Implementing Cryptojacking as a Web Monetization Model for Increased Privacy

MSc Research Project
MSc Cybersecurity

Harshit Sharma
Student ID: x21157081

School of Computing
National College of Ireland

Supervisor: Mr. Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Harshit Sharma		
Student ID:	x21157081@student.ncirl.ie		
Programme:	MSc Cybersecurity	**Year:**	2022-2023
Module:	MSc Research Project		
Supervisor:	Mr. Imran Khan		
Submission Due Date:	1st February 2023		
Project Title:	Implementing Cryptojacking as a Web Monetization Model for Increased Privacy		
Word Count:	10411	**Page Count:**	39 including Appendix

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Harshit Sharma

Date: 1st February 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Implementing Cryptojacking as a Web Monetization Model for Increased Privacy

Harshit Sharma
Student ID-x21157081@student.ncirl.ie

Abstract

Web applications or companies behind the web application tend to collect user data and perform psychographic profiling. Users are served with personalized or targeted advertisements. Laws for protecting user privacy exist but may not be helpful in protecting the privacy of the user. The research investigates, classifies, and compares cookies based on user consent. The study also explores cryptojacking or in-browser cryptocurrency mining as a solution for monetization in exchange for the services web applications provide and how it can help reduce user profiling or cookie-based trackers in the browser. The research also explores an alternate lightweight cryptocurrency that could be mined in a browser or on a low-grade CPU like a mobile phone or a tablet so that it can be used for the mining process and is resource efficient in nature. The study explores various consensus algorithms to determine the control points for selecting an appropriate cryptocurrency so that it is more energy efficient than cryptocurrencies based on proof of work consensus algorithm such as monero[1].

1 Introduction

1.1 Background

The internet has become an indispensable part of our daily life; The internet provides a lot of technological enablement that enables users to perform a plethora of tasks, whether it is consuming content like watching a movie or ordering food and socializing, or connecting with peers, or even scheduling a meeting. The internet has equipped many companies or organizations with a state-of-the-art infrastructure by the means by which they are able to provide services to their users. The internet user or the service consumer has access to cutting-edge technology and web applications but at the cost of their privacy.

1.2 Motivation

Users of a social networking web application called Facebook had their data mined and sold without their consent, and the users were being served targeted advertisements in order to influence an election (Isaak and Hanna, 2018). The scandal was named "Cambridge Analytica". This scandal led to the disclosure of the fact that Facebook user data was mined, but a point to note is the typical internet user is unaware of how many similar scandals have occurred in the past or are likely to take place in the future. Additionally, it is possible that there have been breaches of which the general public is unaware. Post this scandal, GDPR also came into full

[1] https://www.getmonero.org/get-started/what-is-monero/

force, which is a data protection law that helps protect the privacy of users on the internet(Li et al., 2019). Despite laws such as GDPR, companies behind the web applications or services still manage to collect user data. Companies behind these web applications tend to have found some loophole and keep exploiting user privacy. During my study, on 6th December 2022, the parent company of Facebook called "Meta's" business model to serve their user's personalized advertisements was declared illegal[2]. According to a privacy statistic, 67% of internet users in the US are not aware of their country's Privacy[3].

It is also essential for the companies behind these web applications to make money or generate revenue to keep providing their users the intended services; at the same time, it is utterly unethical of these companies to collect user data and exploit their privacy and carry out psychographic profiling to serve targeted advertisements, in layman terms, it is like playing with the human mind (Mandal et al., 2017). Web applications rely majorly on cookies to collect user data, and even after GDPR, these companies still manage to embed cookies that track their users without their consent.

The research also explores Cryptojacking, also knowns as in-browser cryptocurrency mining, which is an application of blockchain technology as a viable solution that could be offered to the users entirely or as a substitute for targeted advertisement and would enable the service providers/web applications to generate revenue. Cryptojacking involves a hacker inserting JavaScript into a web application so that when a user browses it, the resources of their computer are utilized to mine cryptocurrency, which is then sent to the attacker's wallet. This could be utilized as a monetization method, where users are made aware of cryptocurrency mining and are given a choice to allow or deny it. This would provide web applications/companies with a revenue stream instead of collecting data and displaying ads to users. Web applications/companies could offer their services in exchange for allowing cryptojacking or cryptocurrency mining. (Papadopoulos et al., 2018).

1.3 Research Question

The main intent of the research project is to investigate how cryptojacking can help improve user privacy if it is used as a method of monetization and investigate and gather evidence if, after rejecting non-essential cookies, the tracker cookies which track the user or collect data or perform profiling are still embedded in the browser, in order to seek answers for the below-given research questions.

- **How using cryptojacking as a method of monetization can improve user privacy and prevent cookie-based user tracking?**

- **If users are still getting targeted or tracked by cookies without their consent, after they have declined non-essential cookies?**

1.4 Research Objective

The objective of this research is to study cookies and classify them as trackers or functional cookies based on the data available publicly and from the privacy policy of the respective services. The comparison must be drawn between the cookies for the instance when the user accepts all cookies and from the instance when the user rejects non-essential cookies in order

[2] https://noyb.eu/en/noyb-win-personalized-ads-facebook-instagram-and-whatsapp-declared-illegal
[3] https://legaljobs.io/blog/privacy-statistics

to determine if the same cookies classified as a tracker are still being embedded in the browser even after rejecting non-essential cookies. Exploring a lightweight cryptocurrency solution or API which provides the functionality of in-browser cryptocurrency mining or cryptojacking such that the mining process is not resource-intensive and profitable.

1.5 Contribution to the scientific literature

The research aims to provide evidence to support the fact that web applications continue to track users without their consent and help determine the appropriate cryptocurrency that is resource efficient for in-browser mining that can help reduce trackers and increase privacy for the users.

1.6 Structure of the paper

The paper mentions the previous work and problems associated that are aligned with the research, the methodology used for the research, and the design specification followed by implementation and evaluation.

2 Related Work

2.1 The need for cookies

Web applications collect user data in the name of improved experience, but this is a major issue that needs to be addressed. Companies have different terms for tracking users, often disguising it as user data collection, yet it's a breach of privacy (Schneier, 2015). The internet relies on TCP/IP suite for communication. The HTTP protocol, used for web applications, is stateless in nature by default. To make it stateful, cookies are used for session management and authentication (Gutzmann, 2001). This means that each subsequent request from a browser is independent of a previous one. Without cookies web application would not be able to provide the intended functionality.

2.2 Privacy issues and Cookies and Data collection practices

Cookies used by applications can be insecure, so they must be secured with flags and tested for against security controls. If the cookie is not secure, it will be sent in an HTTP request and may reveal personal data. The name, value and path attributes of the cookie contain data and related URIs. First and third-party cookies are used by web applications, with third-party cookies used to track user behaviour, which has caused privacy issues (Cahn et al., 2016), but 1st party cookies are being designed to track users as well. Web applications can use cookies responsibly but may still collect personally identifiable information. It is troubling to think of data brokers buying and selling user data. Cookies are necessary for intended function, and 3rd-party ones can be designed to track user actions and display advertisements. Third-party Cookies can be fashioned to enable marketers/data-collectors to observe all user activity and background, thereby enabling them to show users applicable advertisements at the appropriate time (Schwartz, 2001). Cookies are essential, however, cookie data can be collected and used by companies to make decisions, such as declining applications for insurance, given that they collect relevant data about the user like a previous health condition. Furthermore, web applications can collect and sell data to data aggregators or brokers, even if it is not relevant to them (Schwartz, 2001)(Choi et al., 2019).

2.3 Targeted Ads, Privacy Breach, and Social Networks

Companies have been collecting and trading user information through websites and the internet for the purpose of targeted marketing. This raises privacy concerns. Current internet infrastructure cannot ensure privacy, but hardcore cryptography could be a potential solution. To ensure privacy, significant changes must be made to the infrastructure.(Mandal et al., 2017). Social network or similar services share user data with 3rd-parties, such as researchers and ad networks, which makes data vulnerable to reidentification and information disclosure attacks. Privacy-preserving techniques are required and an active research area. Despite the efforts of social networking platforms to clean data or sanitize data before it is shared, it can still be used to identify individuals as the sanitization can be reversed. Evidence of this is currently available (Abawajy et al., 2016).

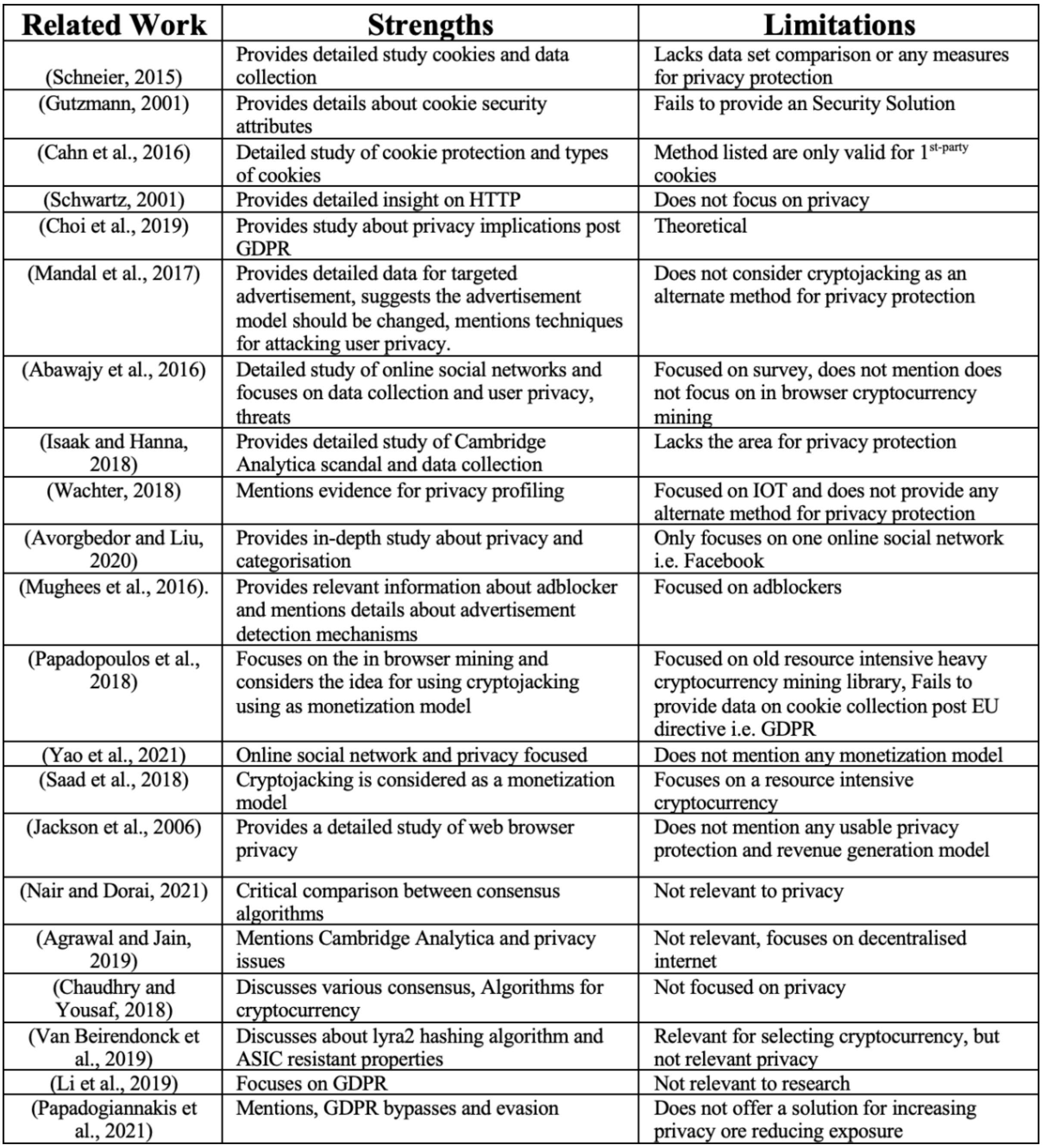
2.4 Cambridge Analytica, GDPR and Privacy Concerns

Cambridge Analytica was data scandal, where user data of 87 million users was mined without user consent and used against the users to serve them targeted advertisements in order to influence an election, psychographic profiling(Isaak and Hanna, 2018), to protect users GDPR(Li et al., 2019) was introduced. It allowed users to request data deletion, and mandated social media platforms to write privacy policies in plain english. However, the current monetization model needs to be altered to guarantee user privacy, as GDPR does not provide full assurance (Wachter, 2018). (Papadogiannakis et al., 2021) In their paper have discussed various methodologies of browser finger printing and clearly mentioned significant proof of how companies are able to bypass user consent and GDPR to track users.

2.5 Cryptojacking as monetization model and the search for a practical cryptocurrency

(Papadopoulos et al., 2018) Reflects on the concept of browser-based cryptocurrency mining, also known as cryptojacking, as a potential monetization mechanism i.e. exchanging services for cryptocurrency mined on the users resource. According to previous research, this model could be an effective way of making money, provided that data collection is stopped, or the user is presented with the choice between sharing data or permitting cryptojacking. The researcher questions the practicality of mining when it comes to normal low-end devices such as mobile phone or a laptop and concludes that it will not be efficient and resource-intensive. The main focus of their research was a cryptocurrency called monero, the research was done in 2018. In 2022 there is some solution that could be used to enable cryptojacking. Monero was based on proof of work consensus algorithm, which requires mining to process and verify transactions and uses a lot of energy and computing power, while cryptocurrencies based on proof of stake consensus do not need much energy as the mining or reward is awarded randomly and cryptocurrency is earned just for holding or maintaining the network(Nair and Dorai, 2021) (Chaudhry and Yousaf, 2018). There are multiple factors such as consensus algorithm, hashing algorithm, design, etc that affects the mining capabilities of a cryptocurrency, (Van Beirendonck et al., 2019) mentions that certain cryptocurrencies are mineable on less powerful computer chips given that they are based on a certain hashing algorithm.

Thus, the current research is valid but outdated. Certain alternatives could be explored from the drawing controls from the existing research both for gathering and classifying cookies for evidence and researching a new cryptocurrency that could be used for monetization and, in turn, enable increased privacy. Given below is a table comparing strength and limitation.



Related Work	Strengths	Limitations
(Schneier, 2015)	Provides detailed study cookies and data collection	Lacks data set comparison or any measures for privacy protection
(Gutzmann, 2001)	Provides details about cookie security attributes	Fails to provide an Security Solution
(Cahn et al., 2016)	Detailed study of cookie protection and types of cookies	Method listed are only valid for 1$^{st-party}$ cookies
(Schwartz, 2001)	Provides detailed insight on HTTP	Does not focus on privacy
(Choi et al., 2019)	Provides study about privacy implications post GDPR	Theoretical
(Mandal et al., 2017)	Provides detailed data for targeted advertisement, suggests the advertisement model should be changed, mentions techniques for attacking user privacy.	Does not consider cryptojacking as an alternate method for privacy protection
(Abawajy et al., 2016)	Detailed study of online social networks and focuses on data collection and user privacy, threats	Focused on survey, does not mention does not focus on in browser cryptocurrency mining
(Isaak and Hanna, 2018)	Provides detailed study of Cambridge Analytica scandal and data collection	Lacks the area for privacy protection
(Wachter, 2018)	Mentions evidence for privacy profiling	Focused on IOT and does not provide any alternate method for privacy protection
(Avorgbedor and Liu, 2020)	Provides in-depth study about privacy and categorisation	Only focuses on one online social network i.e. Facebook
(Mughees et al., 2016).	Provides relevant information about adblocker and mentions details about advertisement detection mechanisms	Focused on adblockers
(Papadopoulos et al., 2018)	Focuses on the in browser mining and considers the idea for using cryptojacking using as monetization model	Focused on old resource intensive heavy cryptocurrency mining library, Fails to provide data on cookie collection post EU directive i.e. GDPR
(Yao et al., 2021)	Online social network and privacy focused	Does not mention any monetization model
(Saad et al., 2018)	Cryptojacking is considered as a monetization model	Focuses on a resource intensive cryptocurrency
(Jackson et al., 2006)	Provides a detailed study of web browser privacy	Does not mention any usable privacy protection and revenue generation model
(Nair and Dorai, 2021)	Critical comparison between consensus algorithms	Not relevant to privacy
(Agrawal and Jain, 2019)	Mentions Cambridge Analytica and privacy issues	Not relevant, focuses on decentralised internet
(Chaudhry and Yousaf, 2018)	Discusses various consensus, Algorithms for cryptocurrency	Not focused on privacy
(Van Beirendonck et al., 2019)	Discusses about lyra2 hashing algorithm and ASIC resistant properties	Relevant for selecting cryptocurrency, but not relevant privacy
(Li et al., 2019)	Focuses on GDPR	Not relevant to research
(Papadogiannakis et al., 2021)	Mentions, GDPR bypasses and evasion	Does not offer a solution for increasing privacy ore reducing exposure

Figure 1: Literature Review Table.

3 Research Methodology

Examination of previous research papers and methodologies indicates that data privacy for users online has been a stumbling block for more than 20 years (Mandal et al., 2017; Schwartz, 2001). The use of stateful HTTP protocol with cookies has further exacerbated the privacy crisis. It is commonly accepted that setting flags on cookies is a way to secure them (Cahn et al., 2016), but this method is not foolproof, as 1st-party cookies used by web applications can be secured and flags can prevent cross-domain communication (Jackson et al., 2006), yet 3rd-party cookies, which are solely used for tracking users, are not protected or are not given additional cookie attributes/flags by design. Different approaches have been proposed for addressing the issue, such as categorizing data (Avorgbedor and Liu, 2020), employing collection methods, encryption, and different infrastructure models (Agrawal and Jain, 2019), and introducing differential privacy models/frameworks (Yao et al., 2021). However, these attempts have not been successful due to the increasing popularity of online social networks, and a change in the current infrastructure for advertisement and profiling or retargeting is necessary (Mandal et al., 2017).

Classification of Cookie.

This research paper suggests an alternative strategy, which involves selecting a group of web applications, such as online social networks, search engines, or other web applications, based on an examination of prior methods. Post selection of all web applications, cookies would be identified and classified according to their data or behaviour, keeping the website tracking configuration on default or, in layman's terms agreeing to accept all cookies; a control point that marks cookies as "Tracker" on the nature if the respective cookie is used for tracking user is defined. Similarly, cookies that are essential to the application would be marked as "Functional", considering the fact that the cookie does not track user is used for applications like storing preferences or making the application session stateful. The practice mentioned above is run twice. i.e., Classifying cookies as tracker or functional for two different data set as described below.

Cookies classified as a tracker for the instance when the user accepts all cookies are stored as “**Data Set A**”, and for the instance when the user rejects all cookies, cookies must again be inspected or classified and stored as “**Data Set B**”. A third data set called “**Data Set C**” comprises N cookies, where N is any number of functional cookies is constructed; Data set C does not contain any cookies classified as a tracker as it uses in-browser cryptocurrency mining as a solution to exchange services; thus trackers are not required, this data set can be self-defined considering the fact that the implementation of the proposed model is done and we have a working in-browser cryptocurrency mining and cryptojacking being an entirely different model for revenue generation.

All three data sets are compared and evaluated in order to determine if the user is still being tracked after rejecting non-essential cookies or reject cookies by comparing the number of cookies classified as trackers for both data set A and Data set B, Presence of cookies classified as tracker in data set B gives the evidence and proves users are tracker even after rejecting non-essential cookies or reject cookies without the user consent.

For data set C, number of cookies classified as a tracker are assumed to be zero as it is a completely different model for monetization due to the fact that the proposed model does not rely on trackers for revenue generation and does not serve targeted advertisements.

Gathering Data Set A and Data Set B.

For the cookie collection and classification, For Data Set A, Chrome Browser with an incognito tab was used. Chrome browser has 3rd party cookies blocked by default. Other browsers also have 3rd party cookies blocked by default. 3rd party cookies are blocked by default in all browsers across all devices, makes analysing 3rd party cookies out of scope and not relevant to research; thus, cookies installed only by the web application itself are analysed. In order to collect data, target web applications were surfed, and cookie collection for the data set was conducted; the cookies were classified on the basis of behaviour and data available about the cookies in the public domain. Similarly, for data set B, the same configuration and methodology were used. The data was stored in a xl file with control points such as name, URL, type, description, maximum retention time, description, and source link.

Selection of Browser Minable cryptocurrency/Cryptojacking API.

In order to select the cryptocurrency and Browser mining API, previous research papers were referred, It was determined that most of the previous APIs and cryptocurrencies mentioned were no longer available to use or the projects were shut down, also as pointed out in the previous paper cryptocurrencies were subjected as an impractical idea for monetization on the internet due to the fact the profitability and resource intensive nature.(Saad et al., 2018). Some control points were drawn from the previous research, and cryptocurrencies were studied, and more research papers were referred from previous research. Some control points were drawn, such as Ensuring the cryptocurrency uses POS. i.e, which is proof of stake instead of proof of work algorithm. The cryptocurrency must be mineable in the browser or on low-end devices such as a tablet, the cryptocurrency should not be resource-intensive and must be resource efficient and should draw less energy(Chaudhry and Yousaf, 2018; Nair and Dorai, 2021b) and. It must use the Lyra2 hashing algorithm, and there should be an API that makes it easy to enable an existing web application to move to the proposed model which using cryptojacking as a method of monetization. Using these controls, new cryptocurrencies and APIs were researched.(Van Beirendonck et al., 2019)

In order to draw a comparison between data sets and the classification of cookies, "google sheets" was used. The data is stored in a file along with all the control points as specified earlier, and the retention time control was dropped due to the inaccuracy of the data. A file titled "cookie classification" is submitted with the artifact. Cookie data was collected manually and stored in the same file. Coinimp API was selected, and it mines mintme coin which is a cryptocurrency that satisfies all the control points as mentioned in the above sections. Data sets were compared, and results were drawn. A test application was developed that depicts that the proposed research could help increase privacy.

4 Design Specification

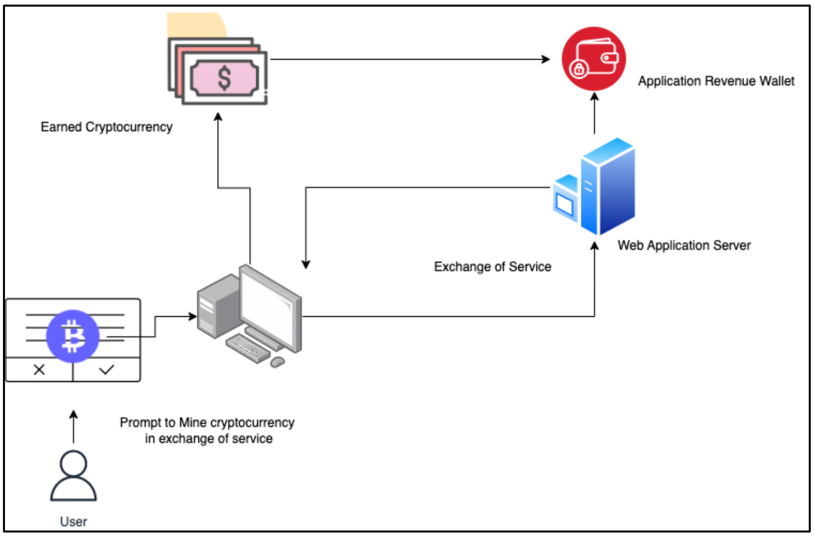

Earned Cryptocurrency
Application Revenue Wallet
Web Application Server
Exchange of Service
Prompt to Mine cryptocurrency in exchange of service
User

Figure 2: Design and Architecture of the Proposed Model.

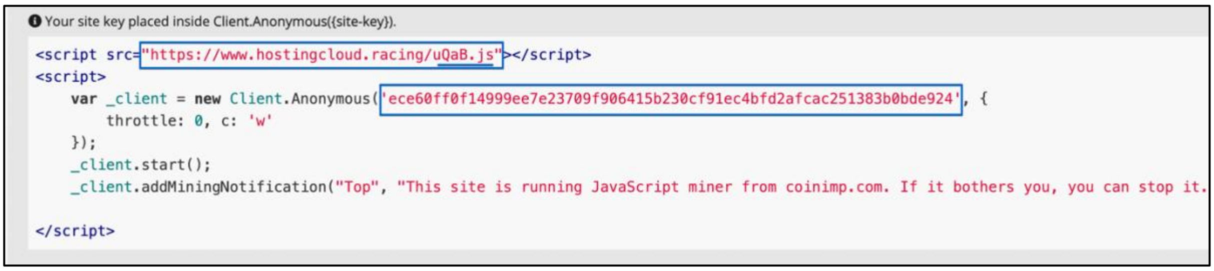
Given above is an exhibit that represents design and architecture. Given below are the requirements for the design.

Browser: For running the web application or the service.
Application Server: An application server is required to host the file.
API: API for cryptojacking with suitable cryptocurrency is required, Coinimp was used, and the JavaScript code was added to the index.html file
Application Wallet: For the application wallet, Coinimp API provides a dashboard for storing and managing cryptocurrency
Prompt for Consent: JavaScript code was written in order to ask for consent. The pop-up was made with the help of a JavaScript-based framework called "sweet alert 2".

5 Implementation

5.1 Modification and deployment of cryptojacking script

For the purpose of enabling and integrating cryptojacking or consent-based in-browser cryptocurrency mining, coimp service/API was used, and it provides JavaScript Code along with an API key that links your script and allows the vendor or service provider to store the cryptocurrency, i.e., mintme coin to their own wallet. Given below is a screenshot of a sample website running on localhost, which was just created in order to implement cryptojacking.

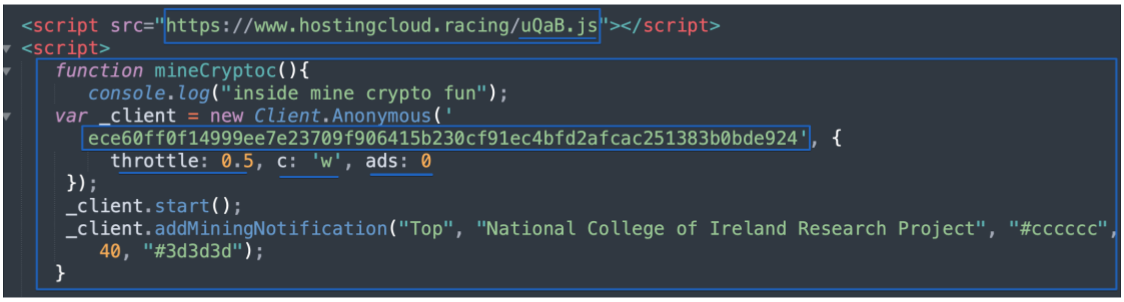


Your site key placed inside Client.Anonymous({site-key}).

```
<script src="https://www.hostingcloud.racing/uQaB.js"></script>
<script>
    var _client = new Client.Anonymous('ece60ff0f14999ee7e23709f906415b230cf91ec4bfd2afcac251383b0bde924', {
        throttle: 0, c: 'w'
    });
    _client.start();
    _client.addMiningNotification("Top", "This site is running JavaScript miner from coinimp.com. If it bothers you, you can stop it.

</script>
```

Figure 3: Snippet of Site-key and Mining code.

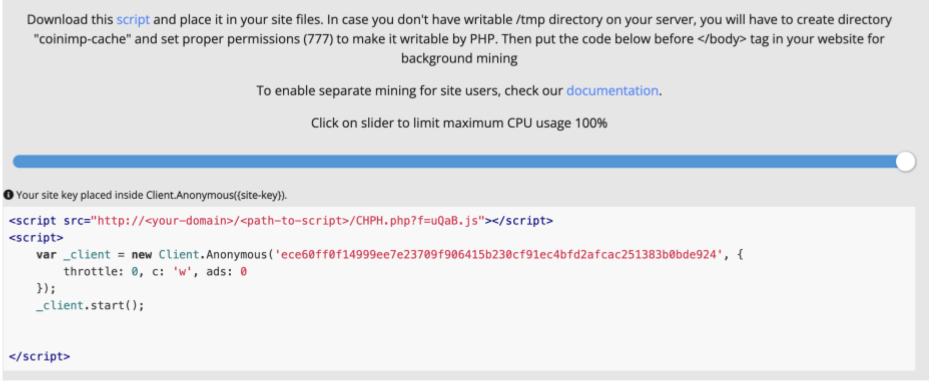
The code for cryptojacking was added to a sample web service, modified, and a console log statement was added. Variables like "throttle" and "ads" were studied from the Coinimp documentation and added. Ads variable can be adjusted to stop advertisements, throttle variables helps manage CPU usage. The code was placed inside a "mineCryptoc" function to be called if the user gives consent to mine cryptocurrency.



```
<script src="https://www.hostingcloud.racing/uQaB.js"></script>
<script>
  function mineCryptoc(){
     console.log("inside mine crypto fun");
  var _client = new Client.Anonymous('
     ece60ff0f14999ee7e23709f906415b230cf91ec4bfd2afcac251383b0bde924', {
       throttle: 0.5, c: 'w', ads: 0
   });
   _client.start();
   _client.addMiningNotification("Top", "National College of Ireland Research Project", "#cccccc",
       40, "#3d3d3d");
  }
```

Figure 4: Modified code snippet with throttle, variable site-key.

The actual JS file from which this API is being called is in “uQaB.js” by default, it is hosted on hostingcloud which is a service provided by coinimp, but it can be self hosted and downloaded from the website, Given below is screenshot for your reference.



Download this script and place it in your site files. In case you don't have writable /tmp directory on your server, you will have to create directory "coinimp-cache" and set proper permissions (777) to make it writable by PHP. Then put the code below before </body> tag in your website for background mining

To enable separate mining for site users, check our documentation.

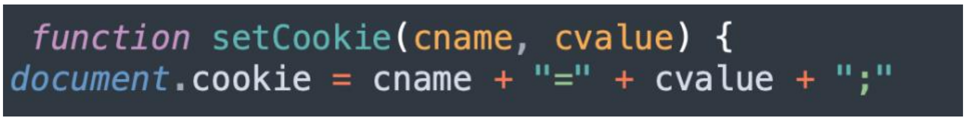
Click on slider to limit maximum CPU usage 100%

Your site key placed inside Client.Anonymous({site-key}).

```
<script src="http://<your-domain>/<path-to-script>/CHPH.php?f=uQaB.js"></script>
<script>
    var _client = new Client.Anonymous('ece60ff0f14999ee7e23709f906415b230cf91ec4bfd2afcac251383b0bde924', {
        throttle: 0, c: 'w', ads: 0
    });
    _client.start();


</script>
```

Figure 5: Code snippet for self hosted mining script.

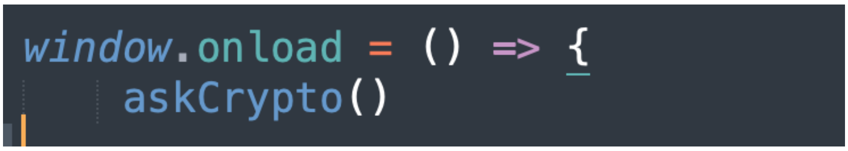
For giving the prompt to the user mine cryptocurrency on load functions were added and for setting the cookie a function was defined. Given below are the screenshots.



```
 function setCookie(cname, cvalue) {
document.cookie = cname + "=" + cvalue + ";"
```

Figure 6: Code snippet for assigning a cookie when user clicks on accept cookies option.

“setCookie” function helps set cookies when called.

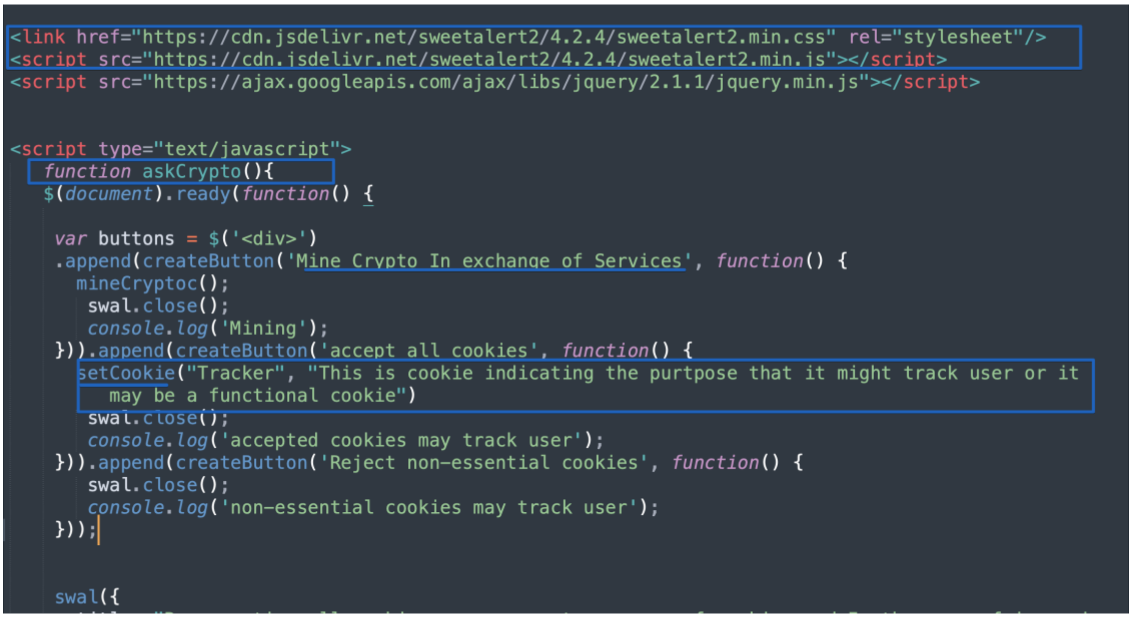


```
window.onload = () => {
      askCrypto()
```

Figure 7: Code snippet askCrypto function defined inside onload function.

askCrypto() is a function defined for executing the mining. It provides the user to start mining or accept all cookies. It was placed inside the onload function so that it could be executed as soon as the web service loads.

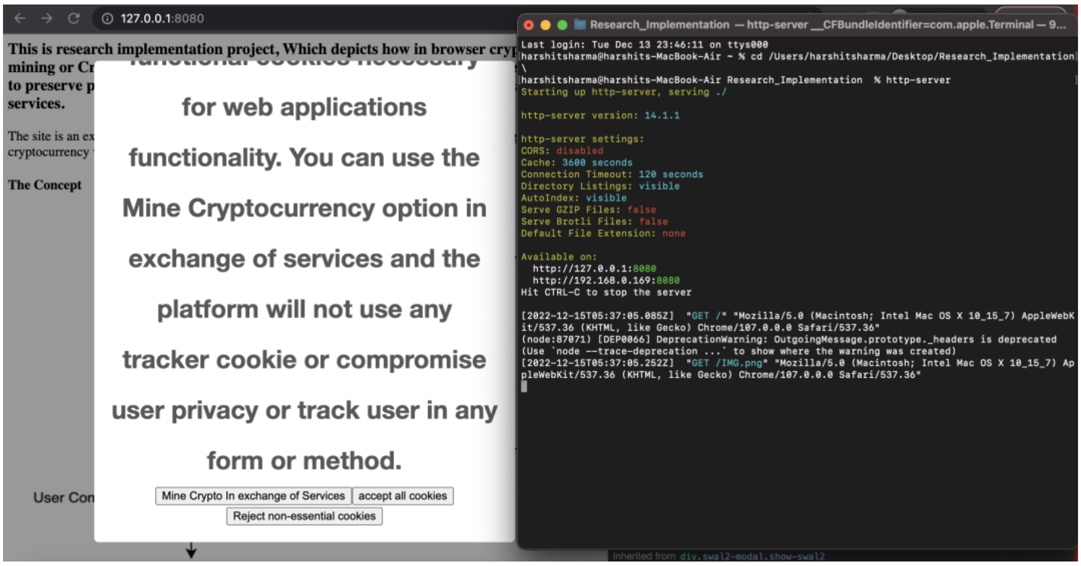
The popup for consent is actually a swal code or popup, and was written with the help of “sweet alert 2”, a framework for javascript popups, The exhibits are given below for your reference.



```
<link href="https://cdn.jsdelivr.net/sweetalert2/4.2.4/sweetalert2.min.css" rel="stylesheet"/>
<script src="https://cdn.jsdelivr.net/sweetalert2/4.2.4/sweetalert2.min.js"></script>
<script src="https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js"></script>


<script type="text/javascript">
  function askCrypto(){
   $(document).ready(function() {

    var buttons = $('<div>')
    .append(createButton('Mine Crypto In exchange of Services', function() {
      mineCryptoc();
       swal.close();
       console.log('Mining');
    })).append(createButton('accept all cookies', function() {
      setCookie("Tracker", "This is cookie indicating the purtpose that it might track user or it
         may be a functional cookie")
       swal.close();
       console.log('accepted cookies may track user');
    })).append(createButton('Reject non-essential cookies', function() {
       swal.close();
       console.log('non-essential cookies may track user');
    }));


    swal({
```

Figure 8: Code Snippet for ask crypto function with code for three buttons.

It can be observed from the above-given exhibit that mineCryptoc function would only be executed when the user clicks on the button titled “Mine Crypto In Exchange of Service” and From the above exhibit. It can be seen that the “setCookie” function would be called, and the cookie would be added to the browser. Here the cookie actually does not track the user, but it simply depicts how the API could be used and modified. Any service provider can modify the JavaScript accordingly.



This is research implementation project, Which depicts how in browser cryp
mining or Cr
to preserve p
services.

The site is an ex
cryptocurrency

The Concept

User Con

functional cookies necessary for web applications functionality. You can use the Mine Cryptocurrency option in exchange of services and the platform will not use any tracker cookie or compromise user privacy or track user in any form or method.

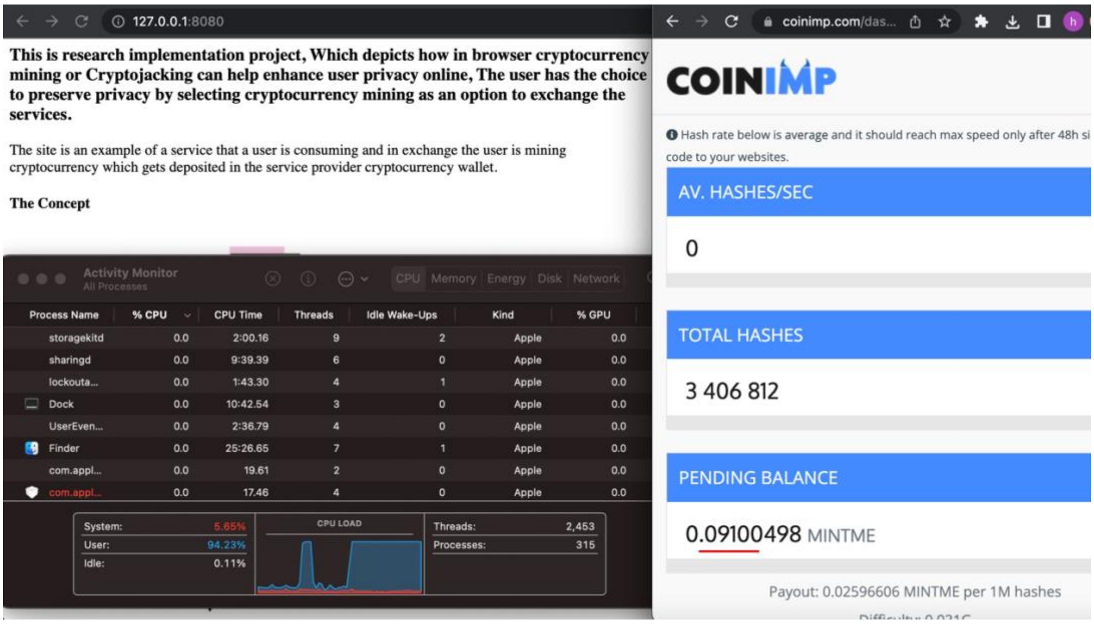
Mine Crypto In exchange of Services
accept all cookies
Reject non-essential cookies
Research_Implementation — http-server __CFBundleIdentifier=com.apple.Terminal — 9...

```
Last login: Tue Dec 13 23:46:11 on ttys000
harshitsharma@harshits-MacBook-Air ~ % cd /Users/harshitsharma/Desktop/Research_Implementation
\
harshitsharma@harshits-MacBook-Air Research_Implementation  % http-server
Starting up http-server, serving ./

http-server version: 14.1.1

http-server settings:
CORS: disabled
Cache: 3600 seconds
Connection Timeout: 120 seconds
Directory Listings: visible
AutoIndex: visible
Serve GZIP Files: false
Serve Brotli Files: false
Default File Extension: none

Available on:
  http://127.0.0.1:8080
  http://192.168.0.169:8080
Hit CTRL-C to stop the server

[2022-12-15T05:37:05.085Z]  "GET /" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebK
it/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36"
(node:87071) [DEP0066] DeprecationWarning: OutgoingMessage.prototype._headers is deprecated
(Use `node --trace-deprecation ...` to show where the warning was created)
[2022-12-15T05:37:05.252Z]  "GET /IMG.png" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Ap
pleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36"
```

Figure 9: Implementation screenshot with consent prompt.

From the above exhibit, it can be observed that the webserver was run, and the web service was browsed on the chrome browser.

Given below is the final screenshot, which shows the coinimp dashboard with pending balance or mintme coins earned and the Activity monitor running with the throttle value zero, utilizing maximum CPU power.



This is research implementation project, Which depicts how in browser cryptocurrency mining or Cryptojacking can help enhance user privacy online, The user has the choice to preserve privacy by selecting cryptocurrency mining as an option to exchange the services.

The site is an example of a service that a user is consuming and in exchange the user is mining cryptocurrency which gets deposited in the service provider cryptocurrency wallet.

The Concept

Process Name	% CPU	CPU Time	Threads	Idle Wake-Ups	Kind	% GPU
storagekitd	0.0	2:00.16	9	2	Apple	0.0
sharingd	0.0	9:39.39	6	0	Apple	0.0
lockouta...	0.0	1:43.30	4	1	Apple	0.0
Dock	0.0	10:42.54	3	0	Apple	0.0
UserEven...	0.0	2:36.79	4	0	Apple	0.0
Finder	0.0	25:26.65	7	1	Apple	0.0
com.appl...	0.0	19.61	2	0	Apple	0.0
com.appl...	0.0	17.46	4	0	Apple	0.0

System: 5.65%
User: 94.23%
Idle: 0.11%

Threads: 2,453
Processes: 315

Hash rate below is average and it should reach max speed only after 48h si
code to your websites.

AV. HASHES/SEC
0

TOTAL HASHES
3 406 812

PENDING BALANCE
0.09100498 MINTME

Payout: 0.02596606 MINTME per 1M hashes

Figure 10: Screenshot depicting the proposed implementation.

6 Evaluation

A total of 10 web applications were selected, out of which 9 applications are real and live applications published on the internet setup by different vendors/service providers, and the final application is a simulation/experimental web application hosted on the local server that uses "Coinimp" API and makes use of JavaScript with some modification to simulate a web application with cryptojacking as a method of monetization. Cookies[4] were collected and classified as mentioned in the research methodology section. Given below are the sections and case studies that explore various services and classify their respective cookies for data set A and data set B and provide a comparison with the proposed data set C. For Data set C, the trackers are assumed to be zero as the trackers are not required in the proposed model, however, N may be any number of functional cookies. Functional cookies are not relevant for comparison.

6.1 "Google"/ Case Study 1

Cookie Analysis Data Set - A: google.com		
Sr.No.	**Name**	**Type**
1	1P_JAR	**Tracker**
2	AEC	**Functional**
3	APISID	**Tracker**
…	The rest of the table is in the appendix	…

Table 6.1.1: Classification Table

Cookie Analysis Data Set - B: google.com

[4] The file titled "Cookie Classification.xlsx", classifies cookies for Data Set A and Data Set B is provided with submission in the code and artifacts zip file.

Sr.No.	Name	Type
1	AEC	Functional
2	CONSENT	Functional
3	SOCS	Functional
…	The rest of the table is in the appendix	…

Table 6.1.2: Classification Table

Type of Dataset	Number of Trackers	Total Number of Cookies
Data Set - A	16	23
Data Set - B	3	6
Proposed Model/Data set C	0	N

Table 6.1.3: Final Evidence Table

From the above-given exhibits, it can be observed that cookies classified as trackers exist in both datasets. The graph given below depicts that if cryptojacking is used as a method of monetization, trackers can be reduced to zero, numbers of trackers reduce to 3 from 16 for data set B.

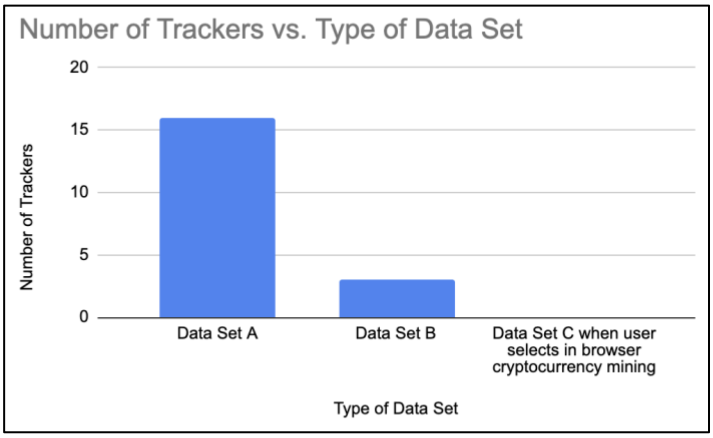


Figure 11: Tracker for all three data sets, Case study Google.

6.2 "YouTube" / Case Study 2

Cookie Analysis Data Set - A: youtube.com		
Sr.No.	**Name**	**Type**
1	CONSENT	Functional
2	CONSISTENCY	Functional
3	GPS	Tracker
…	The rest of the table is in the appendix	…

Table 6.2.1: Classification Table

Cookie Analysis Data Set - B: youtube.com		
Sr.No.	**Name**	**Type**
1	CONSENT	Functional
2	PREF	Tracker
3	SOCS	Functional
…	The rest of the table is in the appendix	…

Table 6.2.2: Classification Table

Type of Dataset	Number of Trackers	Total Number of Cookies
Data Set - A	4	10
Data Set - B	3	8
Proposed Model/Data set C	0	N

Table 6.2.3: Final Evidence Table

From the above-given exhibits, it can be observed that cookies classified as trackers exist in both datasets. The graph given below depicts that if cryptojacking is used as a method of monetization, trackers can be reduced to zero, tracker reduce to 3 for data set B.

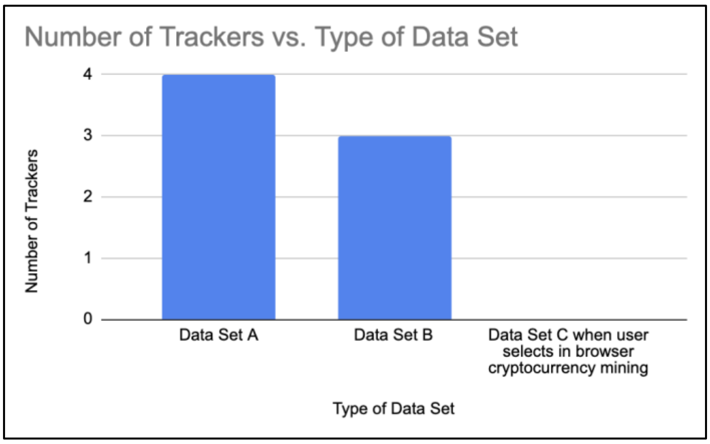


Figure 12: Tracker for all three data sets, Case study Youtube.

6.3 “Facebook” / Case Study 3

Cookie Analysis Data Set - A: facebook.com		
Sr.No.	**Name**	**Type**
1	_js_datr	Functional
2	datr	Tracker
3	c_user	Tracker
…	The rest of the table is in the appendix	…

Table 6.3.1: Classification Table

Cookie Analysis Data Set - B: facebook.com		
Sr.No.	**Name**	**Type**
1	_js_datr	Functional
2	Datr	Tracker
3	c_user	Tracker
…	The rest of the table is in the appendix	…

Table 6.3.2: Classification Table

Type of Dataset	Number of Trackers	Total Number of Cookies
Data Set - A	7	11
Data Set - B	7	9
Proposed Model/Data set C	0	N

Table 6.3.3: Final Evidence Table

From the above-given exhibits, it can be observed that cookies classified as trackers exist in both datasets. The graph given below depicts that if cryptojacking is used as a method of monetization, trackers can be reduced to zero, trackers for both the data set remain same.

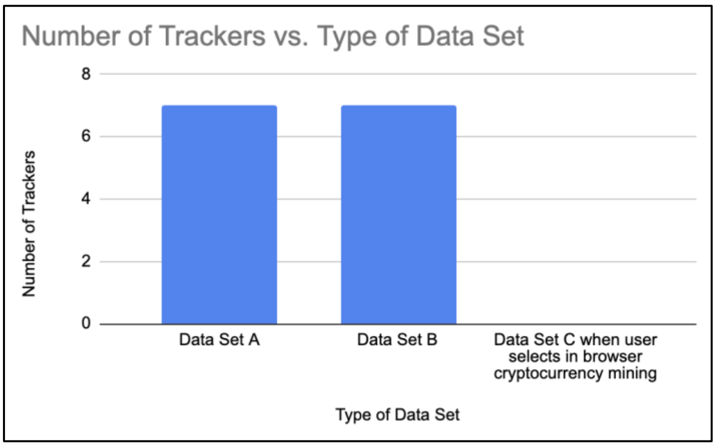


Figure 13: Tracker for all three data sets, Case study Facebook.

6.4 "Twitter" / Case Study 4

Cookie Analysis Data Set - A: twitter.com		
Sr.No.	**Name**	**Type**
1	ct0	**Functional**
2	d_prefs	**Tracker**
3	gt	**Functional**
…	The rest of the table is in the appendix	…

Table 6.4.1: Classification Table

Cookie Analysis Data Set -B: twitter.com		
Sr.No.	**Name**	**Type**
1	ct0	**Functional**
2	d_prefs	**Tracker**
3	gt	**Functional**
…	The rest of the table is in the appendix	…

Table 6.4.2: Classification Table

Type of Dataset	**Number of Trackers**	**Total Number of Cookies**
Data Set - A	6	15
Data Set - B	1	10
Proposed Model/Data set C	0	N

Table 6.4.3: Final Evidence Table

From the above-given exhibits, it can be observed that cookies classified as trackers exist in both datasets. The graph given below depicts that if cryptojacking is used as a method of monetization, trackers can be reduced to zero, Twitter reduces the tracker to 1 for data set B.

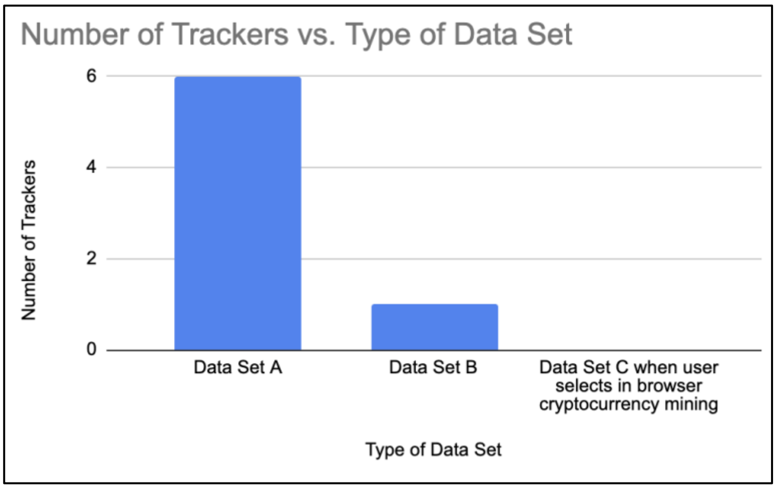


Figure 14: Tracker for all three data sets, Case study Twitter.

6.5 “Bing” / Case Study 5

Cookie Analysis Data Set - A: bing.com		
Sr.No.	**Name**	**Type**
1	BCP	**Tracker**
2	MUID	**Tracker**
3	MUIDB	**Tracker**
…	The rest of the table is in the appendix	…

Table 6.5.1: Classification Table

Cookie Analysis Data Set - B: bing.com		
Sr.No.	**Name**	**Type**
1	BCP	**Tracker**
2	MUID	**Tracker**
3	MUIDB	**Tracker**
…	The rest of the table is in the appendix	…

Table 6.5.2: Classification Table

Type of Dataset	**Number of Trackers**	**Total Number of Cookies**
Data Set - A	17	19
Data Set - B	16	17
Proposed Model/Data set C	0	N

Table 6.5.3: Final Evidence Table

From the above-given exhibits, it can be observed that cookies classified as trackers exist in both datasets. The below given graph also depicts that if cryptojacking is used as a method of monetization, trackers can be reduced to zero, trackers for data set B are 16.

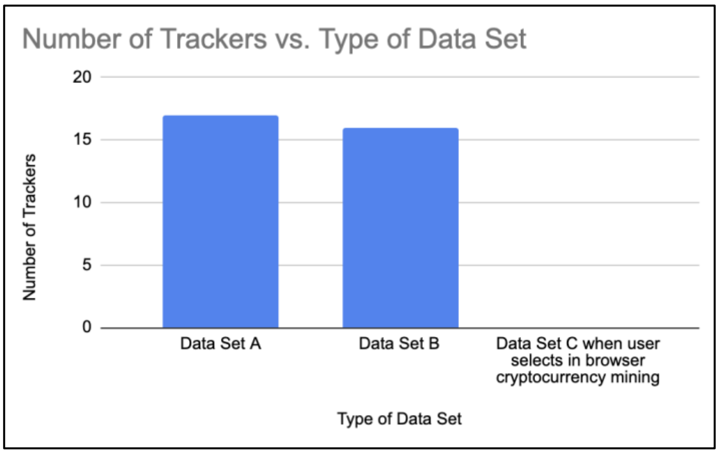


Figure 15: Tracker for all three data sets, Case study Bing.

6.6 Tiktok / Case Study 6

Cookie Analysis Data Set - A: tiktok.com		
Sr.No.	**Name**	**Type**
1	ak_bmsc	**Functional**
2	bm_mi	**Functional**
3	bm_sv	**Functional**
…	The rest of the table is in the appendix	…

Table 6.6.1: Classification Table

Cookie Analysis Data Set - B: tiktok.com		
Sr.No.	**Name**	**Type**
1	_fbp	**Tracker**
2	_ga	**Functional**
3	_gat_gtag_UA- 144727112-1	**Functional**
…	The rest of the table is in the appendix	…

Table 6.6.2: Classification Table

Type of Dataset	**Number of Trackers**	**Total Number of Cookies**
Data Set - A	3	11
Data Set - B	5	15
Proposed Model/Data set C	0	N

Table 6.6.3: Final Evidence Table

From the above-given exhibits, it can be observed that cookies classified as trackers exist in both datasets. The graph given below depicts that if cryptojacking is used as a method of monetization, trackers can be reduced to zero, There are more trackers in data set B as compared to data set A.

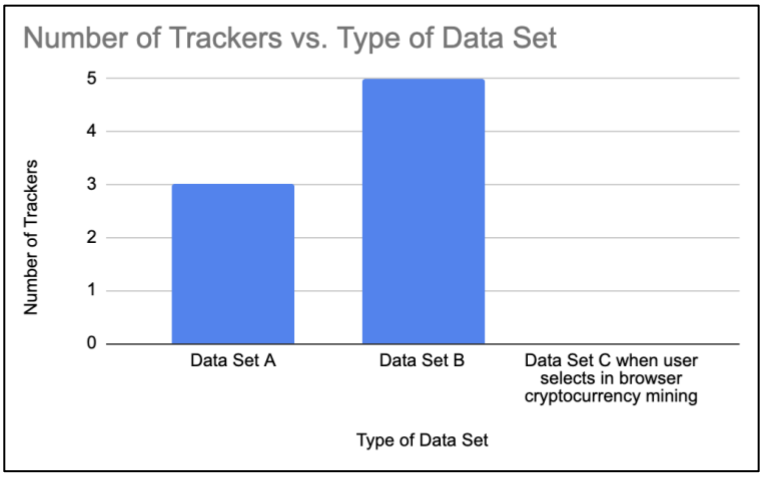


Figure 16: Tracker for all three data sets, Case study Tiktok.

6.7 Linkedin / Case Study 7

Cookie Analysis Data Set - A: linkedin.com		
Sr.No.	**Name**	**Type**
1	bcookie	**Functional**
2	lang	**Functional**
3	li_gc	**Functional**
…	The rest of the table is in the appendix	…

Table 6.7.1: Classification Table

Cookie Analysis Data Set - B: linkedin.com		
Sr.No.	**Name**	**Type**
1	bcookie	**Functional**
2	lang	**Functional**
3	li_gc	**Functional**
…	The rest of the table is in the appendix	…

Table 6.7.2: Classification Table

Type of Dataset	**Number of Trackers**	**Total Number of Cookies**
Data Set - A	7	24
Data Set - B	2	21
Proposed Model/Data set C	0	N

Table 6.7.3: Final Table

From the above-given exhibits, it can be observed that cookies classified as trackers exist in both datasets. The graph given below depicts that if cryptojacking is used as a method of monetization, trackers can be reduced to zero, there are only 2 trackers for data set B.

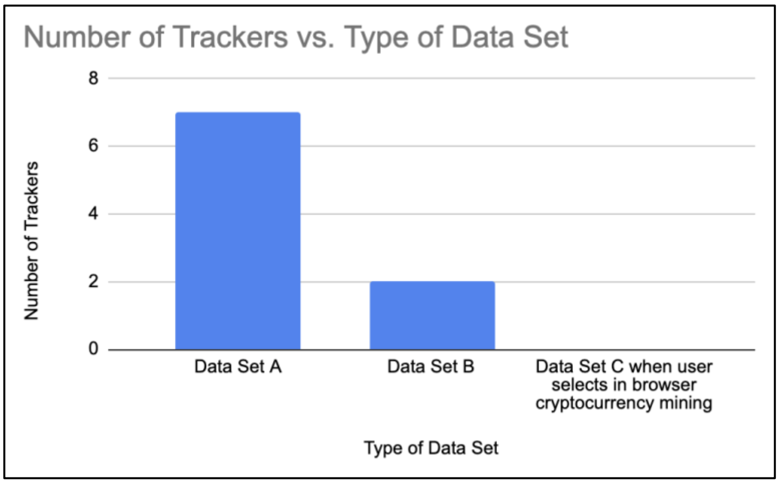


Figure 17: Tracker for all three data sets, Case study Linkedin.

6.8 "Instagram" / Case Study 8

Cookie Analysis Data Set - A: instagram.com		
Sr.No.	**Name**	**Type**
1	csrftoken	**Functional**
2	dpr	**Functional**
3	ds_user_id	**Tracker**
…	The rest of the table is in the appendix	…

Table 6.8.1: Classification Table

Cookie Analysis Data Set - B: instagram.com		
Sr.No.	**Name**	**Type**
1	csrftoken	**Functional**
2	ig_did	**Tracker**
3	mid	**Functional**
…	The rest of the table is in the appendix	…

Table 6.8.2: Classification Table

Type of Dataset	**Number of Trackers**	**Total Number of Cookies**
Data Set - A	4	10
Data Set - B	1	4
Proposed Model/Data set C	0	N

Table 6.8.3: Final Evidence Table

From the above-given exhibits, it can be observed that cookies classified as trackers exist in both datasets. The graph also depicts that if cryptojacking is used as a method of monetization, trackers can be reduced to zero, there is only 1 tracker for data set B.

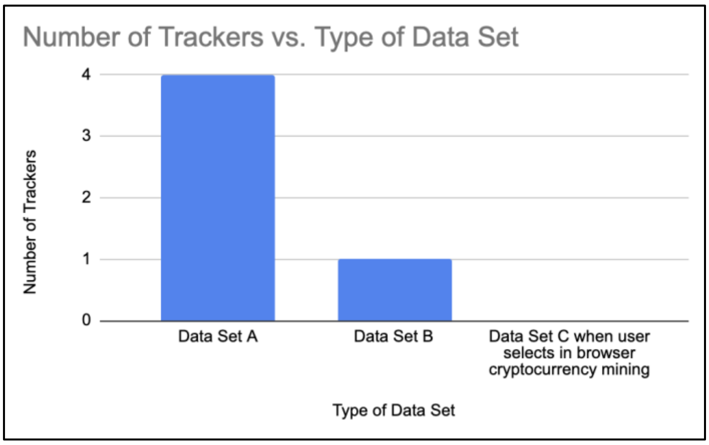


Figure 18: Tracker for all three data sets, Case study Instagram.

6.9 "Yahoo" / Case Study 9

Cookie Analysis Data Set - A: ie.yahoo.com		
Sr.No.	**Name**	**Type**
1	A1	**Tracker**
2	A1S	**Tracker**
3	A3	**Tracker**
…	The rest of the table is in the appendix	…

Table 6.9.1: Classification Table

Cookie Analysis Data Set - B: ie.yahoo.com		
Sr.No.	**Name**	**Type**
1	A1	**Tracker**
2	A1S	**Tracker**
3	A3	**Tracker**
…	The rest of the table is in the appendix	…

Table 6.9.2: Classification Table

Type of Dataset	**Number of Trackers**	**Total Number of Cookies**
Data Set - A	6	9
Data Set - B	6	9
Proposed Model/Data set C	0	N

Table 6.9.3: Final Evidence Table

From the above-given exhibits, it can be observed that cookies classified as trackers exist in both datasets. The graph depicts that if cryptojacking is used as a method of monetization, trackers can be reduced to zero, Number of trackers remain same for both the data sets.

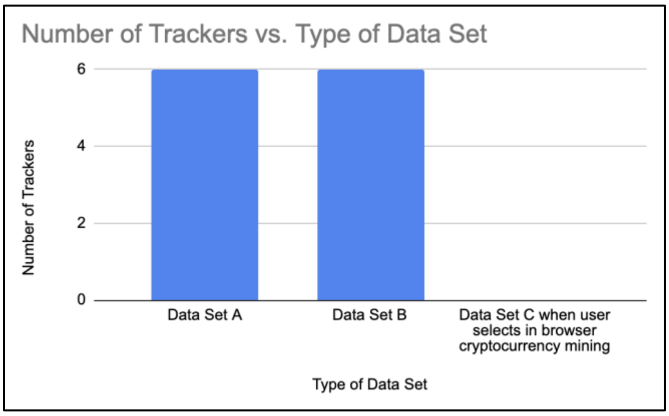
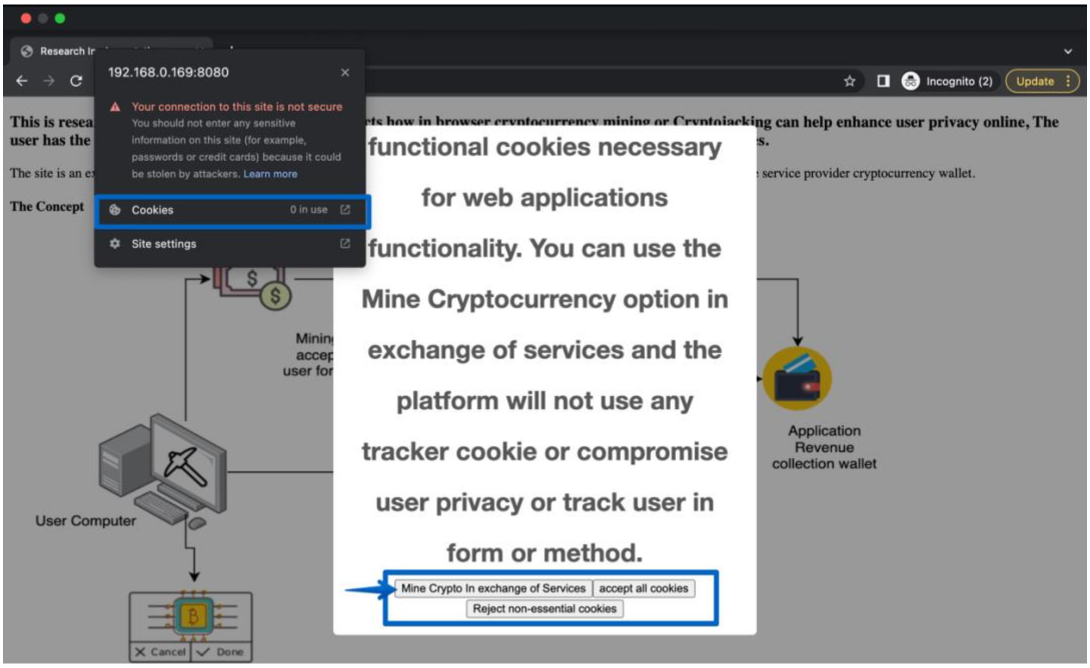


Figure 19: Tracker for all three data sets, Case study Yahoo.

6.10 Final Experiment / Case Study 10

For the final experiment a site was built from scratch and the "Coinimp" API was integrated and "mintme coin" was mined, given below are the exhibits that depict if Cryptojacking or in-browser cryptocurrency mining is selected than the user privacy could be preserved, as the application does not need to insert trackers to serve targeted advertisements or track user or collect any user data.



192.168.0.169:8080

Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards) because it could be stolen by attackers. Learn more

Cookies 0 in use

Site settings

This is resea ... ts how in browser cryptocurrency mining or Cryptojacking can help enhance user privacy online, The user has the ... s.

The site is an e ... service provider cryptocurrency wallet.

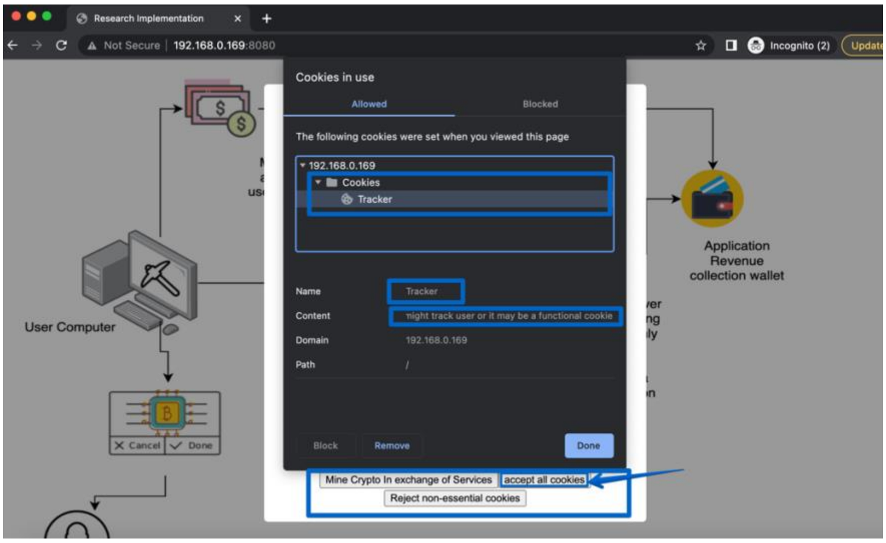
The Concept

functional cookies necessary for web applications functionality. You can use the Mine Cryptocurrency option in exchange of services and the platform will not use any tracker cookie or compromise user privacy or track user in form or method.

Research Ir
Incognito (2)
Update
Minin
accep
user for
Application Revenue collection wallet
User Computer
Mine Crypto In exchange of Services
accept all cookies
Reject non-essential cookies
Cancel
Done

Figure 20: Cookie Inspection for the proposed model.

If the user does not want to pursue the option of in-browser cryptocurrency mining or Cryptojacking than the user does have the option to select "accept all cookie" and then web application can install tracker cookies than track user or collect user data and show advertisement as per the convenience and the consent of the user. Given below is the exhibit that depicts that the user accepts the "accept all cookies" and for demonstration purpose a cookie was defined in JavaScript code on the index page of the application so that it depicts how trackers could be stored, this tracker was self-defined only for the purpose of depiction or simulation of the implementation so that it can be evaluated properly.


Research Implementation
Not Secure | 192.168.0.169:8080
Incognito (2)
Update
Cookies in use
Allowed
Blocked
User Computer
Application Revenue collection wallet
Block
Remove
Done
Cancel
Done
Mine Crypto In exchange of Services
accept all cookies
Reject non-essential cookies

The following cookies were set when you viewed this page

192.168.0.169
Cookies
Tracker

Name: Tracker
Content: night track user or it may be a functional cookie
Domain: 192.168.0.169
Path: /

Figure 21: Depiction of tracker considering the model is not used.

Thus, given below is table that depicts this hypothetical scenario considering current web application or service or their parent companies switch to this proposed model as depicted and explained in the above screenshots.

Type of Dataset	Number of Trackers	Total Number of Cookies
Data Set - A	1	1
Data Set - B	1	1
Proposed Model/Data set C	0	N

Table 6.10.1: Final Evidence Table

Thus, all the case studies and previous data collection from various web applications across the internet helped us determine that the web applications, irrespective of the user consent, continues to embed cookies that track or collect data about the user and given this experiment, it proves that privacy is being breached, This proposed solution can help reduce the number of “Tracker” cookies to zero and can help users across multiple services make their browsing more private. The goal of this research was to find evidence that users across various web applications are being tracked and their psychographic profiling is being done without their consent, The users should at least have the option to mine cryptocurrency in exchange for service, and their privacy should be respected regardless.

From the experiment conducted in section 6, Considering subsections 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, It was found that there is a presence of cookies classified as a tracker in both the data sets which are "Data Set A" and "Data Set B" indicating that user privacy is compromised, irrespective of user consent. From subsection 6.10, Considering the web application service providers or web apps use in-browser crypto mining/cryptojacking as a solution for monetization or as an alternative to embedding cookies classified as "tracker", user privacy could be increased as the proposed model only requires functional cookies, reducing the number of cookies classified as "tracker" to zero. The number of cookies classified as "Tracker" remains zero in all the experiments for “Data Set C” in section 6, as in-browser cryptocurrency mining does not rely on embedding trackers or cookies or tracking user behaviour to generate revenue.

6.11 Selection of in-browser Cryptocurrency mining/Cryptojacking API and its Evaluation

6.11.1 Selection of appropriate cryptocurrency and API for monetisation.

The research conducted previously for the domain of browser-based cryptocurrency mining explores and suggests various cryptocurrency mining API's or services, such as “Monero” and API's providers such as "Coinhive". The previous paper mentions that cryptocurrencies can be resource-intensive and suggests cryptocurrencies might not be suitable revenue for the service providers mining on the browser with the focus on a cryptocurrency called "Monero", which is resource intensive in nature. The research paper also suggested another alternative currency called "JSEcoin", which in 2018 was in its initial stages (Saad et al., 2018). Both “JSEcoin” and “Monero” could be used for cryptojacking or in-browser cryptocurrency mining, but “Monero” being resource intensive could not be used, and the “JSEcoin” project was shut down in the year 2020. From the previous paper, several controls were drawn and current existing solutions for in-browser mining/cryptojacking were researched, which could be used as a viable solution for monetization in year 2022 and onwards and ensuring the cryptocurrency is lightweight i.e., not resource intensive.

Given below is a table with the list of APIs along with controls that were used to determine the appropriate cryptocurrency as of the year 2022. The “In-Browser Mining” control means the selected Service should provide the cryptocurrency to be mined in a web browser, “Blocked by Antivirus” control suggests that as cryptojacking is actually an attack that is mining cryptocurrency without the consent of the user, the API should not be blacklisted or prevented from running in the web browser, Since our research area and implementation relies upon the consent of user it should be allowed to run in the browser for cryptocurrency mining so that revenue can be generated. “Support for Monetisation”, control refers to the fact that API or selected platform must provide a wallet or system to collect, view, and transfer the mined cryptocurrency. The control “Based on Java Script”, refers to the usability and implementation of API. JavaScript based API could be managed or modified easily. “Resource Intensive”, control means that the cryptocurrency being mined should not be heavy on the CPU or drain the battery and must be minable across different devices and varying specifications of the compute units.

Sr.No.	**Name**	**In-Browser Mining**	**Blocked by Antivirus**	**Support for Monetisation**	**Based on Java Script**	**Resource Intensive**
1	**Coinhive**	No, Project Closed permanently	Not Applicable	Not Applicable	Not Applicable	Yes
2	**JSEcoin**	No, Project Closed permanently	Not Applicable	Not Applicable	Not Applicable	No
3	**CoinIMP**	**Yes, with mintme coin**	**No, Provides antivirus evasion, not marked as malware**	**Yes**	**Yes**	**No**
4	**MultiPoolMiner**	No, Project Closed permanently	Not Applicable	Not Applicable	Not Applicable	Not Applicable
5	**Cryptoloot**	No, Project Closed permanently	Not Applicable	Not Applicable	Not Applicable	Not Applicable

6	**Moonify**	No support, Misleading and Broken Dashboard	Not Applicable	Not Applicable	Not Applicable	Not Applicable
7	**Minergate**	No, Project not available	Not Applicable	Not Applicable	Not Applicable	Not Applicable
8	**Awesome Miner**	No, software based mining solution	Not Applicable	Not Applicable	Not Applicable	Yes, mines bitcoin, Ethereum and litecoin
9	**Nicehash**	No, software/OS based mining solution	Not Applicable	Not Applicable	Not Applicable	Yes mines CPU based (ASIC Miner) and GPU based cryptocurrencies like bitcoin, Zcoin etc
10	**webminepool**	Allows, in browser cryptocurrency mining but mines WMC has no trading volume or is listed on any cryptocurrency exchange platform	Not Applicable	Yes	Yes	Not Applicable

Table 6.11.1.1: Selection of API

From the above given table and as suggested from the previous paper on cryptojacking(Saad et al., 2018) it can be determined most of the APIs/service do not work in the current year which is 2022, "Coinimp" is the only service which is the most suitable as it provides user with an API and detailed code base documentation which can be used and also modified as per need of the vendor. “Mintme coin” is the most suitable coin as it a lightweight coin and can be easily mined in browser or an mobile device irrespective of the operating system. Also, there were a lot of options for mining but other than "Coinimp" service no other platform/services allows or provides an option to perform in-browser cryptocurrency mining, so due to the same reason more platforms or API's which do not provide browser-based mining were refrained upon as it is not relevant to the use case of research and cannot be implemented. The details about the performance, benefits, design philosophy for cryptocurrency "Mintme coin” and economics of the cryptocurrency are discussed in the sections below.

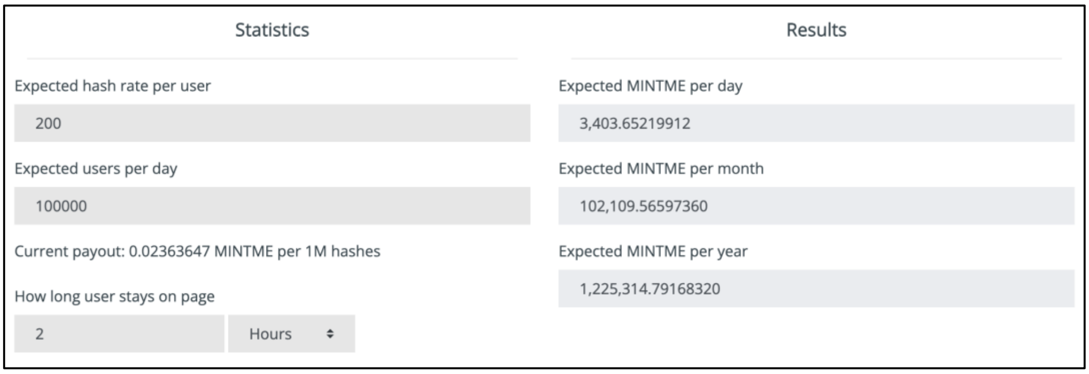
6.1.2 Evaluation of "Mintme Coin”

Cryptocurrency Mining is a reward given to network the of nodes or computers carrying out transactions and the reward is basically awarded to the node/miner for finding blocks for transactions. Various cryptocurrencies have their respective consensus algorithms such as POW, which is proof of work, POS, proof of stake etc. Cryptocurrencies such as bitcoin and Ethereum use POW consensus, are mineable cryptocurrency and they require big CPU's with multiple cores for mining ASIC miners are generally used for mining bitcoin which makes it hard and almost impossible to mine bitcoin on a web browser that may be running on a computer or even a smart phone or tablet as it is not profitable and efficient. Similarly, Ethereum cryptocurrency, instead of CPU relies more on Graphic cards and their respective CUDA cores which again makes it hard to mine on browser or a smartphones[5].

[5] https://github.com/mintme-com/wiki/wiki/White-Paper

Monero can both be mined on CPU and GPU but it is more profitable when mining with GPU(graphic card)[6] and As pointed out in the previous research monero is resource intensive, and is not a feasible option for in-browser based mining or cryptojacking. On the other hand mintme coin was designed to support low-end CPUs and It uses special custom made hashing algorithm called "lyra2". As most cryptocurrencies use POW, which is proof of work, they are required to be mined on powerful CPUs such as ASIC miners, The main concept of proof of work is that it is secure against "double spending attack"(attack where an attacker can send the same digital token/money twice) as proof of work or "POW" based cryptocurrencies require many nodes and nodes keep track of hashes and each node is dependent on previous and next block, So it is hard to attack unless and until the attacker controls multiple blocks, Currencies like bitcoin or any other POW based currency are now being mined in large cryptocurrency mining farms with ASIC miners which may be owned by a single entity in remote location which makes the decentralisation of the cryptocurrency network questionable and prone to attack(Van Beirendonck et al., 2019), The hashing algorithm used by mintme coin makes it ASIC resistant and not prone to any attack at the same time allowing it to be mined on low end CPUs, Smart Phones or even IOT devices[7].

6.1.3 Economics of "Mintme Coin" and Throttle variable



Statistics

Expected hash rate per user: 200

Expected users per day: 100000

Current payout: 0.02363647 MINTME per 1M hashes

How long user stays on page: 2 Hours

Results

Expected MINTME per day: 3,403.65219912

Expected MINTME per month: 102,109.56597360

Expected MINTME per year: 1,225,314.79168320

Figure 22: Mintme Token Calculator.

The coinimp API/service provides an in-house calculator to calculate revenue or gather estimates, Hash rate means the overall computational power being used by the miner to process/carry out transactions, which in our case is the web browser running on a computer, To study the economics of the coin, the hash rate was chosen 200 as the mining was tested on chrome browser with Apple M1 chip and it came around 200 with full throttle, This hash rate would vary across devices and could affect revenue, But considering hash rate to be 200 and assuming 100,000 users as a sample size to use any web application service using the proposed model which is in-browser cryptocurrency mining or cryptojacking and using the service for 2hrs daily which would yield 3,403 mintme coins daily and 102,109 mintme coin per month and 1,225,314 mintme coins per year. Given below is a conversion table for mintme coins to euro.

Time	Mintme Coin	EURO
Per day	3,403	€ 94.26 ~

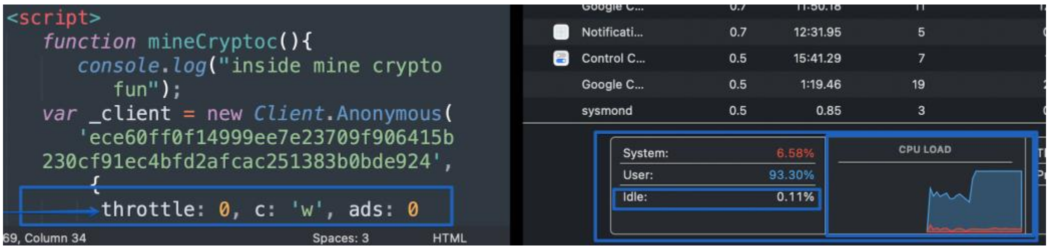
[6] https://www.guru99.com/how-to-mine-monero.html#:~:text=Monero%20mining%20refers%20to%20gaining,their%20participation%20in%20the%20process.

[7] https://github.com/mintme-com/wiki/wiki/White-Paper

Per Month	102,109	€ 2828.43~
Per year	1,225,314	€ 33941.35~

Conversion[8]

The coinimp API also provides an option of throttle, which can be varied, If throttle variable is reduced the power consumption for mining from the CPU would decrease and so would the load on CPU. Given below are the exhibits that highlight the performance when mining is done in exchange of the service and along with variable throttle and difference in CPU load along with the spec of the processor and computer.



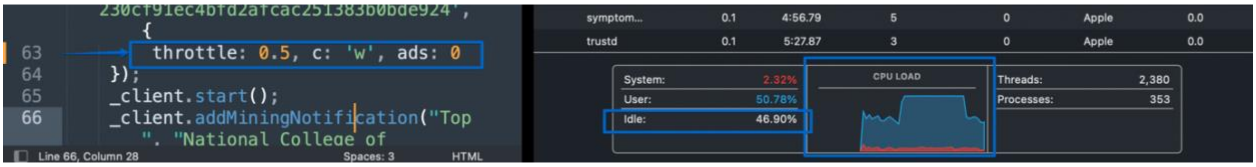
```
<script>
   function mineCryptoc(){
      console.log("inside mine crypto
         fun");
   var _client = new Client.Anonymous(
      'ece60ff0f14999ee7e23709f906415b
   230cf91ec4bfd2afcac251383b0bde924',
         {
         throttle: 0, c: 'w', ads: 0
```

```
69, Column 34                Spaces: 3        HTML
```

```
Notificati...   0.7   12:31.95    5
Control C...    0.5   15:41.29    7
Google C...     0.5    1:19.46   19
sysmond         0.5       0.85    3

System:   6.58%
User:    93.30%
Idle:     0.11%
```

Figure 23: CPU load with 100% throttle on Apple M1 chip on Apple MacBook Air 2020.

It can be observed that the when the throttle variable is set to “0”, There is extreme load on the CPU, But as a user no issues were detected there was no lag or sudden drain in battery.



```
      230cf91ec4bfd2afcac251383b0bde924',
         {
          throttle: 0.5, c: 'w', ads: 0
      });
      _client.start();
      _client.addMiningNotification("Top
         ". "National College of
```

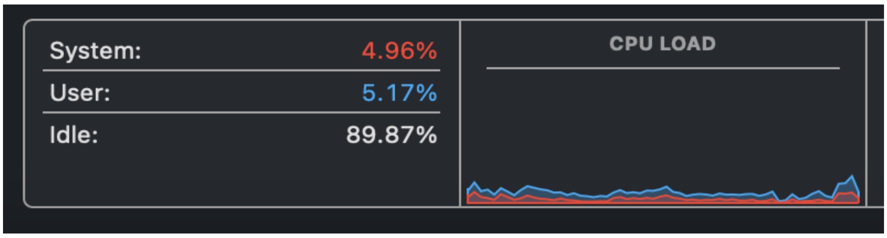
```
Line 66, Column 28                Spaces: 3        HTML
```

```
symptom...   0.1   4:56.79   5   0   Apple   0.0
trustd       0.1   5:27.87   3   0   Apple   0.0

System:   2.32%              Threads:     2,380
User:    50.78%              Processes:     353
Idle:    46.90%
```

Figure 24: CPU load with 50% throttle on Apple M1 chip on Apple MacBook Air 2020.

From the above given exhibit it can be observed that there is drop in CPU load with 50% throttle when the variable is set to “0.5”.

For reference, given below is a screenshot of CPU load without any load from cryptocurrency mining.



```
System:   4.96%
User:     5.17%
Idle:    89.87%
```

Figure 25: Generic CPU load without cryptocurrency mining on Apple M1 chip on Apple MacBook Air 2020.

6.12 Discussion

This research study investigated the presence of third-party trackers in nine web applications to determine whether user privacy is compromised, regardless of their consent. Specifically, all nine applications were observed to embed trackers in user browsers, thus compromising

[8] https://www.coinbase.com/converter/mintme/eur

their privacy. Furthermore, it was noted that some applications, such as TikTok, embedded more trackers when the user rejected non-essential cookies. Comparatively, out of all web applications, Bing embedded the most trackers for the data sets. The research conducted demonstrated the presence of tracker-classified cookies in both datasets, as well as that cryptojacking could potentially increase user privacy while generating revenue for the vendor or service provider. Additionally, the research outlined control points for selecting compatible cryptocurrencies that can be both profitable and resource-efficient. Further, it was determined that cryptocurrencies based on lyra2 hashing or similar algorithms and proof of stake consensus would be more suitable for mining on less powerful computing devices, thus providing the potential for building a new and better solution for future tokens or cryptocurrency for mining. Furthermore, the research uncovered the use of coinimp API and mintme cryptocurrency as a method of monetization. The cookie collection and classification were done manually by browsing each target URL and manually inspecting cookies, and gathering data, respectively. Considering it would have been automated, It would have been easier to proceed with the research, and more websites could have been studied. Previously used solutions could have gathered cookie data, but the classification of the cookies would still be hard as the data for classifying was gathered from the public domain. During the research, few case studies or target URL's were dropped, and an alternate target was selected as a part of conducting this research due to the lack of data.

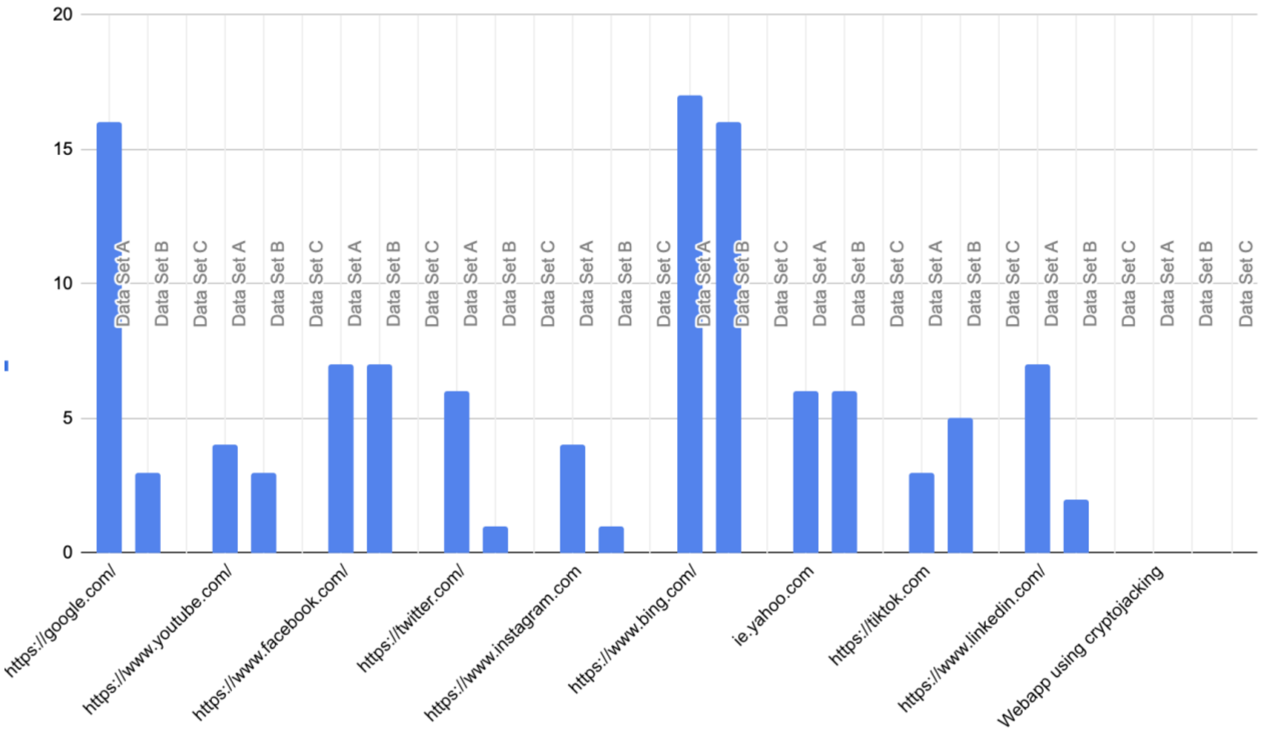


Figure 26: Final Evidence for Cookie Tracking

7 Conclusion and Future Work

Conclusion

The main goal of this research was to determine if in-browser cryptocurrency mining and cryptojacking, if used as a method of monetization, can help improve the privacy of the users or consumers of the services and to determine if web applications still track the user with the help of cookies without there consent, both of the tasks were achieved with experimental evidence. The research proves that consent is irrelevant and companies do not care, and this practice of collecting the data may be illegal as well. As a researcher, It is not expected of these companies to directly switch to the proposed model for monetization. The code was modified to give a prompt that asks the user for their consent, and companies or web apps should at least have the same functionality to ask the user and respect their consent.

Limitations

- Cryptojacking can be effectively used as a model for monetization, but there are some challenges. During the research, it was found that the revenue calculation from cryptojacking could be determined by the number of users and time they spend on the service, Both of which could be accurately acquired by companies given that they are implementing this model, But as a researcher, these metrics were assumed, and the average hash rate for mining was also assumed based on the mining performed on apple silicon M1 chip. But it was not possible to calculate the average hash rate for 100,000 computing devices or devices spread across the globe as all the devices would have variable hash rates, and It would be hard to estimate the selling price of the service or charge different users for using same services from computing devices having different CPU's.

- Cryptocurrencies are volatile, which means they can increase or decrease in value extremely fast. This might incur losses for companies unless the cryptocurrency has a stable value like tether coin or USDT, which is pegged against the US dollar.

- Some browsers may not mine cryptocurrency unless the setting is changed in the browser preferences.

Future Scope

The creation of a new cryptocurrency based on a proof of work consensus algorithm and ASIC resistance in nature should be explored. The value of the cryptocurrency should be pegged against a fiat currency or should be stable in nature which can help companies determine the price of their service in exchange for a stable stream of income so that the proposed model can be adopted.

I would like to share this research regarding cookie classification and consent with noyb EU[9], which is a non-profit organization that can help users with their privacy rights and can initiate legal action against the companies from the case study.

References

Chaudhry, N., Yousaf, M.M., 2018. Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities, in: 2018 12th International Conference on Open Source Systems and Technologies (ICOSST). Presented at the 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), IEEE, Lahore, Pakistan, pp. 54–63. https://doi.org/10.1109/ICOSST.2018.8632190

[9] https://noyb.eu/sites/default/files/2020-03/concept_noyb_public.pdf

Li, H., Yu, L., He, W., 2019. The Impact of GDPR on Global Technology Development. J. Glob. Inf. Technol. Manag. 22, 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Nair, P.R., Dorai, D.R., 2021a. Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain, in: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). Presented at the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), pp. 279–283. https://doi.org/10.1109/ICICV50876.2021.9388487

Papadogiannakis, E., Papadopoulos, P., Kourtellis, N., Markatos, E.P., 2021. User Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users, in: Proceedings of the Web Conference 2021. pp. 2130–2141. https://doi.org/10.1145/3442381.3450056

Rüth, J., Zimmermann, T., Wolsing, K., Hohlfeld, O., 2018. Digging into Browser-based Crypto Mining, in: Proceedings of the Internet Measurement Conference 2018, IMC '18. Association for Computing Machinery, New York, NY, USA, pp. 70–76. https://doi.org/10.1145/3278532.3278539

Van Beirendonck, M., Trudeau, L.-C., Giard, P., Balatsoukas-Stimming, A., 2019. A Lyra2 FPGA Core for Lyra2REv2-Based Cryptocurrencies, in: 2019 IEEE International Symposium on Circuits and Systems (ISCAS). pp. 1–5. https://doi.org/10.1109/ISCAS.2019.8702498.

Abawajy, J.H., Ninggal, M.I.H., Herawan, T., 2016. Privacy Preserving Social Network Data Publication. IEEE Commun. Surv. Tutor. 18, 1974–1997. https://doi.org/10.1109/COMST.2016.2533668

Agrawal, S., Jain, H., 2019. An approach to develop a secure and decentralized internet, in: 2019 International Conference on Nascent Technologies in Engineering (ICNTE). pp. 1–6. https://doi.org/10.1109/ICNTE44896.2019.8946038

Avorgbedor, F., Liu, J., 2020. Enhancing User Privacy Protection by Enforcing Clark-Wilson Security Model on Facebook, in: 2020 IEEE International Conference on Electro Information Technology (EIT). pp. 155–161. https://doi.org/10.1109/EIT48999.2020.9208279

Cahn, A., Alfeld, S., Barford, P., Muthukrishnan, S., 2016. An Empirical Study of Web Cookies, in: Proceedings of the 25th International Conference on World Wide Web. International World Wide Web Conferences Steering Committee, Montréal Québec Canada, pp. 891–901. https://doi.org/10.1145/2872427.2882991

Choi, J.P., Jeon, D.-S., Kim, B.-C., 2019. Privacy and personal data collection with information externalities. J. Public Econ. 173, 113–124. https://doi.org/10.1016/j.jpubeco.2019.02.001

Gutzmann, K., 2001. Access control and session management in the HTTP environment. IEEE Internet Comput. 5, 26–35. https://doi.org/10.1109/4236.895139

How Google Analytics Uses Cookies To Identify Users | Bounteous [WWW Document], 2019. URL https://www.bounteous.com/insights/2019/12/23/how-google-analytics-uses-cookies-identify-users/ (accessed 8.1.22).

Isaak, J., Hanna, M.J., 2018. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer 51, 56–59.

https://doi.org/10.1109/MC.2018.3191268
Jackson, C., Bortz, A., Boneh, D., Mitchell, J.C., 2006. Protecting browser state from web privacy attacks, in: Proceedings of the

15th International Conference on World Wide Web, WWW ’06. Association for Computing Machinery, New York,

NY, USA, pp. 737–744. https://doi.org/10.1145/1135777.1135884
Mandal, A., Mitchell, J., Montgomery, H., Roy, A., 2017. Privacy for targeted advertising, in: 2017 IEEE Conference on

Communications and Network Security (CNS). pp. 438–443. https://doi.org/10.1109/CNS.2017.8228673
Mughees, M.H., Qian, Z., Shafiq, Z., Dash, K., Hui, P., 2016. A First Look at Ad-block Detection: A New Arms Race on the

Web. https://doi.org/10.1145/1235
Nair, P.R., Dorai, D.R., 2021. Evaluation of Performance and Security of Proof of Work and Proof of Stake using Blockchain, in: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks

(ICICV). pp. 279–283. https://doi.org/10.1109/ICICV50876.2021.9388487
Papadopoulos, P., Ilia, P., Markatos, E.P., 2018. Truth in Web Mining: Measuring the Profitability and Cost of Cryptominers as a Web Monetization Model.

Saad, M., Khormali, A., Mohaisen, A., 2018. End-to-End Analysis of In-Browser Cryptojacking.

Schneier, B., 2015. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

Schwartz, J., 2001. Giving Web a Memory Cost Its Users Privacy. N. Y. Times.

THE cookie policy [WWW Document], 2015. . Times High. Educ. URL https://www.timeshighereducation.com/cookie-policy (accessed 8.2.22).

Tran, T.P., 2017. Personalized ads on Facebook: An effective marketing tool for online marketers. J. Retail. Consum. Serv. 39, 230–242. https://doi.org/10.1016/j.jretconser.2017.06.010

Vashchuk, O., Shuwar, R., 2018. Pros and cons of consensus algorithm proof of stake. Difference in the network safety in proof of work and proof of stake. Electron. Inf. Technol. 9, 10. https://doi.org/10.30970/eli.9.106

Wachter, S., 2018. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. Comput. Law Secur. Rev. 34, 436–449. https://doi.org/10.1016/j.clsr.2018.02.002

Yao, X., Zhang, R., Zhang, Y., 2021. Differential Privacy-Preserving User Linkage across Online Social Networks, in: 2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS). pp. 1–10. https://doi.org/10.1109/IWQOS52092.2021.9521333

Appendix

7.1 Google"/ Case Study 1

Cookie Analysis Data Set - A: google.com		
Sr.No.	**Name**	**Type**
1	1P_JAR	**Tracker**
2	AEC	**Functional**
3	APISID	**Tracker**
4	CONSENT	**Functional**
5	HSID	**Tracker**
6	NID	**Tracker**
7	OGP	**Functional**
8	OGPC	**Tracker**
9	SAPISID	**Tracker**
10	SEARCH_SAMESITE	**Functional**
11	SID	**Tracker**
12	SIDCC	**Functional**
13	SOCS	**Functional**
14	SSID	**Tracker**
15	__Secure-1PAPISID	**Tracker**
16	__Secure-1PSID	**Tracker**
17	__Secure-1PSIDCC	**Tracker**
18	__Secure-3PAPISID	**Tracker**
19	__Secure-3PSID	**Tracker**
20	__Secure-3PSIDCC	**Tracker**
21	OTZ	**Tracker**
22	_ga	**Functional**
23	DV	**Tracker**

Cookie Analysis Data Set - B: google.com		
Sr.No.	**Name**	**Type**
1	AEC	**Functional**
2	CONSENT	**Functional**
3	SOCS	**Functional**
4	__Secure-ENID	**Tracker**
5	DV	**Tracker**

6	OTZ	**Tracker**

Type of Dataset	**Number of Trackers**	**Total Number of Cookies**
Data Set - A	16	23
Data Set - B	3	6
Proposed Model/Data set C	0	N

Proposed Model/Data set C is when the user chooses in-browser cryptocurrency mining and N may the number of functional cookies or essential cookies that would be required for web application to function properly considering the web application service provider uses Cryptojacking or in-browser cryptocurrency mining as method of monetisation.

7.2 “YouTube” / Case Study 2

Cookie Analysis Data Set - A: youtube.com		
Sr.No.	**Name**	**Type**
1	CONSENT	**Functional**
2	CONSISTENCY	**Functional**
3	GPS	**Tracker**
4	PREF	**Tracker**
5	SOCS	**Functional**
6	VISITOR_INFO1_LIVE	**Functional**
7	YSC	**Functional**
8	__Secure-YEC	**Tracker**
9	remote_sid	**Functional**
10	LAST_RESULT_ENTRY_KEY	**Tracker**

Cookie Analysis Data Set - B: youtube.com		
Sr.No.	**Name**	**Type**
1	CONSENT	**Functional**
2	PREF	**Tracker**
3	SOCS	**Functional**
4	VISITOR_INFO1_LIVE	**Functional**
5	YSC	**Functional**
6	__Secure-YEC	**Tracker**
7	remote_sid	**Functional**
8	LAST_RESULT_ENTRY_KEY	**Tracker**

Type of Dataset	**Number of Trackers**	**Total Number of Cookies**
Data Set - A	4	10
Data Set - B	3	8
Proposed Model/Data set C	0	N

7.3 “Facebook” / Case Study 3

Cookie Analysis Data Set - A: facebook.com		
Sr.No.	**Name**	**Type**
1	_js_datr	**Functional**
2	datr	**Tracker**
3	c_user	**Tracker**
4	checkpoint	**Functional**
5	dpr	**Tracker**
6	fr	**Tracker**
7	locale	**Functional**
8	presence	**Functional**
9	sb	**Tracker**
10	wd	**Tracker**
11	xs	**Tracker**

Cookie Analysis Data Set - B: facebook.com		
Sr.No.	**Name**	**Type**
1	_js_datr	**Functional**
2	datr	**Tracker**
3	c_user	**Tracker**
4	dpr	**Tracker**
5	fr	**Tracker**
6	locale	**Functional**
7	oo	**Tracker**
8	sb	**Tracker**
9	xs	**Tracker**

Type of Dataset	Number of Trackers	Total Number of Cookies
Data Set - A	7	11
Data Set - B	7	9
Proposed Model/Data set C	0	N

7.4 “Twitter” / Case Study 4

Cookie Analysis Data Set - A: twitter.com		
Sr.No.	**Name**	**Type**
1	ct0	**Functional**
2	d_prefs	**Tracker**
3	gt	**Functional**
4	guest_id	**Functional**
5	_ga	**Tracker**
6	_gid	**Tracker**
7	_twitter_sess	**Functional**
8	att	**Functional**
9	auth_token	**Functional**
10	fm	**Functional**
11	guest_id_ads	**Tracker**
12	guest_id_marketing	**Tracker**
13	kdt	**Functional**
14	personalization_id	**Tracker**
15	twid	**Functional**

Cookie Analysis Data Set -B: twitter.com		
Sr.No.	**Name**	**Type**
1	ct0	**Functional**
2	d_prefs	**Tracker**
3	gt	**Functional**
4	guest_id	**Functional**
5	_twitter_sess	**Functional**
6	att	**Functional**
7	auth_token	**Functional**
8	fm	**Functional**
9	kdt	**Functional**
10	twid	**Functional**

Type of Dataset	Number of Trackers	Total Number of Cookies
Data Set - A	6	15
Data Set - B	1	10
Proposed Model/Data set C	0	N

7.5 “Bing” / Case Study 5

Cookie Analysis Data Set - A: bing.com		
Sr.No.	**Name**	**Type**
1	BCP	**Tracker**
2	MUID	**Tracker**
3	MUIDB	**Tracker**
4	SRCHD	**Tracker**
5	SRCHHPGUSR	**Tracker**
6	SRCHUID	**Tracker**
7	SRCHUSR	**Tracker**
8	SUID	**Tracker**
9	ULC	**Tracker**
10	_EDGE_S	**Tracker**
11	_EDGE_V	**Tracker**
12	_HPVN	**Tracker**
13	_RwBf	**Tracker**
14	_SS	**Tracker**
15	_UR	**Tracker**
16	ipv6	**Functional**
17	SRM_M	**Tracker**
18	MicrosoftApplicationsTelemetryDeviceId	**Tracker**
19	ai_session	**Functional**

Cookie Analysis Data Set - b: bing.com		
Sr.No.	**Name**	**Type**
1	BCP	**Tracker**
2	MUID	**Tracker**

3	MUIDB	Tracker
4	SRCHD	Tracker
5	SRCHHPGUSR	Tracker
6	SRCHUID	Tracker
7	SRCHUSR	Tracker
8	SUID	Tracker
9	ULC	Tracker
10	_EDGE_S	Tracker
11	_EDGE_V	Tracker
12	_HPVN	Tracker
13	_RwBf	Tracker
14	_SS	Tracker
15	_UR	Tracker
16	ipv6	Functional
17	SRM_M	Tracker

Type of Dataset	**Number of Trackers**	**Total Number of Cookies**
Data Set - A	17	19
Data Set - B	16	17
Proposed Model/Data set C	0	N

7.6 Tiktok / Case Study 6

Cookie Analysis Data Set - A: tiktok.com		
Sr.No.	**Name**	**Type**
1	ak_bmsc	Functional
2	bm_mi	Functional
3	bm_sv	Functional
4	cookie-consent	Functional
5	msToken	Tracker
6	tt_chain_token	Functional
7	tt_csrf_token	Functional
8	ttwid	Tracker
9	__tea_cache_tokens_1988	Tracker
10	csrf_session_id	Functional
11	tiktok_webapp_theme	Functional

Cookie Analysis Data Set - B: tiktok.com		
Sr.No.	**Name**	**Type**
1	_fbp	Tracker
2	_ga	Functional
3	_gat_gtag_UA- 144727112-1	Functional
4	_gid	Tracker
5	ak_bmsc	Functional
6	bm_mi	Functional
7	cookie-consent	Functional
8	gat_UA-143770054-3	Functional
9	msToken	Tracker
10	tt_chain_token	Functional

11	tt_csrf_token	Functional
12	ttwid	Tracker
13	__tea_cache_tokens_1988	Tracker
14	csrf_session_id	Functional
15	tiktok_webapp_theme	Functional

Type of Dataset	Number of Trackers	Total Number of Cookies
Data Set - A	3	11
Data Set - B	5	15
Proposed Model/Data set C	0	N

7.7 Linkedin / Case Study 7

Cookie Analysis Data Set - A: linkedin.com		
Sr.No.	**Name**	**Type**
1	bcookie	Functional
2	lang	Functional
3	li_gc	Functional
4	lidc	Functional
5	_14215E3D5995C57C0A495C55%40AdobeOrg	Tracker
6	JSESSIONID	Functional
7	aam_uuid	Tracker
8	bscookie	Functional
9	li_alerts	Functional
10	_gcl_au	Tracker
11	recent_history	Tracker
12	G_ENABLED_IDPS	Functional
13	chp_token	Functional
14	li_at	Functional
15	li_rm	Functional
16	li_theme	Functional
17	li_theme_set	Functional
18	timezone	Functional
19	wwepo	Functional
20	UserMatchHistory	Tracker
21	li_mc	Functional
22	liap	Functional
23	lms_ads	Tracker
24	_guid	Tracker

Cookie Analysis Data Set - B: linkedin.com		
Sr.No.	**Name**	**Type**
1	bcookie	Functional
2	lang	Functional
3	li_gc	Functional
4	lidc	Functional
5	_14215E3D5995C57C0A495C55%40AdobeOrg	Tracker
6	JSESSIONID	Functional
7	aam_uuid	Tracker
8	li_alerts	Functional

9	li_mc	Functional
10	liap	Functional
11	rtc	Functional
12	G_ENABLED_IDPS	Functional
13	chp_token	Functional
14	fcookie	Functional
15	fid	Functional
16	li_at	Functional
17	li_rm	Functional
18	li_theme	Functional
19	li_theme_set	Functional
20	timezone	Functional
21	wwepo	Functional

Type of Dataset	Number of Trackers	Total Number of Cookies
Data Set - A	7	24
Data Set - B	2	21
Proposed Model/Data set C	0	N

7.8 “Instagram” / Case Study 8

Cookie Analysis Data Set - A: instagram.com		
Sr.No.	**Name**	**Type**
1	csrftoken	Functional
2	dpr	Functional
3	ds_user_id	Tracker
4	ig_did	Tracker
5	mid	Functional
6	rur	Functional
7	sessionid	Functional
8	shbid	Tracker
9	shbts	Tracker
10	fbsr_124024574287414	Functional

Cookie Analysis Data Set - B: instagram.com		
Sr.No.	**Name**	**Type**
1	csrftoken	Functional
2	ig_did	Tracker
3	mid	Functional
4	fbsr_124024574287414	Functional

Type of Dataset	Number of Trackers	Total Number of Cookies
Data Set - A	4	10
Data Set - B	1	4
Proposed Model/Data set C	0	N

7.9 “Yahoo” / Case Study 9

Cookie Analysis Data Set - A: ie.yahoo.com

Sr.No.	Name	Type
1	A1	Tracker
2	A1S	Tracker
3	A3	Tracker
4	EuConsent	Functional
5	GUC	Tracker
6	GUCS	Tracker
7	cmp	Functional
8	CFC	Functional
9	RRC	Tracker

Cookie Analysis Data Set - B: ie.yahoo.com		
Sr.No.	**Name**	**Type**
1	A1	Tracker
2	A1S	Tracker
3	A3	Tracker
4	EuConsent	Functional
5	GUC	Tracker
6	GUCS	Tracker
7	cmp	Functional
8	CFC	Functional
9	RRC	Tracker

Type of Dataset	Number of Trackers	Total Number of Cookies
Data Set - A	6	9
Data Set - B	6	9
Proposed Model/Data set C	0	N