



Preserving Privacy and Security in Browser - Case Study of Mantis Browser

C. Sunitharam, Sayimpu Vinay, Sannapaneni Anand

Abstract: *The internet was meant to shorten the distance between the people to ground-breaking level. It is essential tool for everyday task. But with this, internet service providers are allowed to share and sell their customers web browsing data without their concedence. sometimes, sold data makes security weakened and makes unprecedented way to spammers. With third-party trackers, privacy gone under more risk factor, which makes no deterrent for Cyberattacks, terrorism and other phenomena. In today's high tech environment organizations, Government and individual user has to use web browsers and internet for accessing web data. nowadays some Advertisers trying to mislead users. So, we propose a new way of browsing anonymously, untraceable web surfing and strong firewall using new browser. There will be no bookmarks, Advertisements and no selling of data to marketers.*

Keywords: *Advertisements, Anonymity, browser, Privacy, Proxy, Security.*

I. INTRODUCTION

A web browser which is referred as an internet browser is an application in every smart device which is use to access the world wide web as well as the outer world. When a request was sent to browser by the user from web page, retrieval of the optimized solution will be happened in browser. these data will be sent by the web servers. When the data is retrieved, data will be displayed on the device. During the browsing session, meta data will be downloaded by the browser which is called as cookies. These cookies contain the history of user activities, their information and sometimes their passcodes. Now a days, Browser extension become essential part of browser as it makes tasks easier. Web users, privacy activists, and researchers have responded to tracking and advertising concerns by developing ad and tracker blocking tools [7]. But intensions of many extensions are not simple task but users' data. In Dec 2021, as a result, Google removed over 500 Chrome extensions, which were downloaded millions of times. The extensions uploded private browsing data to attacker-controlled servers, compromising your online privacy [5]. According to reports, two main extensions downloaded by users are ad blocker and VPN/Proxy. Primarily web browsers communicate with servers using HTTP (hypertext transfer protocol) to fetch data of web pages.

Manuscript received on February 27, 2022.
Revised Manuscript received on March 06, 2022.
Manuscript published on March 30, 2022.

* Correspondence Author

Dr. C. Sunitharam*, Assistant Professor, Department of Computer Science and Engineering, SCSVMV, Kanchipuram (Tamil Nadu), India
Sayimpu Vinay, B.E Graduate, Department of Computer Science and Engineering, SCSVMV, Kanchipuram. (Tamil Nadu), India
Sannapaneni Anand, B.E Graduate, Department of Computer Science and Engineering, SCSVMV, Kanchipuram. (Tamil Nadu), India

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](http://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

HTTP allows web browsers to submit query to web servers as well as fetch data from them. identification of pages will be done by means of a URL (uniform resource locator), which is considered as an address, beginning with "http://" for HTTP access. The format of file for a web page is HTML (hyper-text markup language) and is HTTP protocol identifies it. Most internet browsers support a variety of additional formats, such as GIF, PNG, and JPEG formatted images, and can be modified to support more through the use of third-party plugins. The combination of URL protocol and HTTP content specification allows web designers to embed images, video, sound, animations and streaming media into a page, or to make them accessible through the web page. Web browser become most essential application in which daily human needs. Majority of the tasks and jobs are running on the browser. According to reports, there are 4.66 billion internet users are there throughout the world. Emailing, social media, online purchasing, visiting web pages, files transactions - this type of activities comes under browsing. Tim Berners was the person who developed the first web browser named Nexus. Some of the most popular browsers are Firefox, edge chrome, opera. There are different operating systems, which follow different hierarchy of the application execution and storage systems.

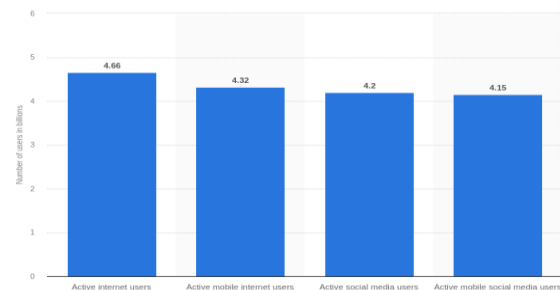


Fig 1: Number of internet users throughout the world in billions [2]

The internet was meant to shorten the distance between the people to ground-breaking level. It is essential tool for everyday task. But with this, internet service providers are allowed to share and sell their customers web browsing data without their concedence. Web browsers are popular targets for hackers, who exploit security holes to steal information, destroy files, and other malicious activities. [3] Sometimes, sold data makes security weakened and makes unprecedented way to spammers. With third-party trackers, privacy gone under more risk factor, which makes no deterrent for Cyberattacks, terrorism and other phenomena. Nowadays some Advertisers trying to mislead users. During the process of accessing website, exchange of data occurs and some traces are left in computing devices.



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

This trace of information will exist in form of cookies, searched terms and cache, information of sessions an URL history. This makes path for the criminals to make criminal activities. These third-party applications are in the form of browsers extensions mainly.

Extensions are the small programs which are written in HTML, CSS and JavaScript. Addon behaviour within the Web browser is characterized by addons making their own decisions independently and often unbeknown to the user, which comprises a complex ecosystem with the user being just one of the participants [1]. Now a days, many browsers have access to install official along with third party extensions. The main drawbacks of the third-party browser extensions are -

- They have access to each and every activity which user do. This access is not manual. Whenever extensions are installed in browser, automatically it consumes more access in the name of flawless experience.
- They can trace the passcodes and personal information. This is possible because They have more access and every activity has to one only through the extensions once they are installed.
- Even if the extension is from trustworthy resource, we will never know if tracking is happening or not. Because there is no guarantee that trust worthy source is always safe.
- Some extensions rewrite the page a show their own advertisements. They make this type of activity because it will generate revenue a make more a traffic.

As per records, Majority extensions downloaded are Ad-blockers and proxy connectors. A search of extensions in the Firefox extensions repository, <http://addons.mozilla.org>, revealed several thousand unsigned extensions and only two that were signed [6]. These extensions are more malicious than any other extensions as these have more access than any other extensions. It is acceptable that user doesn't want to include unnecessary advertisements and have more access to vast websites.

Contradiction with browser extensions is whenever user enter any passcode, or any text, they have access to read it. Browsers has developed special feature call auto-fill password. With help of this feature, extensions are able to see our passwords of any accounts. And coming to Proxy connections, they have history of our records and activity. It makes flawless way to sold our data to other parties.

The increase in cybercrimes that exploits network systems required enhanced information security management. Cybercrime includes theft of intellectual property, financial fraud, hacking, and damage of company service networks [4]. There are many other extensions which are cautious. But compared these two with others, there are less secure and widely used ones. Not only extensions, but also malicious websites, packages and malwares from external devices. As browser cannot guide all these things to users, extensions are still in hands of browsers.

A. Scope of the Project

This project includes several domains namely networking, application, Cyber security, web development. Main agenda of browser is to maintain security, catchy User Interface, support for different web applications and fast & reliable. Implementation of Ad-blocker and proxy settings which are safe and doesn't require third-party packages.

II. PROJECT DESCRIPTION

A. Problem statement

Security of Internet has been a major and rapidly increasing concern for many years. Because it can be occurred not only through the threat of malware, system intrusion, fraud, or damage, but also through the Internet activity tracking. In order to eradicate these vulnerability, encryption of data as a default setting is one of goo choice. Firewalls (which is a software that controls access to and from in network) and anti-malware programs are essential functionalities in the fight against cybercrime. Information commonly stored on a device using Internet browsers include temporary Internet files, cookie information, cache, search history, registry and passwords changes.

Plug-ins and extensions being introduced to the browser can change the page configuration, render the privacy settings unable to perform as it should be, and leave the browser open to attack. Well known browsers such as Google Chrome, Safari, Mozilla Firefox and Microsoft Edge rely on similar methods to ensure speed and popularity of their product. Web Cache is one of the popular ways to store information that can be quickly accessed, thereby no necessity will exist to find data that has already been used. History databases, thumbnails, temporary files, and cookies all help to speed up the user experience and, in their path, leave a plethora of artefact evidence for examiners to feast on. Many studies have been done in this part and free tool, such as Chrome Cache View, Chrome History View, IE Cache View, Internet Evidence Finder, are available to automate the examination process.

All the above browsers have the option to do queries in private mode. Therefore there should be a browser with auto deleting the cache and cookies on user interests, better UI , freedom of choosing search engine , proxy without any external addons . This project is all about satisfying the above conditions.

Proposed system

The Web server sends the data back to the Web browser which renders the results on the desktop or other Internet-accessible device that supports internet browser. Browsers are fully-functional software applications that can extract and render HTML pages, applications, AJAX, JavaScript and other content which are on Web servers.

This architecture depends on three key standards: URLs for naming remote information objects in a global namespace, HTML for encoding document content and HTTP for staging the transfer.

- Hypertext Markup Language (HTML) - the common representation language for hypertext documents on the Web. files of HTML are viewed by using a software called WWW client browser, the primary user interface to the Web. It allows for embedding of images, video streams, sounds, form fields and simple text formatting.

- Universal Resource Identifier (URI) - There are two types of URIs, Universal Resource Names (URN) and the Universal Resource Locators (URL). URLs depends on user location and contain four distinct parts: the protocol type, file name, the directory path and the machine name.

• Hypertext Transfer Protocol (HTTP) - An application-level network protocol for the WWW. For each request, new connection will be established by the HTTP, which is not needed for situations requiring sessions or transactions. Unlike old web browsers, which support only plain HTML files, today's web browsers are large complex software systems. Current browsers, like Mozilla, are equipped with a fully integrated mail and news reader, a composer that allows a user to create web pages as easily as creating a MS Word document, and support for languages and standards that enable users to interact with a web page.

Advantages of proposed system -

- No external ad-blocker is required. Desired websites can show ads or to block advertisement at all.
- Access to clear cache entirely if user insist to.
- Availability of all search engines will make better user experience.
- Connection can be established to any server via proxy which user wants to.

The following modules are used in our project:

- CSS.
- dist.
- ext.
- localization.
- Main.
- node modules
- pages
- reader
- scripts

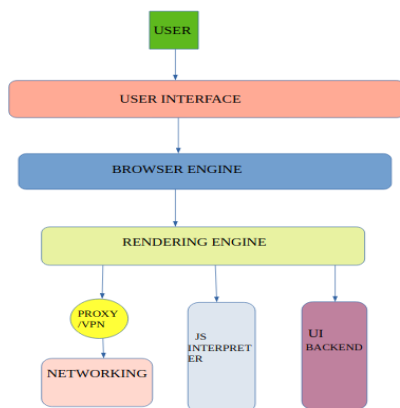


Fig 2: Architecture of MANTIS Browser

B. Algorithm

This whole process begins when the user enters a URL (Uniform Resource Locator) into the browser. Virtually all URLs on the Web start with either https or https which means the browser will retrieve them with the Hyper Text Transfer Protocol (HTTP). In the case of https: the communication between the server and internet browser is encrypted for the purposes of privacy and security. Once a web page has been received from server, it will be rendered on the user's device by the browser's rendering engine. This includes video and image formats supported by the browser. Web pages contain hyperlinks to other resources and web pages. Each link contains a Uniform Resource Locator, and when it is clicked or touched, the browser directs to the respective resource. Thus, the process of bringing data to the user begins. Most internet browsers use cache of web page

resources internally to improve loading times for frequent visits to the same page. The cache can store many items, such as large size images, so they do not need to be retrieved from the web server again. Cached data are usually only existing for as long as the server stipulates in its HTTP response messages.

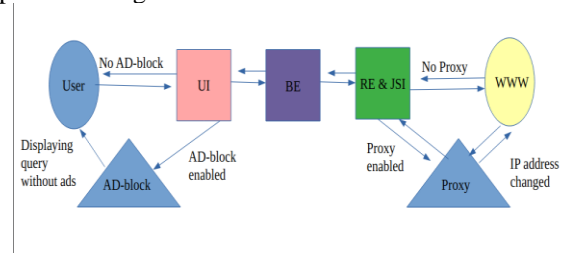


Fig 3: Data flow of MANTIS Browser

III. PROJECT DESIGN AND IMPLEMENTATION

Since this is a MERN based web browser, initialization would be done by npm. When the packages are initialized, npm will begin to start the - NodeJS, ExpressJs, ReactJs, ElectronJs. At first it checks for the IP Address, if user had given any Proxy address, or Manual configurations. When the user enters query, that history will be cached at JavaScript. It cannot save in disk storage. Then the Blink, which is browser engine will come into action. it will receive query from the user and will send the query to the world wide web. If the user enables proxy, query will be passed through proxy encrypted form. A reverse proxy is another common form of a proxy server and is generally used to pass requests from the Internet, through a firewall to isolated, private networks [8]. Thus, the input is reached to web server or destined location. A quality output is one that satisfies the end user's needs and shows information clearly. Any system's processing results are conveyed to users and other systems through outputs. When the web server sends the meta data (which may be either HTML file or Media file) to the browser engine, the rendering engine will receive that data and convert it into respective format. here rendering engine is Webkit. On rendering the Query, the browser will block the Advertisements by default. user has accessibility to toggle the Scripts and Images which leads to the third-party websites. On the deletion tab, whenever the user opens any URL, the data or the passwords cannot be stored in Database and when user closes the tab, the History is terminated from the History stack.

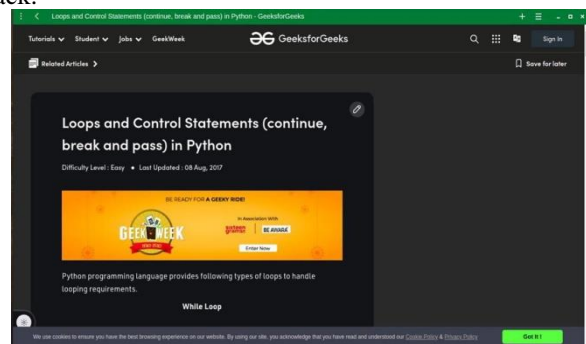


Fig 4: Sample page without ads.



Preserving Privacy and Security in Browser – Case Study of Mantis Browser

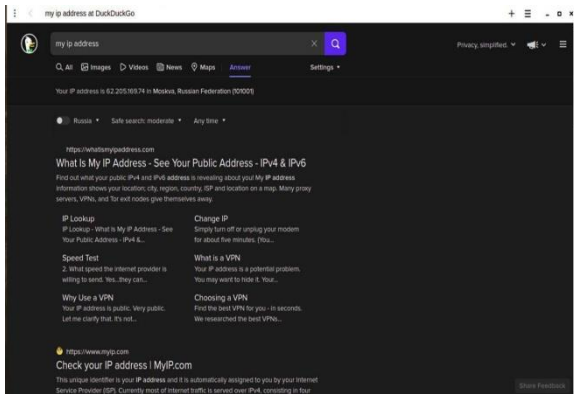


Fig 5: User Query Results

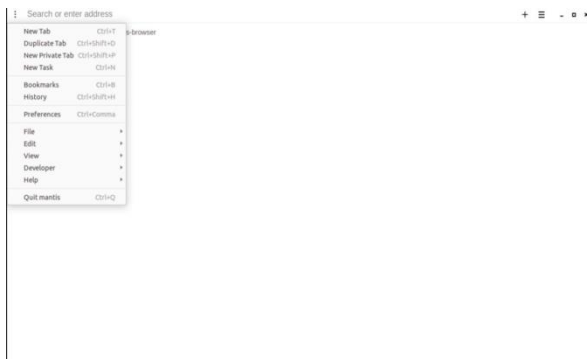


Fig 6: UI of Browser.



Fig 7: Settings

IV. CONCLUSION

The browser main functionality is to present the web resource you choose, by requesting it from the server and displaying it on the browser window. It helps retrieve the information from its vast reservoir viz. internet. It allows collaborators in remote sites to share their ideas and all aspects of a common project. Browser progressively renders the page onto the screen as specified by its HTML, Cascading Style Sheets (CSS), or other page composition languages. Any images and other resources are incorporated to produce the on-screen web page that the user sees. Browser provide common tools enabling users to interact with remote servers in secure fashion.

REFERENCES

1. Ferdman S, Minkov E, Bekkerman R, Gefen D. Quantifying the web browser ecosystem. PLoS One. 2017 Jun 23;12(6):e0179281. doi: 10.1371/journal.pone.0179281. PMID: 28644833; PMCID: PMC5482432.

Retrieval Number: 100.1/ijscce.A35440312122
DOI: 10.35940/ijscce.A3544.0312122
Journal Website: www.ijscce.org

2. <https://www.statista.com/statistics/617136/digital-population-worldwide/>
3. https://en.wikipedia.org/wiki/Web_browser
4. Rasool, Aamir & Jalil, Zunera. (2020). A Review of Web Browser Forensic Analysis Tools and Techniques.
5. <https://www.purevpn.com/blog/chrome-extensions-privacy-breach/>
6. Ter Louw, Michael & Lim, Jin & Venkata Krishnan, V. (2008). Enhancing web browser security against malware extensions. Journal in Computer Virology. 4. 179-195. 10.1007/s11416-007-0078-5.
7. Peter Snyder, Antoine Vastel, and Ben Livshits. 2020. Who Filters the Filters: Understanding the Growth, Usefulness and Efficiency of Crowdsourced Ad Blocking. In Abstracts of the 2020 SIGMETRICS/Performance Joint International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS '20). Association for Computing Machinery, New York, NY, USA, 75–76. DOI: <https://doi.org/10.1145/3393691.3394228>
8. <https://enlargeknowledge.com/what-is-web-browser-and-how-does-it-work/>

AUTHORS PROFILE



Dr. C. Sunitha Ram - Assistant Professor Dr. C. Sunitha Ram received her Ph.D from Sri Chandrasekerandra Saraswathi Viswa Maha Vidyalaya Univeristy, Master of Engineering in Computer Science and Engineering from Sathyabama University and Bachelor of Engineering in Computer Science and Engineering from University of Madras. She has more than 15 years of experience in teaching profession. She is presently working as a Assistant professor in CSE, Sri Chandrasekerandra Viswa Maha Vidyalaya University. She has more theoretical and practical experience in teaching profession. Her area of interest is Principles of compiler design, Computer architecture, System software, Database Management Systems (DBMS), Machine learning and Neural Networks. Her area of specialization lies in Computational intelligence domain. She has been attended more than 20 FDP on various emerging topics, presented various papers in international conferences and also in Journals. She has been served as reviewer committee member for an international journal. She has been an active member in IAENG professional bodies. mail id : csunitharam@kanchiuniv.ac.in



Mr. Sayimpu Vinay, Student, B.E. Mr. Sayimpu Vinay was pursuing his Bachelor of Engineering degree in the stream of Computer Science and Engineering from Sri Chandrasekerandra Saraswathi Viswa Maha Vidyalaya University. For the past 2 years, he has been working on full stack development and he has more theoretical and practical experience in the development area. His area of interest is Principles of compiler design, Computer architecture, System software, Database Management Systems (DBMS), Application development, Blockchain technology and Cyber security and forensics. He had experience as a web developer intern at Verzeo edTech, in which he worked with cutting edge technologies and also developed a few projects. mail id : vinaysayimpu@gmail.com



Mr. Sannapaneni Anand, Student, B.E. Mr. Sannapaneni Anand was pursuing his Bachelor of Engineering degree in the stream of Computer Science and Engineering from Sri Chandrasekerandra Saraswathi Viswa Maha Vidyalaya University. For the past 2 years, he has been working on Machine learning based on python and he has more theoretical and practical experience in the development area. His area of interest is Principles of compiler design, Computer architecture, System software, Database Management Systems (DBMS), Application development, Scikit learn, Numpy, Scipy and Open CV. He had experience as a Machine Learning Intern intern at Verzeo edTech, in which he worked with cutting edge technologies and also developed a few projects. mail id: anandscsvmv2022@gmail.com



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.