiles): we don't give consent to TP cookies (third-party) in the first one, with the goal that every visit we perform compares to a "first visit"; after that, all the pages visited manually, also when the "Accept Cookie" notification obtainable, we explicitly clicked on it. When every third party and first-party domain being seen, the browser eventually accepts any cookie, the visit to the site subsequently compares to a "second visit." We retain the cookie database and delete the cache of the browser at the end. Altogether, we visit five times each. The website pages change their substance and can be extremely dynamic amid the day, such as news sites.

E-Commerce	Forums	News	Sports
www.Daraz.pk	www.ppsc.gop.pk	www.Dawn.com	www.pcb.com.pk
www.Olx.com.pk	www.hamariweb.com	www.javedch.com	www.Psl-t20.com
PakWheels.com	stackoverflow.com	Dailypakistan.com.pk	www.cricingif.com
www.Zameen.com	www.nts.org.pk	www.Jang.com.pk	pakpassion.net
Shophive.com	www.urdupoint.com	Tribune.com.pk	pakhockey.org
Homeshopping.pk	*www.Rozee.pk*	Dunyanews.tv	pakfootball.org
Yayvo.com	www.Blogspot.com	express.com.pk	footballpakistan.com
www.Symbios.pk	yamaha-motor.com.pk	www.bbc.com	espncricinfo.com
technologytimes.pk	www.Hec.gov.pk	TheNews.com.pk	www.cricbuzz.com
Whatmobile.com.pk	www.Paperpk.com	www.Siasat.pk	cricketgateway.pk

Table 1: Websites are grouped by category considered in this research.

Subsequently, we precisely outline our tests, so a similar website page is visited by various profiles in a couple of minutes, boosting the likelihood of experiencing a similar substance. We build to set up for this, the first one without agrees to third-party cookies and the second one with agreeing to third-party cookies. For this experiment, we utilize a Windows-based Intel Core i3 Quad machine equipped with 4GB RAM, using public IP address and a 12mb/s network connected to the Internet.

C. TRACKING LIST

To collect the data about tracker classifications, we used to parallel the also Selenium HQ [19] to drive the automatic Chrome web browser as we discuss above to load every web page. We use Tracking Observer [21] as a Chrome web browser extension that acts as a stage for blocking third-party web trackers, measuring, and detecting. We use the Tracking Observer extension, a browser-based web tracking detection platform. Tracking Observer doesn't utilize a blacklist of known tracking domains; unlike different apparatuses, it automatically detects trackers based on their in-browser behaviors, such as getting and setting third-party cookies than using a blacklist. Diverse trackers display specific actions, which provide them various capacities. For instance, a few trackers can track you just when you come back to a similar site, while others can follow you as you peruse various diverse websites. According to the taxonomy, as discussed above, Tracking Observer automatically classified the trackers.

For analysis purposes, the outcomes were set joint for reporting, and this procedure was repeated. To conclude, the web trackers list be in touch for every web page we processed the resulting data. We visit 40 unique web pages; as discussed above, this process was repeated; we clean the browser, cookie database, and cache at the end.

A tracker can be more than one type. A tracker can be found in more than several different kinds of categories. We classify the types of the tracker by following [6] work. Our analysis based on a cookie-based tracker, a single tracker, may show diverse behaviors crosswise over page loads or various websites.

Analytics (Tracker A): Implements website analytics functionality by a script that the tracker provides. A script characterized analytics trackers, the script runs in the first-party context, but it is sourced from a third party, first-party cookies set by that context, and those cookies leak later to the tracking site.

Vanilla (Tracker B): Uses third-party cookies to track clients crosswise over websites. The top-level page includes the tracker as a third party, for example, an iframe.

Referred (Tracker D): Rather than on its tracker cookies, the tracker depends on an additional tracker to escape distinctive identifiers. In a speculative illustration, adnet.com may put its cookie and afterward unequivocally release that cookie in solicitations to alluded third party cads.com. For this situation, to perform tracking, ads.com not requires to set its cookies.

Personal (Tracker E): Personal trackers typically show up as social gadgets (e.g., "tweet" or "Like" buttons). The private tracker acts like a Vanilla tracker; however, the client visits directly into different contexts. Referred Analytics (Tracker F): The tracker like an Analytics tracker; however, the first-party cookie sets by domain is not the same as the domain to which the first-party cookie is later spilled.

This arrangement is constructing totally in light of the tracker that can be seen from the user side. In this manner, it doesn't detect back-end tracker behavior, for example, connecting a client's browsing conduct utilizing machine and browser fingerprinting methods or the back-end trade of information among trackers. Thus, the prevailing sort of tracker experienced by a client relies upon the client's browsing.

IV. RESULTS

We are keen to understand the effectiveness of trackers-blockers and measure the trackers-blockers effect on the browsing Quality of Experience (QoE) the clients perceived. Consequently, we extract from the HTTP Archive (HAR) files and the Tracking Observer extension the following metrics: Contacted List of Trackers: this metric includes a list of trackers contacted through the browser for each page. Types of Trackers: this metric includes different types of trackers contacted through the browser for each page. Load Time: the time required to display, download overall elements that include on the web page. Precisely, we measure this on the Onload event. Contacted List of Trackers (CLT) and Types of Trackers enable us to identify how efficient every tracker-blocker is by ensuring clients' privacy. Load Time (LT) and Volume (Vol) allow us to understand each plug-in's impact on the page loading speed. In this case, smaller Load Time and Volume should interpret better Quality of Experience (QoE) that the

clients perceived, assuming that all substances expected to render the web page are loaded correctly.

A. TRACKERS-BLOCKERS PROTECTION FROM TRACKERS

First, we analyze the efficiency of trackers blocker's performance that protects client's privacy. We collect the numbers of unique trackers that are contacted by using the Tracking Observer extension. Total individual trackers that have not been blocked represents by CLT size. Thus, the large size of CLT considered browser profile weaker privacy protection.

We compute the results of the overall visit of the given profile in Fig. 2; the leftmost bar represents our baseline result; we call it straight with no plug-in installed. Other browser profiles are sorted by numbers of the unique number of third-party trackers, CLT. Let us focus on tracker-blockers performance; the tracker-blockers demonstrate relatively diverse behaviors. The best one is Ghostery that which misses a couple of third-party trackers. Exactly, eight unique third-party trackers for 50% of web pages visited.

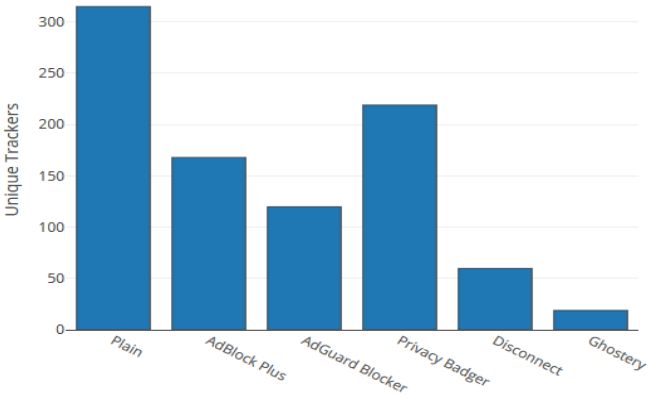

FIGURE 2: The number of the contacted list of trackers, CLT.

We notice that most third-party trackers belong to Facebook and Google ecosystems, such as facebook.com and fonts.googleapis.com. We collect such third-party trackers by using the TrackingObserver extension. For example, we visit www.Yayvo.com, which requires support objects fetch by browser from third party platform addthis.com. We summarize that Ghostery filters out third-party trackers with significant accuracy. The second best is a Disconnect that misses fewer numbers of third-party trackers. In the next rank, AdGuard Blocker and Adblock Plus, although not specialized in detecting third-party trackers, block most third-party trackers compared to the plain (baseline). Moreover, Privacy Badger does not block many third-party trackers, and it shows poor performance. However, Privacy Badger is used differently to blocks third-party requests. Its blocking abilities are depending to a great extent on the pages that have already been visited.

In summary, we found very famous ones among the third-party trackers, for example, scorecardresearch.com, doubleclick.net. On average, Ghostery reduces 93.99% the number of unique third-party trackers as compared to baseline. Second, the best Disconnect reduces 80.9% of them; after that, AdGuard Blocker and Adblock Plus with 61.9%, 46.67% reduction respectively. At last, Privacy Badger with 30.48% reduction.

B. *TYPES OF THIRD-PARTY TRACKERS*

Now we are interested in how many types of third-party trackers they block; for this, we classified third party requests into five different tracking types by using Tracking Observer [21]. The leftmost bar represents the baseline results in which the first one is analytics tracking type with 7.21%, the second one is vanilla tracking, which is larger one among the others with 81.68%, followed by referred tracking, personal tracking, and referred analytics tracking with 6.61%, 0.90%, 3.60% respectively, in Fig. 3.

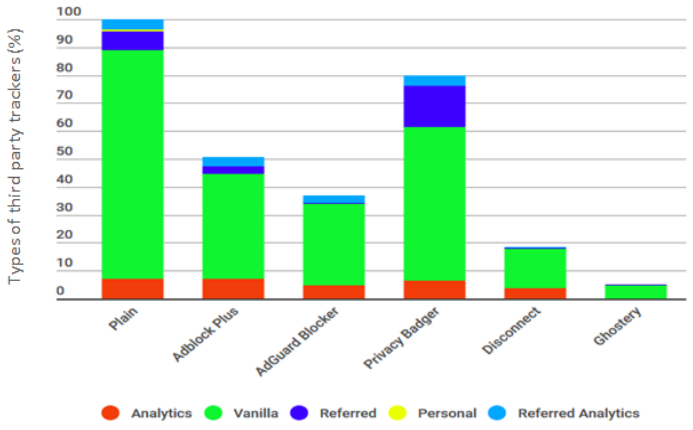

FIGURE 3: Unique types of third party tracking (%).

Adblock Plus is undoubtedly a very famous adblocker; moreover, according to our findings, it blocked the least amount of referred analytics types of trackers and stopped almost more than 50% of vanilla and directed types of trackers. However, Adblock Plus fails to blocks analytics types of trackers in our measurements. Moving on, AdGuard Blocker misses few referred analytics types of trackers and blocks 99% of referred trackers. Additionally, it blocks more than 60% of analytics and vanilla trackers as compared to baseline. Surprisingly, the number of analytics trackers increase by more than 50% rather than decrease by Privacy Badger, comparing to baseline results. Even fails to block referred analytics trackers and blocks 20%, 2% of analytics, and vanilla trackers, respectively. Disconnect completely blocks referred tracker, misses few third-party trackers of analytics and referred analytics trackers, and blocks 80% of vanilla trackers. The best one, Ghostery, blocks the analytics and referred analytics trackers completely misses the least amount of referred trackers and almost 96% blocks of vanilla types. Additionally, personal types of trackers blocks by all tracker-blockers.

C. PAGE LOAD TIME

After installing the tracker-blockers, our focus on investigating how fast the browser is to render the pages. Page load time, PLT, reports in Fig. 4.

The results show that tracker-blockers reduce the time it takes to load a web page by blocking third parties requests, on average. We observe that trackers-blockers decrease the page render time by filtering many third parties to contact by comparing the baseline results with profile installing tracker-blockers results. On average, Ghostery is 32.72% faster than the plain; AdGuard

Blocker Disconnect and Adblock Plus improve the average load time by 14.88%, 15.43%, and 12.20%, respectively. Privacy Badger even increases the page loading speed, too, with only 4.53% improvement.

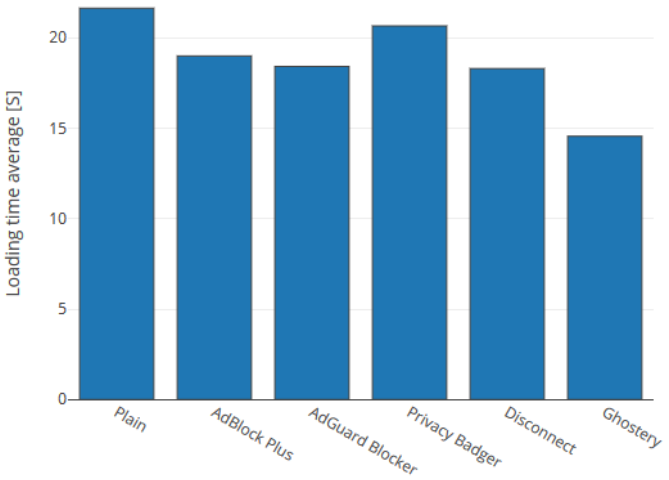

FIGURE 4: Average page load time, PLT.

D. AVERAGE BANDWIDTH SAVING

We are now observing the tracker-blockers provided bandwidth saving. The entire volume of the page to render the volume, Vol, is shown in Fig. 5.

The result shows that tracker-blockers reduce the amount of data to download the page. Instinctively, the tracker-blocker that is betters to blocks third-party trackers then saves the larger bandwidth. Ghostery decreases the amount of data to download by 40% and disconnects with a 36.45% reduction. Then, we notice AdGuard Blocker with 22.24% saving, followed by Adblock Plus with an 18.5% reduction. At last, Privacy Badger provides the least amount of data saving 11.96% only.

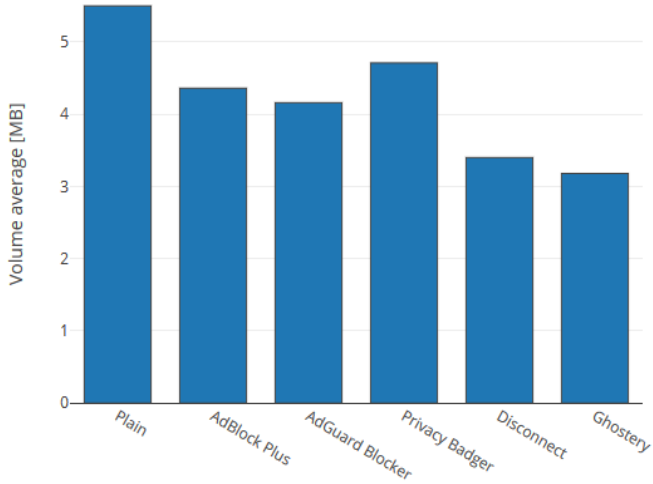

FIGURE 5: Volume average [MB].

E. PER CATEGORY RESULTS

We now focus on understanding the behavior of tracker-blockers on each website page category. We report per-category results in Table 2. The contacted unique third-party trackers (average number) computed during every visit produced via the comparing website pages to browser profile (row) belonging to the relating category (column). Rows and columns sort by the average number of third-party trackers. First row, our baseline (plan profile) includes most numbers of third-party trackers; more interestingly, not similar behavior displays by all categories.

Table 2: Per-category unique trackers (average)

Profile	E-commerce	Sports	News	Forums
Plain	12	8.5	7.6	4.4
Privacy Badger	10.2	5.5	6.8	3.4
Adblock Plus	6.4	3.3	3.1	4
AdGuard Blocker	4.9	3	2.3	1.8
Disconnect	2	1.8	1.3	0.9
Ghostery	0.2	0.6	0.6	0.5

Even though E-commerce, Sports, and News categories are popular among (Pakistani) users, the website pages belonging to these categories host most third-party trackers. Focus on tracker blockers performances, Privacy Badger displays weak performance, and Ghostery blocked many third-party trackers.

V. CONCLUSION

We introduced a systematic comparison and benchmark of tracker-blockers. We utilized sizable dataset summaries to assess various tracker blockers' efficiency to qualitatively estimate how they affect web Quality of Experience (QoE) and clients' browsing protection from third-party trackers by automatically generating traffic. We found mainly famous tracker-blockers are relatively efficient in detecting as well as blocking third-party trackers. Specifically, by default, Ghostery does not provide protection; if the setting correctly enabled, then it gives the best amount of protection from third party trackers (93.99% of third-party trackers blocked) and few third-party trackers missed by Disconnect, while AdGuard Blocker and Adblock Plus provide minimal protection from trackers, which are unexpectedly not able to block prevalent third party tracker domains. We analyzed different third-party trackers blocked by tracker-blockers; the results show much difference in tracker blocker's behavior to block requests to distinct kinds of third-party trackers domains. We also assessed the tracker-blockers effectiveness of client web QoE and bandwidth usage. Up to 30% bandwidth usage decreases by enabling tracker-blockers. For example, Ghostery decreases data to download by 40% and Disconnect with a 36.45% reduction. Ghostery is also faster than the baseline, with page loading 32.37% acceleration. Privacy Badger shows a negative effect on load time, with only 4.53% improvement. We believe our results help practitioners and developers design better tracker-blocking technologies and support the normal web client make a knowledgeable selection of tracker-blockers.

REFERENCES

[1] Plus A, The world's #1 free ad blocker, March 20, 2021

[2] [Online] privacy made easy. (2021, March 04). Retrieved March 20, 2021, from https://www.ghostery.com/

[3] [Online] A fast and efficient ad Blocker. easy on CPU and memory. (2019, July 24). Retrieved March 20, 2021, from https://www.ublock.org/

[4] [Online] Privacy badger. (n.d.). Retrieved March 20, 2021, from https://www.eff.org/privacybadger

[5] [Online] https://disconnect.me.

[6] Metwalley, Hassan, Stefano Traverso, Marco Mellia, Stanislav Miskovic, and Mario Baldi. "The online tracking horde: a view from passive measurements." In International Workshop on Traffic Monitoring and Analysis, pp. 111-125. Springer, Cham, 2015.

[7] Mayer, Jonathan R., and John C. Mitchell. "Third-party web tracking: Policy and technology." In 2012 IEEE symposium on security and privacy, pp. 413-427. IEEE, 2012.

[8] Li, Tai-Ching, Huy Hang, Michalis Faloutsos, and Petros Efstathopoulos. "Trackadvisor: Taking back browsing privacy from third-party trackers." In International Conference on Passive and Active Network Measurement, pp. 277-289. Springer, Cham, 2015.

[9] Hoofnagle, Chris Jay, Jennifer M. Urban, and Su Li. "Privacy and modern advertising: Most us Internet users want'do not track'to stop collection of data about their online activities." In Amsterdam privacy conference. 2012.

[10] Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. "Americans reject tailored advertising and three activities that enable it." Available at SSRN 1478214, 2009.

[11] [Online] Quantable.https://www.quantable.com/analytics/how-many-users-block-google-analytics/.

[12] B. Krishnamurthy and C. Wills, "Privacy diffusion on the web: a longitudinal perspective," in Proceedings of the 18th international conference on World Wide Web. ACM, 2009.

[13] Altaweel, Ibrahim, Nathan Good, and Chris Jay Hoofnagle. "Web privacy census." 2015.

[14] A. Lerner, A. K. Simpson, T. Kohno, and F. Roesner, "Internet jones and the raiders of the lost trackers: An archaeological study of web tracking from 1996 to 2016," in 25th USENIX Security Symposium, 2016.

[15] S. Englehardt and A. Narayanan, "Online tracking: A 1-million-site measurement and analysis," in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2016.

[16] J. Bau, J. Mayer, H. Paskov, and J. C. Mitchell, "A promising direction for web tracking countermeasures," in Proceedings of the Web 2.0 Security and Privacy conference. IEEE, 2013.

[17] F. Roesner, T. Kohno, and D. Wetherall, "Detecting and defending against third-party tracking on the web," in Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation., 2012.

[18] [Online]Selenium Web Browser Automation, http://www.seleniumhq.org/.

[19] [Online] http://www.softwareishard.com/blog/har-export-trigger/

[20] Pujol, Enric, Oliver Hohlfeld, and Anja Feldmann. "Annoyed users: Ads and Ad-block usage in the wild." Proceedings of the ACM Conference on Internet Measurement Conference, 2015.

[21] Kaizer, Andrew J., and Minaxi Gupta. "Towards automatic identification of javascript-oriented machine-based tracking." Proceedings of the ACM on International Workshop on Security and Privacy Analytics, 2016.

[22] Storey, G., Reisman, D., Mayer, J., & Narayanan. "The Future of Ad Blocking: An Analytical Framework and New Techniques." arXiv, 2017.