

Extension to Block and Customize Websites in the Browser to Isolate the User from Piracy Websites, Fraudulent Risk, Online Gambling, and Social Media Addiction

Mathan Ram S M¹, Vijayakumar J²

¹PG Student, Department of Electronics and Instrumentation, Bharathiar University, Coimbatore, India

²Associate Professor, Head of Department, Department of Electronics and Instrumentation, Bharathiar University, Coimbatore, India

Abstract - Website-blocking browser extensions are tools that users can install in their web browsers to block access to certain websites or content. This extension is a tool that can be installed on web browsers to restrict access to the websites like social media platforms, piracy websites, online fraudulent risk websites, gambling websites, and websites that are unsafe to the users. Users can temporarily block social media, piracy, and other dangerous websites with this extension. A website blocking extension is designed to help users limit their exposure to distracting or harmful websites while browsing the internet. This extension allows users to manually turn on and off to block or restrict access to social media sites, online shopping platforms, piracy websites, and adult content websites. When a user tries to open a website on their blocklist, the extension redirects to a different website and shows them a 404 error message. Website blocking extensions are often used by people who want to improve their focus on studies and productivity or reduce internet usage. Parents can protect their children from unsafe online content.

Key Words: Extension, Websites, Browser, social media, Piracy, Fraud.

1. INTRODUCTION

Our browser extension is the best solution for those who want to increase productivity and maintain focus by blocking distracting websites. With this browser extension, you can quickly turn it on and off manually to activate and create custom lists of websites you want to stop, and the extension will prevent access to those sites while you browse the web. You can stay at work, avoid addictive social media platforms, or protect your privacy and security. This browser extension covers you and controls your online habits, especially for students. Web blocking extensions can help users to stay focused on their work or other essential tasks by blocking access to distracting websites, such as social media or entertainment sites. Web blocking extensions can help to protect user privacy by blocking access to websites that track user behaviour or collect personal information. Web blocking extensions can protect students from accessing inappropriate content, such as pornography or sites that promote hate speech or violence, and addiction to games and social media. Web blocking extensions can also help to protect users from cyber-attacks and other online threats by blocking access to websites that distribute malware or phishing scams and giving security. Web blocking extensions can help users to manage their digital habits and reduce the amount of time they spend on social media or other potentially addictive websites, which can have positive impacts on mental health. This extension can help to increase productivity, protect privacy, enhance security, and promote a healthy and balanced digital lifestyle.

Website-blocking browser extensions are designed to help users control their online experience by blocking access to certain websites or types of content. These extensions can help promote productivity, reduce distractions, and protect users from harmful or offensive content. Using the extension by blocking access to distracting websites, users may be able to focus more on their work and studies or other essential tasks. This can lead to improved efficiency and performance. Another potential outcome is reduced exposure to harmful or offensive content. Website blocking extensions can block access to websites containing malware, phishing scams, or other harmful content. They can also block access to websites with offensive or inappropriate content, such as adult content or hate speech. Social media websites are one of the biggest distractions in the modern workplace. With a blocking extension, employees can temporarily restrict access to these websites and increase productivity. This allows them to focus on their work and studies to complete their tasks quickly.

Using our extension helps users reduce social media addiction, better time management, Increased focus, improve mental health, increase online security, and Enhance privacy. Students must know social media awareness is essential for maintaining online privacy, avoiding cyberbullying, and developing healthy online relationships. Using our extension, students can take control of their addiction. Online gambling is the risk of addiction. Online gambling can be risky due to the lack of regulation. Some online casinos may not be licensed and approved or regulated by a reputable authority, leading to fair play, security, and handling of personal and financial information issues. This can make it difficult for individuals to trust online casinos, leading to fraudulent activities such as identity theft and economic problems.

Using our Extension, Online gambling websites are blocked and keep control at low risk. Piracy websites are illegal and can have severe consequences for the individuals who use them and the creators of the copyrighted material. Piracy websites violate the intellectual property rights of the copyright owners and can result in significant financial losses for the creators. Using our extension, the piracy websites are blocked, and keeping control of online piracy websites is at low risk. Unsafe websites can pose a range of disadvantages and risks to users. One of the main risks of dangerous websites is the potential for downloading malware and viruses onto the user's device. This can lead to severe consequences, including data loss, identity theft, and financial fraud.

2. LITERATURE SURVEY:

These attacks include phishing, spying, DDoS, email spamming, affiliate fraud, mal-advertising, payment fraud, etc. In this paper, we showcase the vulnerability of the current browsers to these attacks by taking Google Chrome as the

case study, as it is a popular browser [1]. The SCB is based on creating ephemeral browser instances and executing them in a controlled environment [2]. BRENDA is a browser extension that can automate the entire process of credibility assessments of false claims [3]. A system that aims to support workers' transitions from breaks back to work—moments susceptible to digital distractions [4]. Understanding the relationship between copyright policy and consumer behavior is an increasingly important topic for participants in digital media markets [5]. The article illustrates the complexities of regulating online gambling [6]. This information, as well as the possibility of contacting thousands of users, also attracts the interest of cybercriminals [7]. Online Social Networks (OSNs) are deemed the most sought-after societal tool the masses use to communicate and transmit information. They are also fast becoming a playground for the spread of misinformation, propaganda, fake news, rumors, and unsolicited messages [8]. It provides an organization and system safeguard mechanism monitoring beforehand prevention, in the matter intervention, and afterward evaluation of this system [9]. Problem-based learning approach encourages instructors to use authentic real-life problems as stimulus and focus for student activity in the context of teamwork [10]. We proposed to apply a block importance model to improve the usability of mobile search interfaces [11]. This work presents a model that combines several techniques (data integrity analysis, changes in the value of deception, and the adoption of high availability architecture) to develop a tool against this type of attack. Several approaches have been proposed to foil website defacement [12]. WebEnclave Extension, while the developers can also leverage WebEnclave middleware to deploy secure web applications with ease in practice [13]. The paper described a method where the Web Service communication between a browser and a Web Service was secured using a plugin implementing the procedures described in the WS-Security for protecting SOAP messages [14]. Our main objective is to allow users to access social media applications safely, which will be achieved with our tool [15].

3. METHODOLOGY

In this methodology, our extension is uploaded to the browser. It creates a wall for the unwanted website. According to the block diagram, the extension blocks the website from the user database. It checks the condition given by the user to block or allow the website's content. If the user adds the website's content to the blocklist to the user database, then the website is blocked. If the website's content is not added to the block list, then the website is accessed, and the user can access the website. The scope of the extension is a web-blocking browser extension, a tool that can be installed on your web browser. It allows you to block specific websites that you find distracting, time-consuming, or harmful and helps you stay focused on your work or studies.

BLOCK DIAGRAM

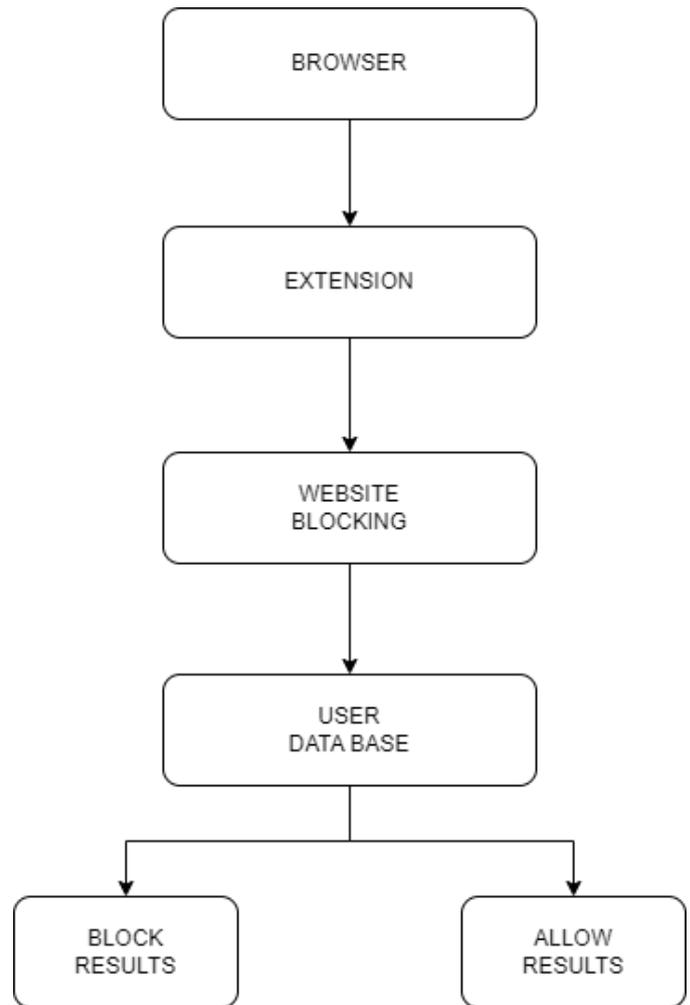


Fig -1: Block diagram of extension

BROWSER: A browser is a software program that permits users to gain access and view information on the web, such as web pages and encoding documentation, in a form suitable for display. It is a piece of software that gets information from the internet and conveys it on a smartphone or tablet. Users of browsers may browse the web and personalize their browsing experience using a number of features, including buttons, menus, and settings. It offers a user interface where users can type in website addresses or search terms, after which the associated pages on the internet or search results are shown. Additionally, users can switch between various pages on the internet, bookmark their favorite websites, and personalize their browsing with add-ons like extensions and plugins using browsers. The most widely used web browsers consist of Microsoft Edge, Google Chrome, Opera, Apple Safari, and Mozilla Firefox.

EXTENSION: It is a software that adds features to your web browser or modifies existing ones. It can be downloaded from the browser's extension store and is typically focused on one function, such as blocking ads or allowing you to print a PDF file of a web page directly from your browser. Browser extensions can also integrate your browser with other services you use and help you stay up-to-date on important notifications. They are created using web-based technologies like HTML, CSS, and JavaScript.

WEBSITE BLOCKING: Website blocking refers to preventing access to certain websites or web content. It has to increase productivity or protect an organization from security threats. Administrators can implement website blocking using tools such as Chrome Enterprise, which allows them to block or allow specific URLs. Users can also block websites on their own devices using browser settings or third-party software. Techniques for website blocking include deep packet inspection (DPI) blocking, which identifies and blocks certain types of content based on signatures or rules.

USER DATABASE: A user database is a set of organized, structured data that is typically stored digitally in a computer system and that is accessible to users. It usually includes related applications and is managed by a database management system (DBMS). A database user is a security principal in the context of an SQL Server that permits a user to connect to a database to access its objects. Based on how they interact with the database, database users like administrators, creators, system analysts, and application programmers can be divided into various types.

BLOCK RESULTS: The user database has checked the results to block if the condition is unsatisfied with the browser extension.

ALLOW RESULTS: If the condition is satisfied with the browser extension, then the user can access the websites when the results are comfortable to allow results.

3.1 FEATURES

We have loaded our extension in the browser to block unknown and spam websites. Our extension makes users stay focused and blocks harmful and distracting websites. There is a user database to check the results to intercept or access the websites. It is a customized extension, that users can turn on and off manually. Our extensions can block specific websites or categories of websites for a specified amount of time in the browser. Using our extensions, we can offer website-blocking features that allow parents to set up rules to limit their children's access to inappropriate websites. It is a parental control mode. Content filtering can block website access based on specific keywords or categories of content. Colleges and organizations often use this approach to prevent students and employees from accessing inappropriate or non-work-related websites. In browser settings, some web browsers include built-in settings for blocking websites. For example, Google Chrome has a feature called "Site Settings" that allows users to block or allow access to specific websites.

In our extension, there are two launchers:

1. Quick Launcher
2. Profile Launcher

QUICK LAUNCHER DISPLAY:

This is the quick launcher display. It is a popup extension that displays the websites to access quickly. It is customized by the user easily. It provides direct link addresses of the websites. The quick launcher display preview is shown in the results.

PROFILE LAUNCHER DISPLAY:

Our extension has a profile launcher registration page to access the blocked websites. The extension has a user registration page to access the blocked websites in the browser. Especially for students, employees, and users who need to access the blocked websites, it requires a registration process to get details about the user to access the website. And the particulars require users' names, ID numbers, designation, departments, name of college/company, gender, country, and date. The user's data will be stored in the database, and the user can access the blocked website easily. Otherwise, the website is stopped every time. After registration, it shows a popup launcher of our extension to customize the websites by the user. It offers an edit option to edit the user registration to access the websites. The profile launcher display preview is shown in the results.

3.2 DESIGN AND IMPLEMENTATION

Creating a browser extension to block websites contains design, implementation, and such coding works.

THE PROGRAMMING LANGUAGE: The programming languages JavaScript, HTML, and CSS are used to build this extension. These languages are used to design and develop our extension.

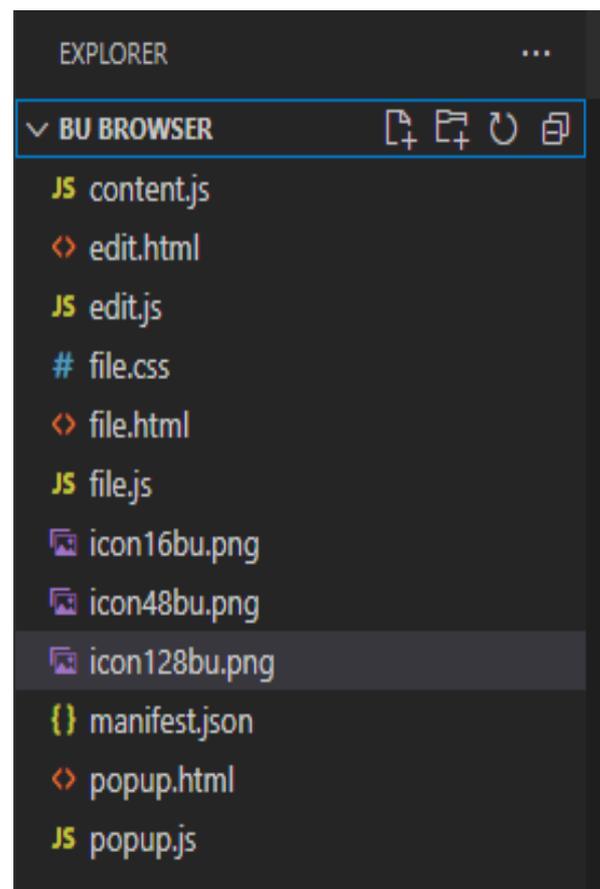


Fig -2: Extension code preview

CREATE THE MANIFEST FILE: A JSON file containing information about the website blocking Extension, including its name, description, version number, and permissions.

```

edit.html JS content.js {} manifest.json X popup.html
{} manifest.json > ...
1  {}
2  "manifest_version": 2,
3  "name": "BU Browser",
4  "version": "0.1.1",
5  "description": "Bharathiar University Secure Browser",
6  "content_scripts": [{
7    "matches": ["<all_urls>"],
8    "js": ["Content.js"]
9  }],
10
11  "icons": {
12    "16": "icon16bu.png",
13    "48": "icon48bu.png",
14    "128": "icon128bu.png"
15  },
16
17  "browser_action": {
18    "default_popup": "popup.html",
19    "default_title": "BU Browser",
20    "default_icon": "icon128bu.png"
21  },
22  "permissions": [
23    "https://www.youtube.com/*",
24    "https://www.facebook.com/*",
25    "https://www.netflix.com/*",
26    "https://open.spotify.com/*",
27    "https://www.snapchat.com/*",
28    "https://www.rummycircle.com/*",
29    "https://www.imdb.com/title/tt15135188/*",
30    "https://www.instagram.com/*"
31  ]
32

```

Fig -3: Manifest file code

IMPLEMENT THE BLOCKING FUNCTIONALITY:

Implement the blocking functionality to block unsafe websites, such as URL blacklist, DNS blocking, or keyword filtering. Implement the code to perform the blocking functionality.

```

edit.html JS content.js X {} manifest.json X popup.html JS popup.js
JS content.js > generateHTML
254 switch (window.location.hostname) {
255   case "www.youtube.com":
256     document.head.innerHTML = generateSTYLES();
257     document.body.innerHTML = generateHTML("YOUTUBE");
258     break;
259   case "www.facebook.com":
260     document.head.innerHTML = generateSTYLES();
261     document.body.innerHTML = generateHTML("FACEBOOK");
262     break;
263   case "www.netflix.com":
264     document.head.innerHTML = generateSTYLES();
265     document.body.innerHTML = generateHTML("NETFLIX");
266     break;
267   case "www.instagram.com":
268     document.head.innerHTML = generateSTYLES();
269     document.body.innerHTML = generateHTML("INSTAGRAM");
270     break;
271   case "open.spotify.com":
272     document.head.innerHTML = generateSTYLES();
273     document.body.innerHTML = generateHTML("SPOTIFY");
274     break;
275   case "www.snapchat.com":
276     document.head.innerHTML = generateSTYLES();
277     document.body.innerHTML = generateHTML("SNAPCHAT");
278     break;
279   case "www.rummycircle.com":
280     document.head.innerHTML = generateSTYLES();
281     document.body.innerHTML = generateHTML("RUMMY CIRCLE");
282     break;
283   case "www.imdb.com":
284     document.head.innerHTML = generateSTYLES();
285     document.body.innerHTML = generateHTML("TAMIL ROCKERS");

```

Fig -4: Blocking functionality code

TESTING THE EXTENSION: Testing the Extension runs the entire program and checks the code at runtime, blocks the unknown and spam websites, redirects them to a different website, and shows them a 404-error message in the browser.

```

edit.html JS content.js {} manifest.json X popup.html
JS edit.js > UpdateLinks
1  var name_text = document.getElementById('name');
2  var website_link = document.getElementById('website');
3  var linkedin_link = document.getElementById('linkedin');
4  var medium_link = document.getElementById('medium');
5  var twitter_link = document.getElementById('twitter');
6  var github_link = document.getElementById('github');
7  var whatsapp_link = document.getElementById('whatsapp');
8  var website_link = document.getElementById('website');
9  var save_button = document.getElementById('save');
10
11  let array = ["name", "website", "linkedin", "medium",
12             "twitter", "github", "whatsapp", "website"];
13  chrome.storage.sync.get(array, function(links) {
14    if (!chrome.runtime.error) {
15      console.log(links);
16      if (links.name)
17        name_text.value = links.name + " ";
18      if (links.website)
19        website_link.value = links.website;
20      if (links.linkedin)
21        linkedin_link.value = links.linkedin;
22      if (links.medium)
23        medium_link.value = links.medium;
24      if (links.twitter)
25        twitter_link.value = links.twitter;
26      if (links.github)
27        github_link.value = links.github;
28      if (links.whatsapp)
29        whatsapp_link.value = links.whatsapp;
30      if (links.website)
31        website_link.value = links.website;
32    }

```

Fig -5: Testing the extension

PUBLISH THE EXTENSION: Publish the Extension in the browser marketplace, such as the Chrome Web Store, Microsoft Store, App Store, and Mozilla Add-ons. The extension is updated and maintained up to date with the latest browser versions.

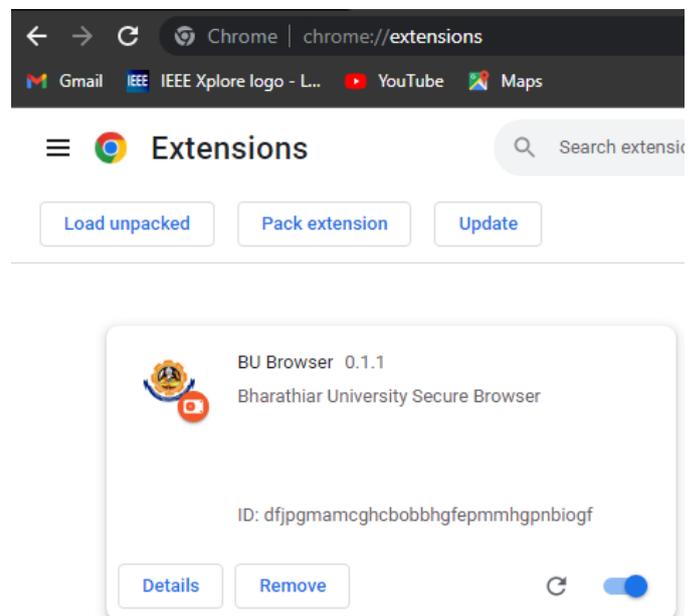


Fig -6: Publish the extension

3.3 BROWSER EXTENSIONS PLATFORMS

This extension operates in multiple browsers, such as Google Chrome, Mozilla Firefox, or Microsoft Edge. Each browser has its own set of APIs and development frameworks. Browser extensions are used on multiple platforms, but the specific platforms that support them depend on the browser being used.

Google Chrome: Chrome extensions can be used on Windows, Mac, Linux, and Chrome OS.

Microsoft Edge: Edge extensions can be used on Windows, Mac, and Android.

Mozilla Firefox: Firefox extensions can be used on Windows, Mac, Linux, and Android.

Safari: Safari extensions can be used on Mac and iOS.

Opera: Opera extensions can be used on Windows, Mac, Linux, and Android.

3.4 TECHNICAL ASPECTS OF CREATING A BROWSER EXTENSION TO BLOCK WEBSITES

The extension will identify the website requests made by the user and intercept them to determine whether to allow or block them. The extension provides users to customize the list of websites they want to stop and provides an easy way to add or remove websites from the blocklist. The extension will be compatible with different web browsers and operating systems and manage user privacy and security. The extension provides notifications to users when a website is blocked and gives feedback and instructions on unblocking the site if necessary. These are the technical aspects of browser extensions to block websites and are designed to help users take control of their online experience.

4. RESULTS

A website-blocking browser extension is a tool that allows users to block access to specific websites or categories of websites while using their web browser. When a user installs and configures a website-blocking extension, the extension will prevent the user from accessing the blocked websites by redirecting them to a different page, displaying a warning message, or simply blocking access altogether.

The specific result of a website blocking extension will depend on the settings chosen by the user. For example, if the user creates a blocklist of particular websites, they will be inaccessible when the user tries to access them. Depending on the extension and the user's settings, they may be redirected to a different page, such as a warning page or a custom message created by the user, when they try to access a blocked website.

Web-blocking browser extensions can be very useful to users who want to take control of their online experience and manage their digital habits. If users visit an unknown or spam website, it redirects them to a different website, showing them a 404 error message in the browser.

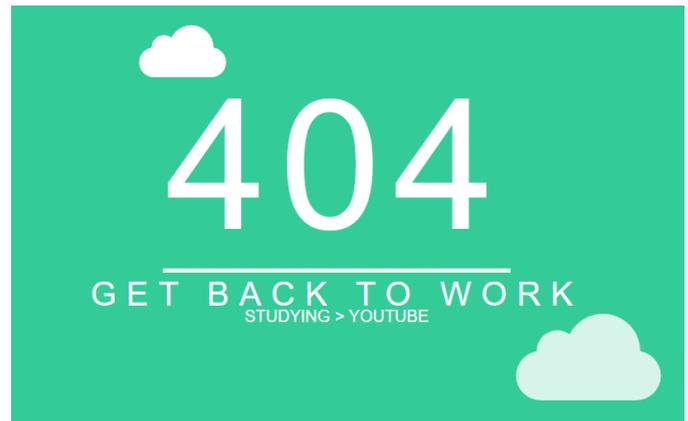


Fig -7: Preview of 404 Error Display

4.1 PROFILE LAUNCHER DISPLAY

This is the profile launcher user registration page to access the blocked websites.

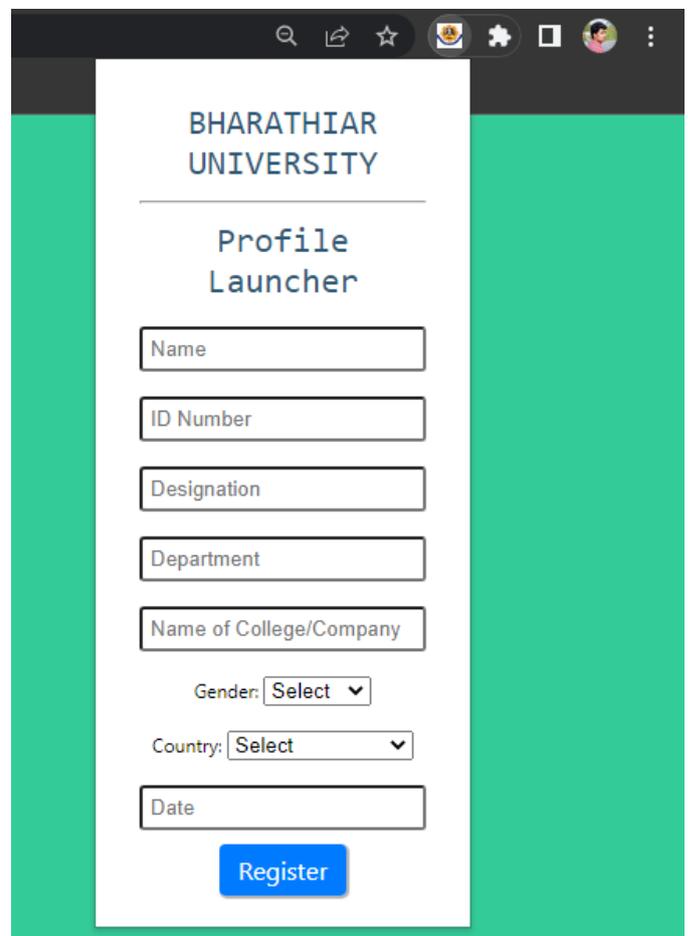
A screenshot of a web browser showing a registration form titled 'Bharathiar University Profile Launcher'. The form is white and centered on a green background. It contains several input fields: 'Name', 'ID Number', 'Designation', 'Department', 'Name of College/Company', 'Gender' (with a dropdown menu), 'Country' (with a dropdown menu), and 'Date'. A blue 'Register' button is at the bottom of the form.

Fig -8: Profile Launcher Display

The profile launcher contains the user's data for registration. And it stores the data to protect and secure it. This is the additional technical work that we made to help the users. This feature satisfies the user's needs.

4.2 QUICK LAUNCHER DISPLAY

This is the Quick Launcher display preview in our Extension

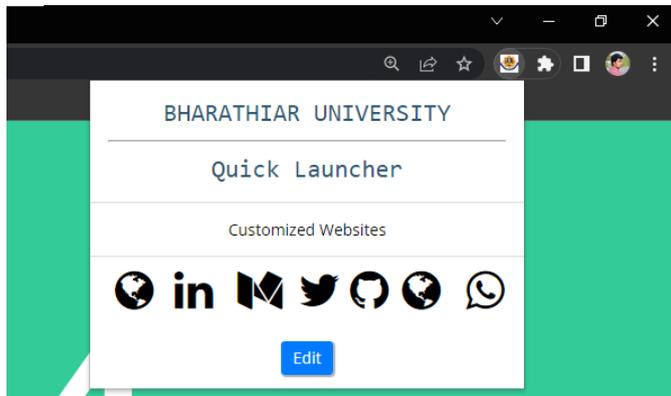


Fig -9: Quick Launcher Display

Quick launcher display is a popup display that shows the direct website link to access quickly and displays with the website's logo. It is a customized popup display that the user can edit or modify the website.

5. CONCLUSIONS

A website-blocking browser extension can be helpful for individuals wishing to control their internet usage or limit distractions. This extension evaluates effectiveness, ease of use, customization options, security, privacy, and support to the user. This extension meets your needs and preferences while maintaining your privacy and security. With the right website-blocking browser extension, you can control your internet usage and focus on your work and studies to complete the tasks.

REFERENCES

1. Gaurav Varshney, Sumant Bagade, and Shreya Sinha. Malicious browser extensions: A growing threat: A case study on google chrome: Ongoing work in progress. In 2018 International Conference on Information Networking (ICOIN), pages 188–193, 2018.
2. Marta Palanques, Roberto Dipietro, Carlos del Ojo, Marcel Malet, Miquel Marino, and Toni Felguera. Secure cloud browser: Model and architecture to support secure web navigation. In 2012 IEEE 31st Symposium on Reliable Distributed Systems, pages 402–403, 2012.
3. Vinay Setty Bjarte Botnevik, Eirik Sakariassen. Brenda: Browser extension for fake news detection. In SIGIR, 2020.
4. Daniel Avrahami Matthew L. Lee, Laurent Denoue. Overcoming distractions during transitions from break to work using a conversational website blocking system. In CHI Conference on Human Factors in Computing Systems, 2019.
5. Rahul Telang Brett Danaher, Michael D. Smith. The effect of piracy web site blocking on consumer behavior. In SSRN, 2015.
6. Sylvia Kairouz Martin French, Dani Tardif and Annie Claude Savard. A governmentality of online gambling website blocking provisions. In Canadian Journal of Law and Society, 2021.
7. Giovanni Vigna Gianluca Stringhini, Christopher Kruegel. Detecting spammers on social networks. In ACSAC Annual Computer Security Applications Conference, 2010.

8. Arushi Gupta and Rishabh Kaushal. Improving spam detection in online social networks. In 2015 International Conference on Cognitive Computing and Information Processing (CCIP), pages 1–6, 2015.
9. Zhang FuSheng, Yang Ling, Jia ZongFu, Qi XinJun, and Zong Mingkui. The monitoring and early-warning system of students' learning based on the campus cloud. In 2017 12th International Conference on Computer Science and Education (ICCSE), pages 587–590, 2017.
10. Hsiu-Ping Yueh and Wei-Jane Lin. Developing a web-based environment in supporting student's team working and learning in a problem-based learning approach. In Third International Conference on Creating, Connecting and Collaborating through Computing (C5'05), pages 145–149, 2005.
11. Xing Xie, Gengxin Miao, Ruihua Song, Ji-Rong Wen, and Wei-Ying Ma. Efficient browsing of web search results on mobile devices based on block importance model. In Third IEEE International Conference on Pervasive Computing and Communications, pages 17–26, 2005.
12. Barerem-Melgueba Mao and Kanlanfei Damnam Bagolibe. A contribution to detect and prevent a website defacement. In 2019 International Conference on Cyberworlds (CW), pages 344–347, 2019.
13. Xinyu Wang, Yuefeng Du, Cong Wang, Qian Wang, and Liming Fang. Webenclave: Protect web secrets from browser extensions with software enclave. IEEE Transactions on Dependable and Secure Computing, 19(5):3055–3070, 2022.
14. L. Lo Iacono and H. Rajasekaran. Secure browser-based access to web services. In 2009 IEEE International Conference on Communications, pages 1–5, 2009.
15. S. Shivangi, Pratyush Debnath, K. Sajeewan, and D. Annapurna. Chrome extension for malicious URLs detection in social media applications using artificial neural networks and long short-term memory networks. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pages 1993–1997, 2018.

BIOGRAPHIES



Mathan Ram S M currently a P. G. student in Department of Electronics and Instrumentation, Bharathiar University.



Vijayakumar J obtained his Bachelor of Engineering in Electronics and Communication Engineering from Maharaja Engineering College, Avinashi, affiliated to Bharathiar University, Coimbatore in 2003. He obtained his Master of Engineering in Applied Electronics from Bannari Amman Institute of Technology, Sathyamangalam under Anna University, Chennai in the year 2005. He received Doctor of Philosophy in Information and Communication Engineering from Anna University, Chennai in 2015. He is a member in IE, IETE, ISECE, and UASEE. He has so far published over 50 papers in various National and International Journals and Conferences. His area of interest is Digital signal and Image Processing.