Virtual Private Network (VPN) Router using Raspberry-PI

Shwetha N[1], Raghu J[2], Sahas V G[3], Mujahid Khan[4], Siddesh G M[5] and Vinay H N[6]
[1]Department of ECE, Dr. Ambedkar Institute of Technology, Bangalore, INDIA
[2]Department of ECE, NIE, Mysore, INDIA
[3]Department of ECE, Dr. Ambedkar Institute of Technology, Bangalore, INDIA
[4]Department of ECE, Dr. Ambedkar Institute of Technology, Bangalore, INDIA
[5]Department of ECE, Dr. Ambedkar Institute of Technology, Bangalore, INDIA
[6]Department of ECE, Dr. Ambedkar Institute of Technology, Bangalore, INDIA

[1]Corresponding Author: shwethaec48@gmail.com

Received: 28-05-2023 Revised: 14-06-2023 Accepted: 29-06-2023

ABSTRACT

This research paper investigates the implementation of a VPN router the use of a Raspberry Pi, a cost-effective and flexible single-board pc, with a number one recognition on security concerns. The observe explores the feasibility and overall performance of utilizing the Raspberry Pi as a VPN router, supplyinga sensible answer for people and small-scale agencies in search of stable and private internet connectivity. The paper outlines the research method, along with hardware requirements, software configurations, and experimentalsetup. Throughout the examiner, strong security measures are emphasized, addressing capability vulnerabilities and providing measures to beautify the security of the Raspberry Pi-based totally VPN router. The performance of the Raspberry Pi as a VPN router isevaluated via rigorous testing, evaluating it to present business solutions. The findings contribute to the expertise of secure VPN router implementations and highlight the Raspberry Pi's capability for value- powerful and customizable network protection answers, empowering customers to shield their internet communications and defend sensitive information.

***Keywords*--** Raspberry PI, Private Network, Data Protection, Sensitive Data, Secure Internet Connectivity, OpenVPN

I. INTRODUCTION

Nowadays, public wireless network (Wi- Fi) is rapidly increasing due to the demand of free wireless services. This free Wi-Fi service is available in most public places such as restaurants, hotels, cafes, and airports. However, free Wi-Fi services normally implement lower security measures which use weak encryption and authentication that produce increased risk of attacks for intercepting data. Although 68.02% of Wi-Fi hotspots use WPA2 which is better in terms of security, they are still vulnerable to brute-force and dictionary attacks. Recently, WPA2encryption was found to have a severe flaw that allows attackers perform Key Reinstallation Attack to break the encryption.

When users are connected to the public Wi- Fi, it is difficult to validate correctness of access pointsand they may be connected to spoofed access points. This can occur if an Evil Twin AP is maliciously placed. As a result, the attacker(s) can do various Man- in-the-Middle (MITM) attacks including eavesdropping, falsification of contents, presenting fake log-on pages for identity theft purposes, and carrying out active attacks on users' devices. With the availability and ability of wireless attacking tools such as network scanners, attackers care able to find the most vulnerable wireless networks and plan an attack that can affect a large number of users. One of the popular network scanners, Vistumbler has the functionality to detect and extract information from access points such as SSID, authentication mode, encryption, network type, router manufacturer, and signal strength. This information will help attackers tolaunch the attack.

In effort to solve this problem, VPN is used when browsing on public Wi-Fi. The essence of VPNis to build a secure tunnel in the public network using relevant encryption technology. Thus, the data transmission is secure and protected from being sniffed. This research paper provides valuable insights into cost-effective and customizable network security solutions. The findings will equip individuals and small-scale businesses with the knowledge and practical guidance needed to establish their own VPN routers, enhancing their ability to safeguard sensitive data and protect their online activities.

II. LITERATURE REVIEW

Virtual Private Network

VPN is a service which provides secure webaccess by privately routing your connection through a VPN server and hiding the client's online actions. TheVPN software will encrypt the data, even before an Internet Service Provider

(ISP) or the public Wi-Fi provider sees it. The data then goes to the VPN, and from the VPN server to the client's online destination.There are four core technologies in VPN which are tunneling, encryption, identity authentication and key exchange management. VPN protocols define how the service handles data transmission over a VPN. The most common protocols are Point-To-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol , Secure Socket Tunneling Protocol , Internet Key Exchange, Version 2, and OpenVPN . OpenVPN takes the best in the above protocols and does away with most of the flaws. It is based on SSL/TLS protocol, and is an open- source project, which means that it is constantly being improved by hundreds of developers (Aung & Thein, 2020). It secures the connection by using keys that are known only by the two participating parties on either end of the transmission.

Taib et al. (2020) implemented a VPN with Pi-Hole and Intrusion Prevention System (IPS) using Raspberry Pi to secure the network. The researchers named the project VPiSec where the system was developed using OpenVPN protocol and Pi-Hole application to block any known tracking Domain Name System (DNS) and advertising domain. This project also implemented Intrusion Prevention System (IPS) to prevent the brute force attack. The network performance had no significant difference while the users were connected to the VPN.

Taib et al. (2020) also developed an integrated tool that implemented OpenVPN protocol, DNS blocker and Intrusion Detection System (IDS) known as NetGuard. The researchers used Raspberry Pi to develop the system. OpenVPN was used as the protocol to provide the security and encryption for the network traffic while DNS blocker prevented unwanted advertisements. The researchers provided data that confirmed that the respondents were satisfied with the network performance and security during their connections using this system.

Pooja, Akansha, and Anurag (2018) developed their project Secure VPN Server deployed on Raspberry Pi. They conducted their research on public Wi-Fi security and concluded that users who used public Wi-Fi risk their privacy being intruded by unauthorized individuals. In accordance with the problem stated above, the researchers decided to implement a VPN Server into the Raspberry Pi. The project established the connection between VPN Server on Raspberry Pi and VPN client to provide multiple layers of protections. Once VPN session was established, the researchers implemented VPN authentication mechanism by incorporating three layers of verification. Finally, the project aimed at portability, is fully deployed on a Raspberry Pi environment. This enables the system to become extremely portable, reusable and user friendly.

III. METHODOLOGY

Design Phase

The design phase includes the use of a scenario for the situation of the problem and the solution for the scenario. After that, an illustration diagram was used to illustrate the design of the system architecture. Figure 1 shows the graphical scenario of securing network connection using Raspberry Pi.

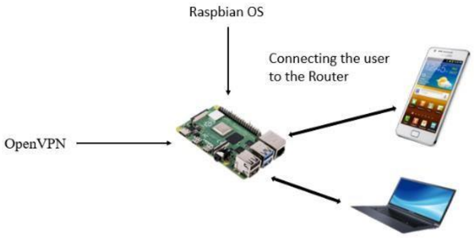


Figure 1: Graphical Scenario

An architecture system is a conceptual model that defines the structure, behavior and explains more view of a system. It is a formal description and representation of a system, organize in a way that supports reasoning about the structures and behaviors of the system. A system architecture can comprise system components, the expand systems developed, the connection between the systems and other components that will work together to implement the overall system.

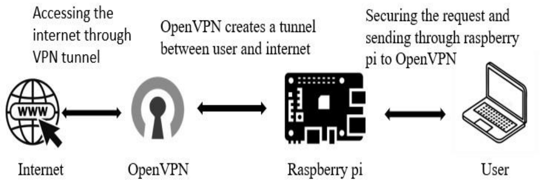

Accessing the internet through VPN tunnel
OpenVPN creates a tunnel between user and internet
Securing the request and sending through raspberry pi to OpenVPN
WWW
Internet
OpenVPN
Raspberry pi
User

Figure 2: System Architecture

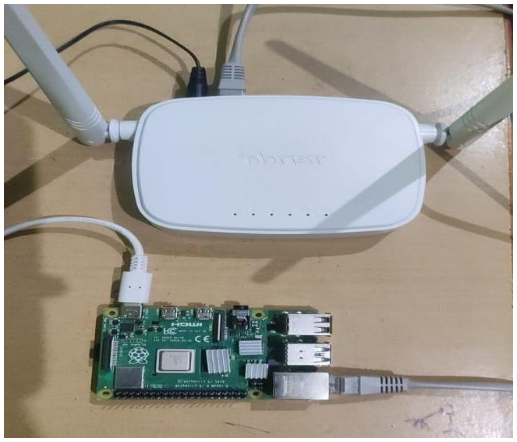


Figure 3: Hardware Setup

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.29

Setting up OpenVPN into Raspberry pi

Setting up OpenVPN on a Raspberry Pi permits for the advent of a stable and personal virtual personal community (VPN) within a home or small- scale network. OpenVPN is an open-source VPN protocol recognized for its robust safety and flexibility. The technique of putting in OpenVPN on aRaspberry Pi involves numerous steps. First, ensure that the Raspberry Pi is walking the ultra-modern model of the Raspbian working device. Install the OpenVPN software program bundle and generate cryptographic certificates and keys for the VPN server and consumer. Configure the OpenVPN server through enhancing the server configuration report, specifying network settings, encryption parameters, and consumer authentication techniques. Next, create purchaser configuration documents, including the important certificates and keys, and distribute them tothe gadgets to be able to connect with the VPN. Finally, begin the OpenVPN carrier at the Raspberry Pi, and join the customer devices to the VPN server the usage of the supplied configuration documents. With OpenVPN efficaciously set up on a Raspberry Pi, users can securely get right of entry to their domestic network remotely or browse the internet even as cashing in on the added privacy and encryption furnished by the VPN.

Implementation of OpenVPN

Implementing OpenVPN on a Raspberry Pi includes several steps to establish a stable and personal virtual personal network (VPN) connection. First, ensure that the Raspberry Pi is walking the latest model of the operating system, which include Raspbian. Install the OpenVPN software program bundle the use of the package deal manager, with a view to include the essential components for growingand managing VPN connections.

Next, generate cryptographic certificates and keys for the VPN server and client. This involves the usage of the OpenVPN Easy-RSA application to create a public key infrastructure (PKI) and generate the necessary certificates, inclusive of the server certificate and customer certificates. The certificates and keys make sure stable verbal exchange between the server and customers.

After producing the certificates and keys,configure the OpenVPN server. This includes modifying the server configuration report to specify community settings, encryption parameters, and user authentication methods. The configuration report permits customization of the VPN settings primarily based on particular desires, along with defining the VPN subnet, enabling routing, and specifying DNS servers.

Once the server configuration is ready, createpatron configuration files for every tool so that it will hook up with the VPN. The client configuration files will consist of the vital certificate and keys for authentication. Distribute these files securely to the respective customer gadgets, ensuring the confidentiality of the certificates.

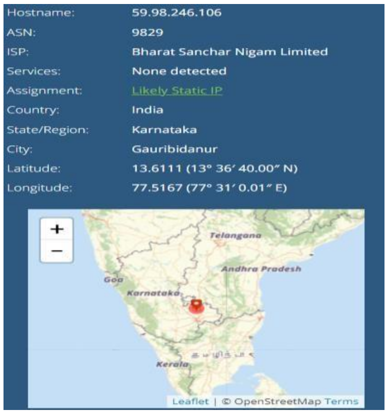
Finally, begin the OpenVPN service on the Raspberry Pi to activate the VPN server. This may be finished the usage of the correct command or provider management tool. The client devices can then connectto the VPN server the usage of the furnished configuration files and set up a secure and encrypted connection. With OpenVPN successfully implemented on a Raspberry Pi, customers can experience secure faraway access to their domestic community or browse the net with greater privacy and encryption furnished by means of the VPN. The implementation method ensures a strong and dependable VPN answer for protecting sensitive statistics and maintaining on line privateness.

IV. TESTING AND ANALYSIS

OpenVPN Anonymity

IP Address and Location Leak Test

The first part of this testing is by using the tool with an existing internet connection without using OpenVPN. Figure 3 shows the result of the testing that indicates the user's IP address location is exposed. This exposure allows the attacker to trace the user's current location.

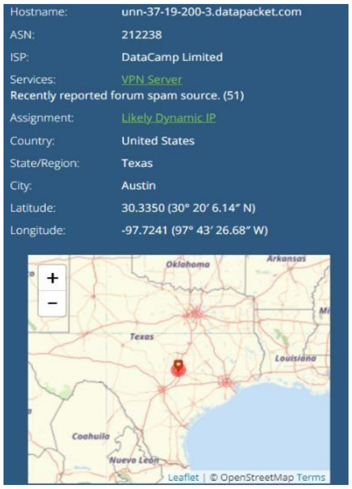


Hostname:	59.98.246.106
ASN:	9829
ISP:	Bharat Sanchar Nigam Limited
Services:	None detected
Assignment:	Likely Static IP
Country:	India
State/Region:	Karnataka
City:	Gauribidanur
Latitude:	13.6111 (13° 36′ 40.00″ N)
Longitude:	77.5167 (77° 31′ 0.01″ E)

Figure 4: IP Address and Location Leak Test without VPN

The second part is using the tool after connecting to the implemented OpenVPN. The result as in Figure 4 shows that the ISP of the network has been replaced from Celcom to Digital Ocean which is the VPS used for the OpenVPN. Besides, the IP address has also been replaced with the IP address of the OpenVPN server which is also the IP address of the cloud server. In the tool display, it stated that the IP address is exposed, but it is the IP address given by Digital Ocean. The VPN hides the user and even the tool cannot detect if the user hides his/her IP with a VPN or not.

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.29

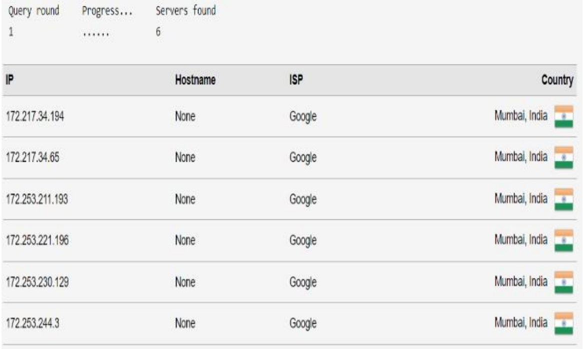


Hostname: unn-37-19-200-3.datapacket.com
ASN: 212238
ISP: DataCamp Limited
Services: VPN Server
Recently reported forum spam source. (51)
Assignment: Likely Dynamic IP
Country: United States
State/Region: Texas
City: Austin
Latitude: 30.3350 (30° 20′ 6.14″ N)
Longitude: -97.7241 (97° 43′ 26.68″ W)

Figure 5: IP Address and Location Leak Test with VPN

DNS Leak Test

In the beginning, the DNS leak test was tried on the network that is not connected to the VPN. Figure 5 shows the result of the DNS leak test which displays the DNS requests exposed. That means all the DNS requests made by the user while browsing the internet are possibly exposed to the ISP. ISP can track users’ browsing and all the sensitive data sent and received. Besides, if there is a MITM attack to the ISP’s DNS server, the attacker may also gain the users’ sensitive data.

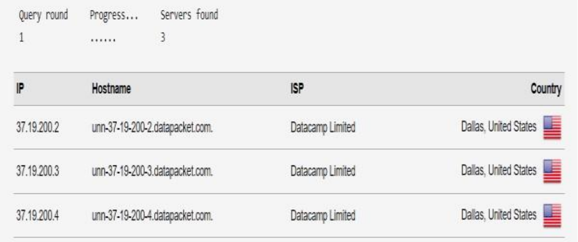


Query round	Progress...	Servers found
1	......	6

IP	Hostname	ISP	Country
172.217.34.194	None	Google	Mumbai, India
172.217.34.65	None	Google	Mumbai, India
172.253.211.193	None	Google	Mumbai, India
172.253.221.196	None	Google	Mumbai, India
172.253.230.129	None	Google	Mumbai, India
172.253.244.3	None	Google	Mumbai, India

Figure 6: DNS Leak Test without VPN

Then, the test was conducted again after connecting the network to the VPN. The result in Figure 6 shows that the DNS provider has changed from the original ISP to Google and two DNS providers’ addresses are leaked. The tool states that the DNS request is exposed because it does not know that the network has already being implemented and connected to the VPN to prevent DNS requests from being monitored and captured by ISP.



Query round	Progress...	Servers found
1	......	3

IP	Hostname	ISP	Country
37.19.200.2	unn-37-19-200-2.datapacket.com.	Datacamp Limited	Dallas, United States
37.19.200.3	unn-37-19-200-3.datapacket.com.	Datacamp Limited	Dallas, United States
37.19.200.4	unn-37-19-200-4.datapacket.com.	Datacamp Limited	Dallas, United States

Figure 7: DNS Leak Test with VPN

V. CONCLUSION

In end, the deployment of a VPN router the usage of a Raspberry Pi presents a cost- effective and adaptable approach to bolstering community safety and maintaining privateness. By channeling all community site visitors via a VPN, the Raspberry Pi permits the encryption of facts, thereby fortifying it towards potential threats and unauthorized get admission to. While the performance of this answer may exhibit variability, it generally proves suitable for domestic or small-scale workplace environments. This do-it-yourself assignment empowers users with community manage, ensures compatibility across quite a number gadgets, and offers a stimulating possibility to accumulate understanding about networking and security. However, it is of paramount importance to meticulously pick out a good VPN company and diligently keep ordinary software program updates to maximize the security blessings derived from this setup.

REFERENCES

[1] M. A. Elsadig, A. Altigani & M. A. Ali Baraka. (2019). Security issues and challenges on wireless sensor networks. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(4), 1551–1559.

[2] D. Rani & N. S. Gill. (2019). Lightweight security protocols for the internet of things: a review. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(3), 707–719.

[3] V. Osamor, O. Emebo, B. Fori & M. Adewale. (2019). Engineering and deploying a cheap recognition security system on a raspberry pi platform for a rural settlement. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(6), 2904-2909.

[4] P. Garms & S. MurphySep. (2018). Consider data security. *Security Today*. Available at: https://securitytoday.com/articles/2018/09/01/consider-data-security.aspx?admgarea=ht.networkcentric.

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://doi.org/10.31033/ijemr.13.3.29

[Accessed:14-Apr-2019].

[5] F.M. Rustono, D.G.S Achmad, D. Agus, S. Wa Ode, P.M. Alfred. Information Security Risk and Management in Organizational Network. International *Journal of Engineering and Advanced Technology (IJEAT).* Volume-8 Issue-6S2, August 2019.

[6] A. Mat Taib, M. Tholhah Zabri, N. A. Mohd Razi, E. Abdul Kadir. "NetGuard; Securing Network Environment using Integrated OpenVPN,-Pi-Hole, and IDS on Raspberry Pi. International Conference on the future of ASEAN. 2019.

[7] S. Taylor, VPN Ad Blockers - The Best and the Worst," Restore Privacy, 20-Sep-2019. [Online]. Available: https://restoreprivacy.com/vpn-ad-blocker-comparison/. [Accessed: 27-Mar-2019].

[8] A. A. Amjad and N. H. O. Hebah, Intrusion Prevention System, vol. 3, no. 1, pp. 432–434, Jan. 2011.

[9] H. Tasmi, D. Setiawan, D. Stiawan, S. Husnawati, Analar Valiata. Determining Attributes of Encrypted Data Traffic Using Feature Selection Method. *International Journal of Engineering and Advanced Technology (IJEAT)*. Volume-9, Issue-1, October 2019.

[10] S. Wilkins, *Basic Intrusion Prevention System (IPS) Concepts and Configuration, Cisco Press, 29- Jun-2011. [Online]*. Available: http://www.ciscopress.com/articles/article.asp?p=1722 559. [Accessed: 15-Apr-2019].

[11] N. Shwetha, L. Niranjan, V. Chidanandan and N. Sangeetha, "Advance System for Driving Assistance Using Arduino and Proteus Design Tool," *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, Tirunelveli, India, 2021, pp. 1214-1219, doi: 10.1109/ICICV50876.2021.9388620.

[12] S. N, N. L, G. N, S. Jahagirdar, S. A. R and S. N, "Efficient Usage of water for smart irrigation system using Arduino and Proteus design tool," *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, 2021, pp. 54-61, doi: 10.1109/ICOSEC51865.2021.9591709.

[13] N. Shwetha and M. Priyatham, "Performance Analysis of Self Adaptive Equalizers using EPLMS Algorithm," *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2020, pp. 872-876, doi: 10.1109/I-SMAC49090.2020.9243512.

[14] Shwetha, N., Niranjan, L., Chidanandan, V. & Sangeetha, N. (2021), Smart driving assistance using Arduino and proteus design tool. Expert Clouds and Applications, 647–663.

[15] R. Taseen, H. Yaseen, N. L, G. Radha, M. B. Neelagar and S. N, "An Innovative Method for Energy Intensive Routing and Transmission Network Positioning in Integrated Wireless Detector Networks," *2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC)*, Mysore, India, 2023, pp. 1-7, doi: 10.1109/ICRTEC56977.2023.10111924.

[16] Shwetha, N., Gangadhar, N., Neelagar, M.B., Shilpa, K.C. (2022). ANN-based Hybridization Approach for Detection of Cardiac Disease. In: Shakya, S., Balas, V.E., Kamolphiwong, S., Du, KL. (eds) Sentimental Analysis and Deep Learning. Advances in Intelligent Systems and Computing, vol 1408. Springer, Singapore. https://doi.org/10.1007/978-981-16-5157-1_20.

[17] Shwetha, N., Manoj Priyatham, and N. Gangadhar. "Adaptive Channel Equalization Using Seagull Optimization with Various Initialization Strategies." *J. Commun.* 17, no. 4 (2022): 302-307.

[18] Shwetha, N., Priyatham, M. (2021). Performance Analysis of Self Adaptive Equalizers Using Nature Inspired Algorithm. In: Smys, S., Balas, V.E., Kamel, K.A., Lafata, P. (eds) Inventive Computation and Information Technologies. Lecture Notes in Networks and Systems, vol 173. Springer, Singapore. https://doi.org/10.1007/978-981-33-4305-4_37.

[19] Shwetha, N., Priyatham, M. (2021). Convergence Analysis of Self-Adaptive Equalizers Using Evolutionary Programming (EP) and Least Mean Square (LMS). In: Bindhu, V., Tavares, J.M.R.S., Boulogeorgos, AA.A., Vuppalapati, C. (eds) International Conference on Communication, Computing and Electronics Systems. Lecture Notes in Electrical Engineering, vol 733. Springer, Singapore. https://doi.org/10.1007/978-981-33-4909-4_48.

[20] H. Tabassum, N. L, S. P. Atti, A. Pasha, N. Shwetha and M. B. Neelagar, "A Fiber-Wireless Monitoring System with a QoE Instrument for Smart Grid Technology," *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2023, pp. 404-410, doi: 10.1109/ICEARS56392.2023.10085662.

[21] Shwetha, N., Priyatham, M., & Gangadhar, N. (2021). Adaptive filter equalizer optimization using hybrid approach. International Journal of Advanced Research in Engineering and Technology, 12(1), 473–483.