

AD-BLOCKING USING RASPBERRY PI-HOLE¹D Jagan,²K Amarender,³M Sunitha,⁴D Vijayalaxmi^{1,2,3}Assistant Professor,⁴Student

Department Of ECE

Christu Jyothi Institute Of Technology & Science,Colombo Nagar,Telangana

ABSTRACT

This study aimed to design an ad-blocker which would run widely on the whole network and block the ads from the web pages of any web site. To define it properly, a small computer with a SoC (System on Chip) which is widely regarded as Raspberry Pi is used and it is connected to the home network, the network for which we have to block the ads. Software called Pi Hole is used to filter the web pages with ads on the home network. So, after this all the devices say, smart phones, laptops, PCs are connected to this home network. Then these devices are pointed to the Pi and the Network Traffic through devices now go through the Pi. So, eventually the ads get filtered out in the Raspberry Pi even before reaching the use r's devices. This setup will only work when your devices are connected to the network on which the Raspberry Pi is running. This decreases the latency and increase the browsing speed of any browser by cutting out the extra data these ads take up while loading a web page. Also the user can add a set of websites or a bunch of web pages to be white listed on the Pi Hole software, disabling the ad block over these particular websites or web pages.

Keywords: Raspberry pi, ad-blocker, Pi Hole, network traffic, whole network, home network, Raspbian , browsing speed, web page.

I. INTRODUCTION:

The most annoying element present in a webpage might probably be the ads. People don't want to waste their time watching ads while checking their daily News feed on Facebook or while watching a web series on Netflix. Ads have become the key to make money for a website owner and people would always want to get rid of those ads. So, rather than using a third party ad blocker from an unknown source a project have been designed on an ad blocker which would run widely on the whole network and block the ads from the web pages of any web site.

Based on the way the landscape is evolving, the future of online advertising is growing day by day. It's been a wonder: is there a way that content producers and ad publishers can make money without creating a hugely disruptive and annoying ad experience. A previous Hub Spot study revealed people really vent their ire on specific types of ads (think pop-ups and auto playing videos), so it is to be set out to find out more. To figure out what to ask, a study with Ad Block Plus, one of the most widely used ad blocking extensions in the world, to create the study questions and secure survey responses through SSI, an independent survey panel provider.

With the use of Ad Block Plus and responses got through the Server Side Include, an idea of how and why should the ads have to be blocked that occurs in the webpages that work through in times. Additionally, now-adays hackers publish ads in webpages which gives link to their gateway, where at the times when the ad is clicked it gets linked to the hacker's website where it will be asked to fill up the personal details of the end-users and by having all those details the hacker can threaten the end-user. In this case, Ad Blocker play its role in dealing to filter all the ads where the end-user can work in their stuffs in a cool manner.

The aim of this project is to develop a low power Network Ad Blocker using Raspberry pi that is capable of blocking all the ads that is published in the websites.

Pi hole which installed in the Raspberry pi with the help of the pi hole all the ads will get filtered. The router which is connected to the Raspberry pi, which provides the interconnection to all the devices connected to it, with having the Raspberry pi connected to it all the ads are filtered in an effective way that not even a single ad will appear in the website.

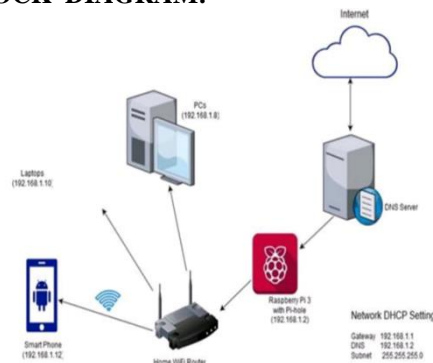
1.2 BLOCK DIAGRAM:

Fig1: Block Diagram

1.2.1 Function of Block Diagram**• RASPBERRY PI-HOLE:**

Pi-hole is a network-wide ad blocker based on the Raspberry Pi. It's simple to set up on the Raspberry Pi Zero by performing certain installation instructions on a Raspberry Pi running Raspberry Pi OS. Once Pi-Hole is setup, you may configure your devices to utilize its IP address, directing all traffic via it. When a website (that serves advertisements) requests the domain of its ad servers to receive an ad, Pi-hole compares the domain name to its list of banned ad-servers.

Then, to begin blocking advertising straight immediately, redirect computers to the Raspberry Pi's IP address. We can also add your favorite websites to a whitelist, which we highly encourage you to do to help them keep the lights on.

• INTERNET ROUTER:

A router is a device that connects two or more packet-switched networks or subnet works. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between LANs (local area networks) and WANs (wide area networks). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

• DNS SERVER:

The domain name system (i.e., “DNS”) is responsible for translating domain names into a specific IP address so that the initiating client can load the requested Internet resources. The domain name system works much like a phone book where users can search for a requested person and retrieve their phone number. DNS servers translate requests for specific domains into IP addresses, controlling which server users with access when they enter the domain name into their browser.

1.3 PROJECT ELABORATION:

1.3.1 Methodology:

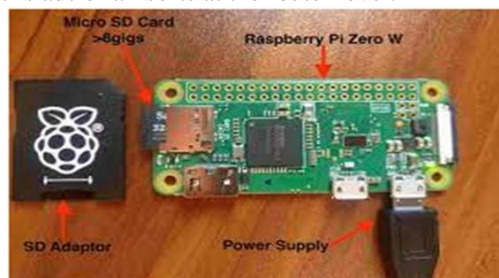
Pi Black-hole is a little application that runs on the Raspberry Pi and block adverts at the DNS level, it can optionally act as your DHCP server as well. Pi Black-Hole works at the DNS level. So, when an ad is blocked, it’s actually prevented from being downloaded in the first place because the DNS query is intercepted. Since these ads images, videos, and sounds are not being downloaded, network will perform better. For better understanding, domains trying to spread malware through bougs ‘Adobe Flash’ updates can be blocked at Network level. For devices such as Smart TVs which don’t use a browser but still feature ads, these can also be blocked using Pi Black-Hole. Viewing YouTube videos on mobile phones, PlayStation and Xbox gaming consoles, all ads will be blocked.

1.3.2 Framework of Proposed System:

A software is designed in such a way that it is capable of blocking all the ads that is published in the websites. Pi hole which installed in the Raspberry pi with the help of the pi hole all the ads will get filtered. The router which is connected to the Raspberry pi, which provides the interconnection to all the devices connected to it, with International Journal of Pure and Applied Mathematics Volume 119 No. 10 2018, 1771-1775 ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version) url: <http://www.ijpam.eu> Special Issue [ijpam.eu](http://www.ijpam.eu) 1771 having the Raspberry pi connected to it all the ads are filtered in a effective way that not even a single ad will appear in the website. A new framework is developed with three components (i) Raspberry pi, (ii) Router and (iii) Keyboard. The first

thing is needed to do is download and burn the PiHole image. The image is a version of a Raspberry Pi operating system called Diet Pi, which cuts a lot of junk from Raspbian, and is packed with all the software needed to run the ad blocker. Insert the SD card into the Raspberry Pi and connect the keyboard. Connect the Ethernet cable to the WiFi router, then plug in the Raspberry Pi, and wait for it boot.

Once the Raspberry Pi is running the Pi-Hole software, still need to route devices traffic through it so ad blocking works. To do this, one need to change the device's DNS settings. Thisway, the devices ping the Pi to block ads as long as the same network remains constant. This is pretty simple, but varies depending on the devices and what the software is running. A user can have software to block ads on a computer, but if any user want to block ads on all devices— from smartphone to the tablets— need something a little stronger. Enter the Pi-Hole, a Raspberry Pi image that blocks ads of all sorts at the router level.



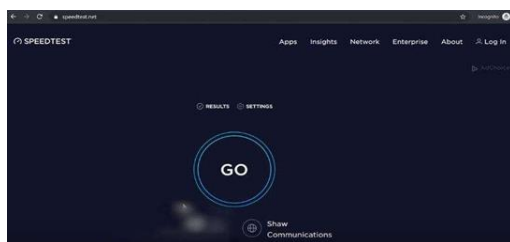
Fig(1.2): Proposed System

II. RESULT:

This project goes on with a network based Ad Blocker, where only the connected devices will be filtered with the ads that appear in websites. The end-user need to be within the network to be filtered with the ads that appear in web pages that the user views. It is better to use a ad-blocker created by us instead of third party ad blocker. Moving on with a non-traditional ad blocker where there is no third party involved only the end users connected with router will get filtered with the ads.



Fig(5.1): Before connecting the device



Fig(5.2): After connecting the device

Thus increases security within the network. Now-a-days there are some traditional ad blockers in the internet, which will be added as a extension.

2.2 APPLICATIONS:

This software or similar process is used in many applications and android apps as mention below:

- AdAway
- Adblock Plus
- AdGuard
- Blokada
- Browsers with ad-block
- Change your DNS
- DNS66
- Brave Browser

2.3 ADVANTAGES:

- Increase in network speed
- No advertisements
- Secured personal information
- Protection from malware
- No third party-cookies
- No online tracking
- Cost and availability
- Excellent power efficiency
- Huge processing power in a compact board.
- Supports Linux, Python (making it easy to build applications).
- Many interfaces (HDMI, multiple USB, Ethernet, onboard Wi-Fi and Bluetooth, many GPIOs, USB powered, etc.).

2.4 DISADVANTAGES:

- Browsing data privacy risk — Some ad blocking software may be sending your browsing behaviour to a third-party server.
- Risk of web pages breaking — Blocking page scripts may hamper the functionality of some websites and lead to a broken browsing experience.
- There is not any fuse protection on the Raspberry pi,so if you connect pins incorrectly, you can damage the board.
- It is not as fast in terms of CPU processing speed nor does it have as much memory as traditional pc or laptops.

III. CONCLUSION AND FUTURE SCOPE

3.1 CONCLUSION:

A framework that uses electronic gadgets with less power utilization to filter ads containing Raspberry Pi, router, keyboard (For initial set up) and Ethernet cable. Apart from the traditional Ad Blockers, which might

cause problems in situations because it is developed by a third party developer. This project goes on with a network based Ad Blocker, where only the connected devices will be filtered with the ads that appear in websites. The end-user need to be within the network to be filtered with the ads that appear in webpages that the user views. It is better to use a ad-blocker created by us instead of third party ad blocker. Moving on with a non-traditional ad blocker where there is no third party involved only the end users connected with router will get filtered with the ads. Thus increases security within the network. Now-a-days there are some traditional ad blockers in the internet, which will be added as a extension. Later it will add some harmful software, which in turn downloads some viruses which causes the user to face issues in the device. So it is better to go on with a ad blocker created within the network.

3.2 FUTURE SCOPE:

There are numerous mobile advertising blockers were present in the form of application centre such as Google Play Store and the increasing numerous user related defects were suggest significant ineffectiveness or usability problems , so that to examine the unexpected environment is important. The approximate mobile phone user gives positive rating towards using advertisement blocker in mobile phones though using the presence of malware tools. After taking he survey, Negative reviews of around 16% interconnected itself to the unsuccessful towards the advertisement blocking applications, they were complaining some of the serious issues in their performances. Besides, our testing of Advertisement Blockers, Several practicing issues were occurred at the same time of working some other induced applications or browsing in the browser caused by number of Advertisement blockers such as F secure freedom VPN.These were found by testing the Advertisement blockers from the results or evaluations or the reviews given by the users. The scientists believes that this work will definitely will helps to study the effectiveness of the advertisement blocking. In the complement of providing the Intuition given by our research with an exhaustive set of energetic evaluations to tell the runtime characteristic features of the advertisement blocking applications to be provided as its future work. Future Work to enable UI to the admin and to get the feedback from the users about the ad free network.

BIBLOGRAPHY

Websites:

- <https://www.the-diy-life.com/setting-up-a-pi-hole-network-ad-blocker-on-a-raspberry-pi-zero-w/>
- <https://acadpubl.eu/jsi/2018-119-10/articles/10b/59.pdf>

- <http://www.jsrpublication.com/gallery/6-jsr-february-s356.pdf>
- <http://www.raspberrypi.org/downloads/>
- <https://www.lifehacker.com.au/2015/02/turn-a-raspberry-pi-into-an-ad-blocker-with-a-single-command/>
- <https://github.com/pi-hole/pi-hole>

Books:

1. K. W. Y. Au, Y. F. Zhou, Z. Huang, and D. Lie. PScout: Analyzing the Android Permission Specification. In CCS, (2012).
2. Android Permissions. <http://developer.android.com/guide/topics/security/permissions.html>.
3. M. Ikram, N. V. Rodriguez, S. Seneviratne, D. Kaafar, and V. Paxson. An analysis of the privacy and security risks of android VPN permission-enabled apps. In ACM IMC, (2016).
4. A. Lerner, A. K. Simpson, T. Kohno, and F. Roesner. Internet jones and the raiders of the lost trackers: An archaeological study of web tracking from 1996 to 2016. In USENIX Sec., 2016.
5. C. Wills and D. Ununoglu. What Ad Blockers Are (and Are Not) Doing. Technical Report, (2016).
6. S. Seneviratne, H. Kolamunna, and A. Seneviratne. A Measurement Study of Tracking in Paid Mobile Applications. In ACM WiSec, (2015).
7. W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. TaintDroid: An Information Flow Tracking System for Real-Time Privacy Monitoring on Smartphones. CACM, (2014).
8. J. Jeon, K. K. Micinski, J. A. Vaughan, A. Fogel, N. Reddy, J. S. Foster, and T. Millstein. Dr. Android and Mr. Hide: Fine-grained Permissions in Android Applications. In ACM SPSM, (2012).
9. A. Bose, X. Hu, K. G. Shin, and T. Park. Behavioral Detection of Malware on Mobile Handsets. In ACM MobiSys, (2008).
10. N. Wang, B. Zhang, B. Liu, and H. Jin. Investigating effects of control and ads awareness on android users' privacy behaviors and perceptions. MobileHCI, (2015).
11. M. Ikram, H. J. Asghar, M. A. Kaafar, B. Krishnamurthy, and A. Mahanti. Towards seamless tracking-free web: Improved detection of trackers via one-class learning. PETS, (2017).