Proceedings of the 4th South American Conference on Industrial Engineering and Operations Management, Lima, Peru, May 9 - 11, 2023

NETBLK: Network Adblocker using Raspberry Pi

John Ezekiel Dunglao, Sean Deniel Agustin, Jay Tanglao, Vraelle Velarde
College of Computer Studies
Angeles University Foundation
Angeles City, Philippines
Mr. Ray A. Nicolas - Adviser
Faculty - College of Computer Studies
Angeles University Foundation
Angeles City, Philippines

Abstract
Advertisement blocking refers to the practice of using software or browser extensions to prevent advertisements from displaying on web pages or mobile applications. It is a growing trend among internet users, with an increasing number of people opting to block ads online. The use of adblockers has become a significant concern for businesses and advertisers who rely on online advertising to generate revenue. This study aims to design a DNS server that will have a similar function as a firewall. A small board computer called Raspberry Pi will be used to connect to a network where websites with ads will be filtered. A small open-source networking tool called Pi-Hole will be used for configuring the Raspberry Pi. The device will now be the location of network traffic traveling through the network. This system is applied through the use of waterfall methodology which is a linear, sequential approach to project development, where the development process is divided into distinct phases. These phases typically include requirements gathering, design, implementation, testing, and maintenance. The results of the survey show that the system has been accommodating to the evaluators. While adblocking software can improve the user experience by blocking annoying and intrusive ads, adblocking can be effective in mitigating certain information threats particularly those that originate from malicious ads. Malicious advertisements can contain malware or lead users to phishing sites, and adblocking can prevent them from being displayed on a user's device. It is very important to protect such information from being stolen by attackers within a network.

Keywords
Advertisement blocking, DNS, firewall, network

1. Introduction
Online Advertising is a way of getting revenue for a certain application or website. It is helpful in earning money by making users watch a 10-second video or publishing links that will pop up on a certain website. This is a way to reach the audiences and a way to monetize the content that was produced. The downside of online advertisements is that people tend to ignore them. Ads are found to be an annoying aspect that is present on the internet. People would not want to watch advertisements while browsing on social media as it is considered a waste of time. Another major problem with online advertising is that it could impose security and privacy risks. Cybercriminals use advertisements as an advantage in installing malware or collecting information by publishing phishing sites which is a domain of a website with the same appearance. It is difficult to identify which is a “good” or “bad” website for a user to visit. At present, cybersecurity plays a vital role in the devices the people use every day. Since all the transactions are accessible on the computer, mobile phones, and other devices, security threats need to be prioritized. The cyber threats range from Trojan and viruses to botnets and toolkits. At that time, 96% of smartphones do not have pre-installed security software in which, which opens a lot of security threats on the devices. There is traditional security software on the PC, e.g., firewalls, encryption, and antivirus but they are not currently available on smartphones. This study aims to protect devices from tracking, malware, and phishing domains that are found on malicious sites or even remove ads that are found to be annoying.

1.1 Objectives
The study aims to implement an adblocker on a network level that will enable filtering and efficiency from the devices that are connected to a network against malicious domains and trackers. Websites that contain malicious, tracking and unwanted content will be filtered out. The study will provide protection to the devices using the DNS server and interactions between the client and server.

2. Literature Review
Adblocking

In the year 2018, a milestone was reported that digital media will surpass the time spent over televisions for the first time ever. From an internet user's perspective, paid content is being bombarded into his/her daily browsing activities. According to Karageorgos and Zhang (2018), these exposures to paid content can be a concern for a user's privacy. Adblocking has been used in order to control such exposures to these paid contents. Adblocking has been changing the internet because of extended usage. The 2014 report of PageFair and Adobe has stated that there is around 41% increase of desktop adblocking users in a year reaching 198 million users in the year 2015. Meanwhile, PageFair stated that by end of 2016, there were 236 million desktop adblocking users. Since the adoption of ad-blocking technologies from a more significant proportion of users, there is a projected loss of digital advertisements. Reducing internet providers' capacity to control their personal websites and data publicity through online advertising (Thomas 2018). Various kinds of digital marketing are developed as a result of the availability of internet advertising techniques, such as advertising messages, flashing ads, and web banners. Each web user can avoid adverts by using ad blocking software on their device as well as knowing online users' perspectives about online advertising. Since free content on websites seems to be impossible, adverts are made to ensure overall sustainability (Ha 2021). Internet ads may be beneficial and helpful to certain users, disturbing to others, and intrusive to others.

Raspberry Pi

Technology has been vastly evolving every day and there are now low-cost small board computers that are existing today such as the Raspberry Pi. Raspberry Pi is created to help people engage in different projects and provides computing access. Most projects that are related to internet of things (IOT) use Raspberry pi as one of their materials. Most projects that use Raspberry pi are security-related from Passive Infrared (PIR) sensors to malware detection (Johnston and Cox 2017). As regards to adblocking, the study of Kadav et al. (2021) stated that an inexpensive and energy-efficient device such as the Raspberry Pi has the capability to act as a DNS sinkhole whereas every device connected to a network can be protected from such unwanted content. It is designed to be used on home networks (Kadav et al. 2021). The Raspberry Pi Foundation encourages the use of Raspberry pi inside a classroom to provide students a better understanding and make them do different experiments in the field of technology. There are currently many versions of Raspberry Pi depending on the specifications and the clients that will be using it. For this study, the proponents will use the Raspberry Pi Zero W which has a WiFi function and it can be used for 50 users and below. Selecting which version of Raspberry pi to use depends on the complexity of a project.

The raspberry pi is a low-cost device that has a similar size to a credit card but it is powerful. It can be used on televisions and computers. The capability of this little device is that it helps in the exploration of computing on all ages. Program raspberry pi can be used with different programming languages such as Python but this study will only configure the Raspberry Pi with Pi-hole. The RPi foundation is founded in 2009 in the United Kingdom, and it is led by David Braben, one of its biggest goals is to provide a low-cost computer to teach other people about computer science. Raspberry Pi measures about 85.60mm x 56mm x 21mm and it weighs 45g. It also has an HDMI port to connect to the TV or monitor, USB port for keyboard and mouse (Nayyar and Pu ri 2017). The Raspberry Pi is a popular device to be used in IoT projects. The most common Raspberry pi projects are automation and security systems. It may be a low-cost device but it can be powerful enough to create such projects. In a recent study in January 2022, a team of researchers made up of Annelie Heuser, Matthieu Mastio, Duy-Phuc Pham, and Damien Marion from the Research Institute of Computer Science and Random Systems (IRISA) were able to scan and detect malware through electromagnetic waves using Raspberry Pi. The unique thing is that no software or modifications were made during the process.

Pi-Hole

Pi hole is discovered by Mark Drobnak who is a college freshman from Rochester Institute of Technology. He created an ad blocker named Pi-hole which is also called advertising black hole. The advertisements blockers only cater to devices that wish to download the plug-ins, but Pi-hole blocks all the ads across the network including all the apps that are used daily by the user. The use of Pi-hole is intended for those devices that have a capability to a network such as Raspberry Pi. The difference between the ad blockers and Pi-hole is that the advertisement blocker is keeping the web browser from totally viewing ads inside the browser yet the ads were still being downloaded, advertisement blockers would only hide the ad from the user. On the other hand, Pi-hole is preventing ads to leave the network using Domain Name System (DNS). In summary, Pi-hole prevents ads to get downloaded and getting in the network (Taib, 2020). It is capable of blocking advertisements by simply configuring it with the Raspberry Pi or use a docker container then point each device to the DNS server. The proponents will apply an enhanced configuration using the tool through scripting and improvements to its listing function.

Summary

In summary, the threat of online advertisement can produce a massive impact within a device and it has always been a matter of concern. Malware, on the other hand, has its own set of concerning factors as technology evolves, cybercriminals, tend to create new techniques in exploiting web pages in order to steal information through phishing. As years pass, more and more people will engage in using adblockers in order to protect their private information and to avoid being disturbed and interrupted by advertisements that will display through the whole webpage. About 42%

of internet users in the world are found to be using adblockers and are mostly using browser extensions such as Adblock. The two most common reasons for the use of adblocking are having too many ads and they are being annoying or irrelevant. The use of adblockers among users has been questioned and it is said to be unethical because it will affect an advertiser's right. However, users of the internet develop trust issues, concerns and attitudes which are the main reasons for the use of adblockers. There is no guarantee that a system will never be attacked and this project will take part in avoiding such attacks. Based on the collected studies, privacy and system attacks are the main concerns as regards to malware and phishing that have come to online advertisements. With the literatures gathered by the proponents, they serve as guide on how the proposed system will be conducted and take action on the concern of online ads as well as generate ideas through the configuration process.

3. Methods

3.1 Creating a DNS resolver

Pi-Hole was used as the DNS sinkhole for the network. A DNS sinkhole is used to protect and filter devices from unwanted content found on websites without the use of client-side software such as browser extensions. A standard DNS request happens when a DNS client issues a DNS request while providing a hostname and the DNS server will receive it. The DNS resolver on the other hand will provide the IP address for the provided hostname. This also includes requesting URLs for the advertisements; the catch is that configuring Pi-Hole manually that is containing a blacklisted domain or URL will respond to the client that the IP address that was requested is not existing. It will send an unspecified IP address as if that IP address does not exist; thus, it blocks the advertisement. Figure 1 provides the process of a client's requests for an IP address.

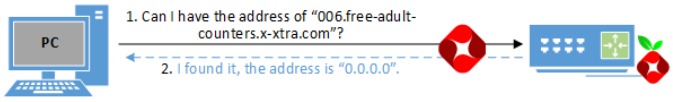

Figure 1. DNS Request

3.2 Configuration of the proposed system

The standard Pi-Hole was identified as to how its configuration uses default caching forwarding DNS. Requests are forwarded to an assigned DNS provider or a 3rd party DNS provider. It is not ensured that these providers are private and secured. If a single DNS server is poisoned, multiple users can be affected. The proponents have applied tweaking into the configuration by applying a local recursive DNS server. Using recursive DNS will reduce the chance of visiting malicious websites and will encrypt DNS traffic. Figures 2 and 3 show a Forwarding DNS server response and a Poisoned DNS provider response

Figure 2. Forwarding DNS response

Figure 3. Poisoned DNS provider response

3.2 Network Diagram

The Network Diagram is the overview of the existing network design of the establishment. It provides the existing devices that are being used inside the establishment as shown in Figure 4.

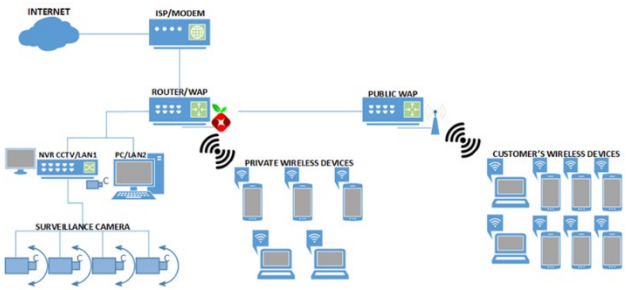

Figure 4. Network Diagram/Design

3.4 Waterfall model

The waterfall model is a step-by-step process methodology. It allows the proponents to work on a phase before moving to the next one. This model was selected because each of the phases have been completed one at a time and will undergo proper processing before proceeding. This model is somehow similar to the top-down approach though each face will not be divided into sub phases or sub modules. The process can be slow but it will allow each of the phases to be completed properly. The model is divided into 5 phases: Requirements, Design, Implementation, Verification, and Maintenance as shown in Figure 5.

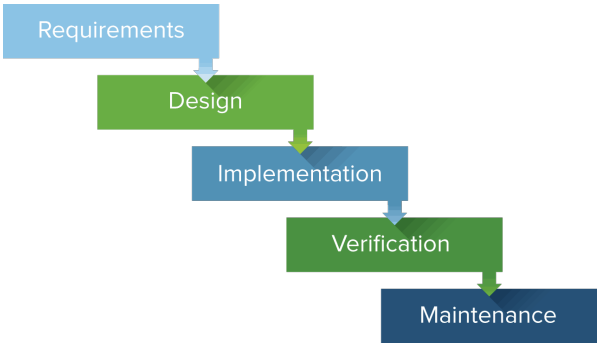

Figure 5. Waterfall model

Requirements

In this phase, the planning and designing of a solution that will eliminate online advertisements was done. The proponents have brainstormed on what materials will be used such as the device required and applications that will be used for the configuration process. Researching is also part of this phase as it provides ideas.

Design

In this phase, the proponents created a design on how the proposed system will be implemented as well the flow of its functionality. Gathering of the devices that is present in the establishment will be included in this phase as they will be used for configuring and testing.

Implementation

The actual installation and configuration were done in this phase. The activities that will be performed include assembly of the Raspberry Pi, installing the operating system to be used and configured using Pi-Hole as well the application of tweaking and improvement on the listing.

Verification

After the installation and the configuration, testing will be done during this phase. This is to ensure that the adblocking system is working on the devices connected into the network. Testing of blocked websites or domains will be done to see if they are still accessible or fully blocked.

Maintenance

This is the final phase wherein the whole configuration and testing have been executed. Further updates to the Raspberry Pi and to the listing configuration must be applied in order for the system to maintain its functionality. Updating can also help increase the security of the Raspberry Pi.

4. Results and Discussion

4.1 Project Description

The objective of the study was to incorporate a Network Adblocker that will protect the devices from malicious domains and trackers. The study serves a protection to the devices that are using the DNS server and interactions between the client and server. One of the elements of the system is the Raspberry Pi Zero W.

The researchers implemented a Network Adblocker that will block online advertisements at a DNS level and to protect devices that are connected to a network from malicious domains and trackers. This would protect the devices using the DNS server and interactions between the client and server.

This study included a Pi-Hole as a DNS sinkhole for the network. On the other hand, the DNS resolver will give the IP address the given hostname. This also applies to requesting URLs for the advertising, with the exception that manually establishing Pi-Hole with a blacklisted domain or URL will inform the client that the requested IP address does not exist.

4.2 Development of the System

Hardware and Software Requirements for Development

Raspberry Pi

The Raspberry pi is a small board computer that has been developed from the United Kingdom. It is a good device for cybersecurity and networking projects. The Raspberry Pi runs on the Linux operating system which is known for having a tight system. There are many variants for the Raspberry Pi and for this study, the proponents have used the Raspberry Pi Zero W.

Pi-Hole

Pi-Hole is a an open-source network-level advertisement blocker which will be applied on the Raspberry Pi for configuration. Upon setting Pi-Hole within the device, it will now serve as the network's DNS sinkhole and personal DNS server. The proponents will be implementing domains and trackers that will be blocked on the establishment's network.

Unbound

Unbound is a caching DNS resolver which will be configured on the Raspberry Pi. Instead of using 3rd party DNS servers, client devices will now communicate with authoritative servers. It will also provide encryption and avoid unnecessary traffic within the establishments network.

4.4.2 Testing

I. Adblocking test

Two websites where tested to see if banner advertisements where blocked. The speedtest.net by Ookla and a Pihole ad tester site where selected to see the system's adblocking function. Figure 6 shows comparison of the two websites running with and without the system.

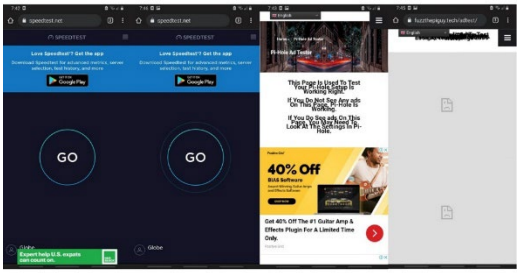

Figure 6. Websites showing blocked ads

II. Cron

The system has been enhanced by making it an automated system. The purpose of using Cron is that the users will no longer need to manually update the system to add the unnecessary domains that are affecting their network to be blocked. Cron has been configured to automatically update the domain list to be added within the system.

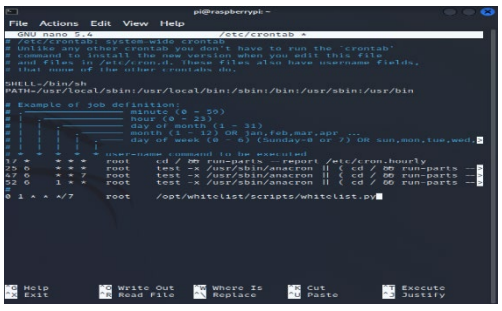

Figure 7. Crontab running on SSH

III. Blocklist

Figure 8 shows the blocklist contains websites that are handling unwanted content that are found within the internet. The Raspberry pi is connected to a repository where the list of domains is being updated and will automatically be integrated within the device so it continues to block more unwanted content such as malware sites, phishing and others websites that are not be accessed.

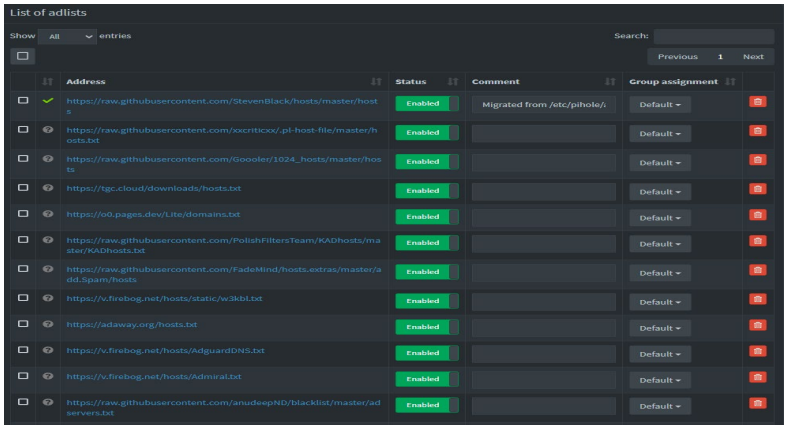

Figure 8. Blocklist

4.3 Implementation Plan

Hardware and Software Requirements for Implementation

Router

The Raspberry Pi will be plugged into the establishment's main router. The main router's provided DNS server will be changed and set the Raspberry Pi's IP address as its new DNS server. The system's function will now work on a network-level.

Client devices

The system's functionality will be applied on client devices such as mobile phones and personal computers. Since these devices are connected to the establishment's network, they will now be protected against unnecessary traffic and advertisements as well as unwanted sites will be blocked.

Web browsers

The web browser can be used access the system's provided dashboard so clients can view the activities that are happening within the system. Since the network is protected from unwanted advertisements and domains, the clients can have a safe browsing experience.

Deployment plan

The proponents have designed the establishment's current network setup. The Raspberry Pi will be connected on the main router. Devices connected within the system will be tested for the system's functionality. Several websites with advertisements will be accessed to try and see if they are blocked.

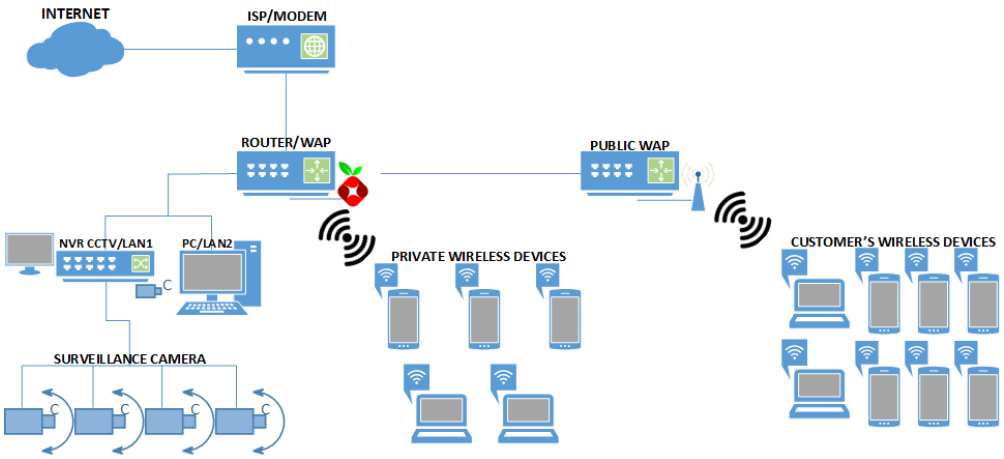

Figure 9. Network setup of the establishment with the system's integration

Training

The proponents provided a summary of the study to the staff and oriented them on the threats of online advertising. Selected users will use their mobile phones to test the adblocking function of the system and introduce them to the dashboard. The proponents have provided a walkthrough how they can monitor the system and instruct them on how to use it manually especially on blocking domains or websites. The proponents will provide a survey for the system's evaluation.

4.4 Statistical Evaluation

The system was evaluated using Google Form and it was deployed to the staff of the establishment as well as additional users. A walkthrough was provided first before giving the survey. The evaluation has 4 criteria: System Functionality, System Reliability, System Security and System Overall Performance. The weighted mean of each survey has been calculated.

Criterion I: System Functionality

Figure 10 shows the satisfaction of the respondents on the system functionality where 11 have answered "Very satisfied" while 3 have answered "Satisfied". This criterion has a weighted mean of 4.8. The respondents are very satisfied with system's functionality.

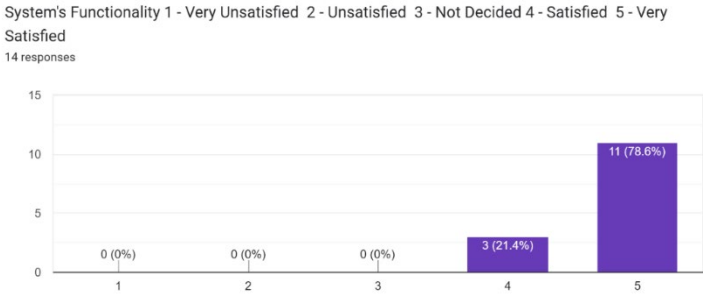

Figure 10. System Functionality

Criterion II: System Reliability

In Figure 10, 11 have answered "Very satisfied" while 2 have answered "Satisfied". This criterion has a weighted mean of 4.9. The evaluators are very satisfied with system's reliability.

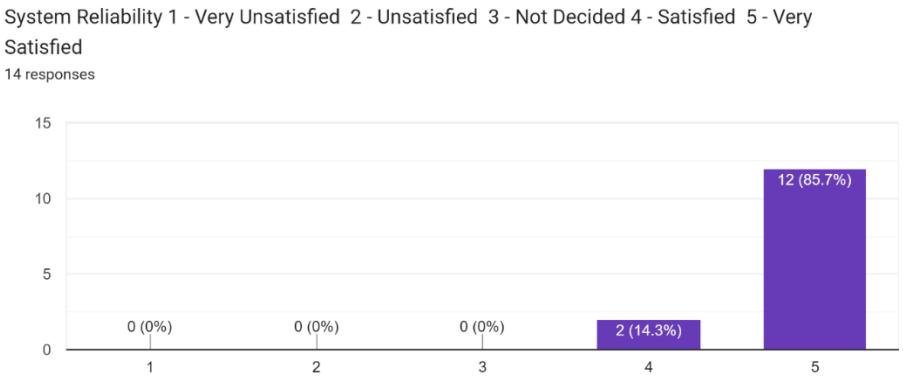

Figure 11. System Reliability

Criterion III: System Security

In this criterion as shown in Figure 12, 12 have answered "Very satisfied" while 2 have answered "Satisfied". This criterion has a weighted mean of 4.9. The evaluators are very satisfied in regards to the security of the system.

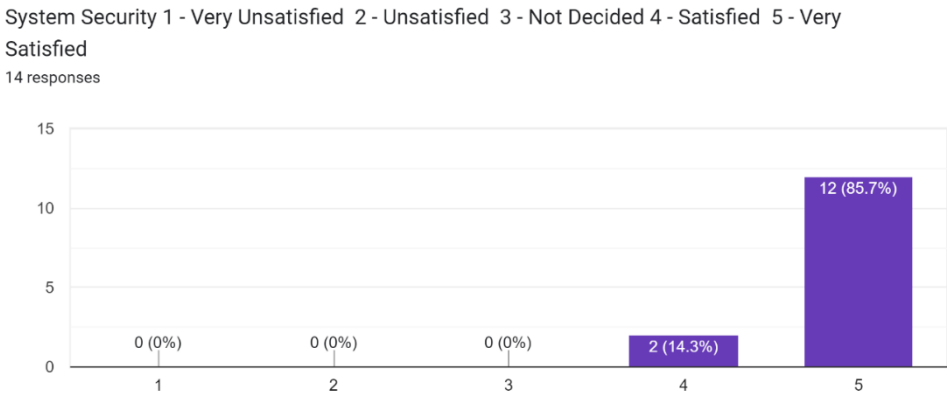

Figure 12. System Security

Criterion IV: System Overall Performance

In this criterion, 12 have answered "Very satisfied" while 2 have answered "Satisfied". This criterion has a weighted mean of 4.9. The system's overall weighted mean is 4.9. The overall performance of the system was found to be very satisfying as presented in Figure 13.

The general weighted mean of this survey is 4.875. The evaluators find that the system overall is very satisfying.

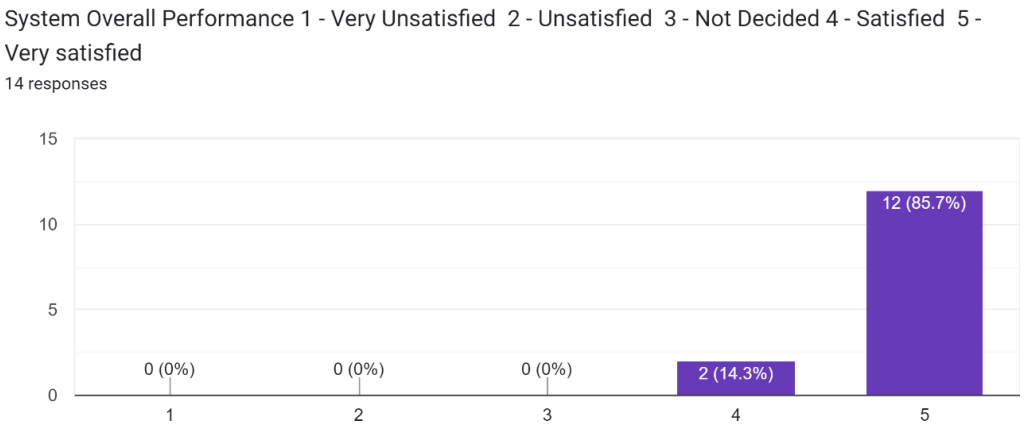

Figure 13. System Overall Performance

5. Conclusion

Network Security is an important feature to be considered today. The proponents and at the same time the users of the internet know that it is a duty to be vigilant against attackers within network. Cybersecurity is not something to be overlooked, it can somehow be challenging to manage but it will ensure that no entities will be able to infiltrate any system.

The goal of this study was to be able to prevent unwanted contents to be accessed by a user and deliver a safe networking environment. It is quite difficult to assume whether a site is safe to visit or not. It is not advised to believe on anything that we see in the internet, whether it is in a form of a post, a message or even an advertisement that will try to persuade anyone into looking through it. It is better to protect important information that a user possesses from being stolen by attackers. The Raspberry Pi is a small computer device yet there are countless of possible projects can be developed using this device especially in regards to security.

Throughout the whole process of this study, challenges were endured during its development and took time to apply all the necessary configurations to ensure that it will use its full potential. Though some issues cannot be addressed, the system was still able to provide its importance and through evaluation, it was found to be very useful to the clients and will be able to provide safety for their network.

References

Al-Turjman, F., & Salama, R. Chapter 3 - Cyber sealcurity in mobile social networks. In F. Al-Turjman & B. D. Deebak (Eds.), Security in IoT Social Networks, pp. 55–81, 2021. Academic Press. Available: https://doi.org/https://doi.org/10.1016/B978-0-12-821599-9.00003-0, 2021.

Blocking Unnecessary Advertising Web Content. Available: https://ncsc.gov.uk/blog-post/ill-make-you-offer-you-cant-refuse, 2017.

Digintrude., Malware and its impact on business. Available: https://www.digintrude.com/malwares-and-its-impact-on-business.html, 2017.

Geary, S. Malware, phishing, spyware and viruses – what's the difference?, August 2017.

Ha, L. Online Advertising Research in Advertising Journals: A Review. Journal of Current Issues & Research in Advertising, vol. 30, 2021. Available: https://doi.org/10.1080/10641734.2008.10505236, 2021.

Johnston, S. J., & Cox, S. J. The Raspberry Pi: A Technology Disrupter, and the Enabler of Dreams. Electronics, vol. 6, no. 3, 2017. Available: https://doi.org/10.3390/electronics6030051, 2017.

Kadav, A., Madhavi, S., Gorivale, T., & Maheta, V. Ad-Blocking with AdGuard Network wide Ad-Blocking with Raspberry Pi, vol. 8, 2021. Available: www.jetir.org, 2021.

Karageorgos, A., & Zhang, M., The motivations of Internet users to avoid online advertisements by employing ad blocking extensions: An exploratory quantitative research, May 2018.

Mary, L., Dheen, S. N., & Narayanan, S. K. Network-wide range ad-blocker using Raspberry Pi. *International Journal of Pure and Applied Mathematics,* vol. 119, pp. 1771-1775, 2018.

Nayyar, A., & Puri, V. Raspberry Pi-A Small, Powerful, Cost Effective and Efficient Form Factor Computer: A Review, vol. 5, 2015. https://www.researchgate.net/publication/305668622, 2015.

Taib, A. M. Securing Network Using Raspberry Pi by Implementing VPN, Pi-Hole, and IPS (VPiSec). *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 1-3, pp. 457–464, 2020.

Biographies

John Ezekiel C. Dunglao is a driven IT student from the Philippines, born and raised in the province of Pampanga. From a young age, he was fascinated by technology and the role it played in the world. His parents noticed his passion for computers and encouraged him to pursue his interests. A student from Angeles University Foundation who is willing to learn and acquire new skills in the field of technology. He has been a fond of technology and computer games since his younger years and it was the reason why he took IT in college. He always read articles regarding the latest trends in technology to keep himself updated. He has provided support to my family and friends whenever they seek my assistance regarding technology. As a student, He has learned different fields such as cloud computing and networking. He is willing to gain new experiences and be committed in the IT industry.

Sean Deniel Agustin is a dedicated student currently pursuing a Bachelor of Science in Information Technology at AUF. Throughout his academic career, Sean has developed a passion for tackling IT infrastructure challenges, which has become a driving force in his studies and career goals. One of Sean's greatest strengths lies in his excellent interpersonal skills, which enable him to communicate and network effectively with colleagues, clients, and other professionals in the IT industry. This skillset allows him to build strong relationships and partnerships that facilitate

successful project outcomes. Sean is also highly skilled in networking, cloud computing, troubleshooting, Cisco, and cybersecurity. His expertise in these areas allows him to identify and resolve IT issues quickly and efficiently, ensuring that systems remain secure, reliable, and functional. Overall, Sean is a talented and motivated individual with a strong focus on IT infrastructure and a keen eye for detail. His excellent interpersonal skills, combined with his technical expertise, make him a valuable asset to any IT team or organization.

Jay G. Tanglao Jr. is a young and ambitious individual with a passion for learning and making a positive impact in the world. Born and raised in Mabalacat City, Pampanga, Philippines. Jay spent his early years exploring the world around him and developing a keen interest in science, technology, and innovation. Jay is currently taking BS Information Technology Major in Networking at Angeles University Foundation and currently attending his OJT. In 2021, he became the Vice President for External Affairs in JPCS Organization in their university. He is interested in troubleshooting, learning more about Microsoft Azure, Cloud Architecting, Linux, Python.

Vraelle R. Velarde is a driven and passionate 4th year Information Technology major at Angeles University foundation with a particular interest in IT infrastructure. He is currently an intern at Cloudstaff and has excelled in his studies while gaining practical experience. Vraelle is recognized for his strong work ethic, attention to detail, and commitment to quality. He plans to use his knowledge and skills to build and maintain robust and secure IT systems for organizations in the future.

Ray A. Nicolas is a professor from Angeles University Foundation. He is a faculty from the college of computer studies. As a professor, his lessons focused on Information Assurance and Security, which tackles the practice of assuring information and managing risks. He also discussed cybersecurity and its threats such as malware and ransomware to help his students gain knowledge in regards to security. As an adviser, he guides his advisory students in addressing their errors within their study for them to lessen the chance of finding any holes from their projects.