Journal of Computing Research and Innovation (JCRINN) Vol. 6 No. 2 (2021) (pp29-40)
https://jcrinn.com : eISSN: 2600-8793

Enhancing Security and Privacy in Local Area Network (LAN) with TORVPN Using Raspberry Pi as Access Point: A Design and Implementation

Mohd Nizam Osman[1*], Khairul Anwar Sedek[2], Nor Arzami Othman[3], Muhammad Afiqhakimi Rosli[4], Mushahadah Maghribi[5]
[1,2,3,4] Faculty of Computer and Mathematical Sciences
Universiti Teknologi MARA, Perlis Branch, Arau Campus, 02600 Arau, Perlis, Malaysia
[5]Politeknik Tuanku Syed Sirajuddin, 02600 Arau, Perlis, Malaysia

Corresponding author: [*]mohdnizam@uitm.edu.my
Received Date: 4 April 2021
Accepted Date: 29 June 2021
Published Date: 1 September 2021

HIGHLIGHTS

- The combination of TOR and VPN services was designed and implemented to enhance the security and privacy in LAN using Raspberry Pi as an access point.
- The graphical user interface application was developed to assist and facilitate the user to enter the network securely, without having the difficulties to configure and install any software.
- Two experiments involved in this study, which is confidentiality test and the Internet connectivity performance test with positive and encouraging results.
- The confidentiality of TorVPN access point network was also proved fully encrypted and secured.

ABSTRACT

Network security is designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Every person, including organization requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today. This paper aims to design and implement TorVPN as an access point using Raspberry Pi in enhancing security and privacy in Local Area Network (LAN). This access point was implemented by using the combination of The Onion Router (Tor) and Virtual Private Network (VPN) services. Then, the graphical user interface application was developed to assist and facilitate the user to access the network securely without having the difficulties to configure and install any software. To determine the effectiveness of the proposed work, there were two experiments involved in this study. Firstly, the confidentiality test which to verify its privacy in keeping the information securely. Secondly, the performance test of the Internet connectivity in terms of ping, download and upload speed. The encourage results was expected as the confidentiality tested on the TorVPN access point network has shown the positive outcome by securing client's Internet data packet. While, the Internet connectivity is not stable enough, when the client's IP

address changed in the network. Hence, the combination VPN and Tor service using Raspberry Pi as an access point inside the LAN is suitable and secure the information in the network, but do not suggest for user who wants a good Internet connectivity.

Keywords: *TOR, VPN, LAN, encryption, access point, raspberry PI*

INTRODUCTION

Security and privacy are very important in our life because its main objective is to provide a protection for a person, community, society and country against threats, especially in cyber security. There are many free tools, software and services provided by the developer for users to enhance and ensure the security protection over the Internet. For instances, the security and privacy protection services available nowadays are The Onion Router (Tor) and Virtual Private Network (VPN). The network security that is provided in Tor and VPN service will ensure the user's privacy, security, and data are protected from any data stealing over the Internet from the third-party person. VPN is a method to channel all or part of the network traffic with diverse middle node as a private network, and it serves interconnectivity to transfer information between different entities that belong to VPN (Younglove, 2000). Meanwhile, Tor is a network service which enables users to stay anonymous over the Internet and prevent from any possible surveillance, traffic analysis, location tracking and others by hiding the Internet traffic path (Phobos, 2010). According to Tiwari et al. (2015), Tor also serve a function that acts as a 'Black Box' which hides the routing information of connected users by offers a secrecy layer for TCP and becomes one of the most well-known anonymity tools over the Internet. Tor's users use this service by connecting through a serial of virtual tunnel rather than direct connection. Therefore, this will be allowed organization and individual to communicate and share information over public network without compromising their privacy. Besides, it also gets connected and passing the data packet with several servers out there randomly.

The Onion Router (Tor) service is one of the ways to surf out over the Internet without being worried too much about the Internet data theft and privacy of the information inside data packet. This service uses an Onion Routing technique to serve the encryption and anonymity for data packet that need to be send to the destination by bounce the data packet to several servers in another country, which located inside the Tor relay. According to Bian et al. (2021), based on their analysis, Tor service provide a good foundation for Tor hidden services content analysis. In terms of the algorithm, some researchers have proposed new algorithm such as Local Distance Neighbor (LDN) to improve the performance of Tor. Meanwhile, to protect the user's data packets inside Local Area Network (LAN), one layer of encryption was needed. Therefore, Virtual Private Network (VPN) was a suitable service which will ensure the encryption for data packet in LAN. Hence, the combination of Tor and VPN service was the best creation and method that needed for users to enhance its security and privacy inside LAN while surfing over the Internet. Unfortunately, the complexity of configuration or installation of hardware and software needed to provide a secure network using Tor and VPN services, it a quite trivial, difficult and challenging to the users, especially for regular users with no knowledge in network security.

Tor service's developer has developed a software application names "Tor Browser" in several platforms such as Windows, Linux, and Android. The software is free to use, and it has been used by 25 million users. The users who are to stay connected with this secured network need to download the software application from the Internet and install it on their computer or device accordingly. For most people who need a better anonymity not missed from installing a software and web browser that required to anonymize web traffic. There is another way to keep surfing anonymously by booting user's computer with a portable flash drive loaded with the Tor installation file and Linux operating system. Unfortunately, by having the Tor software on the personal computer can be mistrustful in itself and many users are not suggested to install the nonstandard software. In addition, it will be difficult for a normal operating system such as OS X or Windows to work with the Linux-based portable drive because of the file type used in Linux is different with OS X and Windows. Therefore, by implementing Tor software on Raspberry Pi that will act as a wireless access point will help users to easily get an anonymous connection and the most important thing is users do not need to install any anonymity software on their computer. Furthermore, this Tor access point may save user's time and every single user or client that is connected with this access point will automatically get connected with Tor network. Besides, Raspberry Pi is a well-known platform to support IoT technology and this electronic board is used for processing data and resources like a normal desktop computer (Sheik & Xinrong, 2014).

This paper focuses on the combination of Tor and VPN to enhance the security and privacy in Local Area Network (LAN) by using a Raspberry Pi as an access point. In general, an access point is a wireless device which will act as a gateway for user's devices to connect to a local network. Access points are used to extend the size of network for existing network and increase the number of users through a wireless. For this study, function of the access point will be used not only for extending the network capacity and accommodate a large number of users, but it is also to implement the VPN service with connected to Tor network inside the access point to ensure every user gets a better secure network connection. It will work in any type of network infrastructure either local, public and private network.

RELATED WORK

Onion Routing was originally a prototype by Sun Solaris 2.5.1/2.6 with implementations for web browsing, remote login, and sanitizing user information while transmitting information through data streams. The further research and implementation of Onion Routing was accomplished by Michael G Reed, Pal F. Syversion and David M. Goldshlag from the US Naval Research Laboratory. The Onion Router project published several design and analysis papers (Syverson et al., 1997; Syverson et al., 2000, 2001). The main advantage of Tor is able to send an encrypted traffic between client and server over the Internet through a proxy. In this system, only the last proxy is capable to learn the primary or original transmission and there is no single proxy has an information of the starting and destination traffic.

Stokkink et al. (2015) evaluate the network performance of tunnel implementation into Tor network. From the observation, normally users are difficult to use a privacy-enhancing technology and it will slow down the Internet performance and speed after a user successful connect into Tor network. With the advancement

of the technology, the use of IoT to support in any fields including the network security and privacy implementation become a common nowadays (Islam et al., 2020; Kadir et al., 2020; Thakur et al., 2020). Besides, the use of the microprocessor board enables the existence of devices or tools that can be used to increase the security and privacy within the network. For example, Kutukian (2016) implements the network monitoring tools on Raspberry Pi 3 to enable network admin to get fully monitoring access against networking hardware such as router, firewall and core switch. Several studies focus in intrusion detection system using Raspberry Pi for network monitoring and security were established (Osman et al., 2016; Tripathi & Kumar, 2018; Sumanth & Bhanu, 2020).

Meanwhile, Vitosinchi (2016) uses a Tor node into Raspberry Pi in order to protecting user privacy. The study performs a traffic capturing by using Wireshark. There are three types of Tor nodes, which are a bridge node, relay node, and exit node. For the testing the level of privacy protection, the researcher finalizes the experiment by describing the process of communication among web server and client. Jamal et al., (2019) were designed and developed a portable Tor router with Raspberry Pi, which provide anonymous browsing to enhance the privacy of users who do not want their personal information to be shared. In order to improve the security and privacy in local network, Raspberry Pi is able to be used as a VPN server in a local home network. This will provide connection between public Internet and home network (Lales & Carranza, 2013).

METHODOLOGY

This section gives a details discussion on the system architecture, system design and implementation for developing a secure network architecture using Raspberry Pi.

System Architecture for Developing a Secure Network Architecture using Raspberry Pi

Figure 1 shows the system architecture for the proposed work, which represents a design for developing a secure network infrastructure using Raspberry Pi as an access point. The Raspberry Pi board will act as the access point as it connects directly to a router and then allowing the connection from the router for users through the wireless interface. In this proposed system, VPN installation and configuration were implemented on Raspberry Pi. It will automatically be started and connected to the VPN server once it is booted. This will be able for Raspberry Pi to route the user's traffic into the encrypted network which is VPN network. On the VPN server side, all the traffic which has been sent by Raspberry Pi access point will be routed into several Tor servers randomly. By doing this, user's connection will be safe from any data theft or traffic analysis. therefore, user can browse securely and anonymously over the Internet. In addition, user also will be able to browse any blocked content over the Internet.

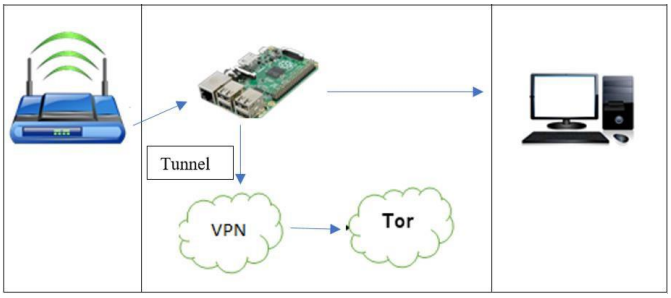


Figure 1: System Architecture

The Raspberry Pi will be booted up a Raspbian operating system which is based on Debian optimization. It provides targeted kernel and software, which support multi type of ARM (ARM5, ARM6, ARM7 and ARM8) instruction. In addition, this operating system also gives fully control and responsibility over the system. Besides, the Raspberry Pi is able to be remotely connected by using Putty software after all the configuration needed for remote control has been setup. Next, the other way to use and manage this Raspberry Pi system is by using Virtual Network Computing (VNC). This kind of platform uses a graphical remote desktop. So, Raspberry Pi system may be controlled easily with the graphical view.

Design for Developing a Secure Network Architecture using Raspberry Pi

Figure 2 shows the case diagram of anonymous network connection by using Raspberry Pi. This require user to apply Raspberry Pi TorVPN access point to get an anonymous and better security connection in network and users is protected from any Internet surveillance, which also known as traffic analysis. This Raspberry Pi TorVPN access point provides users to become an anonymous user while browsing through the Internet, and all user activities will be difficult to trace by third person such as hacker or traffic analysis either internal or external network. In addition, user will feel safe to browsing anything over the Internet without worry about any attacks and data theft.

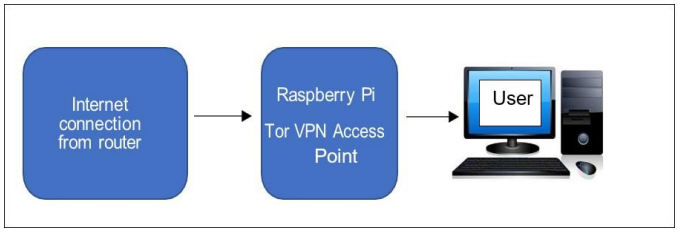


Figure 2: Case Diagram

Meanwhile, Figure 3 shows the logical design contains of two areas of networks, which are direct sim router network and TorVPN access point network. Direct sim router network works as a gateway to route the data packet to the Internet and TorVPN works as a gateway to direct sim router. In general, this logical design includes the TorVPN area network that will work inside the direct sim router area network. The Internet connectivity was served by ISP that going through direct sim router before it pass-through TorVPN access point in order to give the Internet connectivity to its clients. The ISP chosen in this research was Celcom and its internet connectivity was up to 50Mbps.

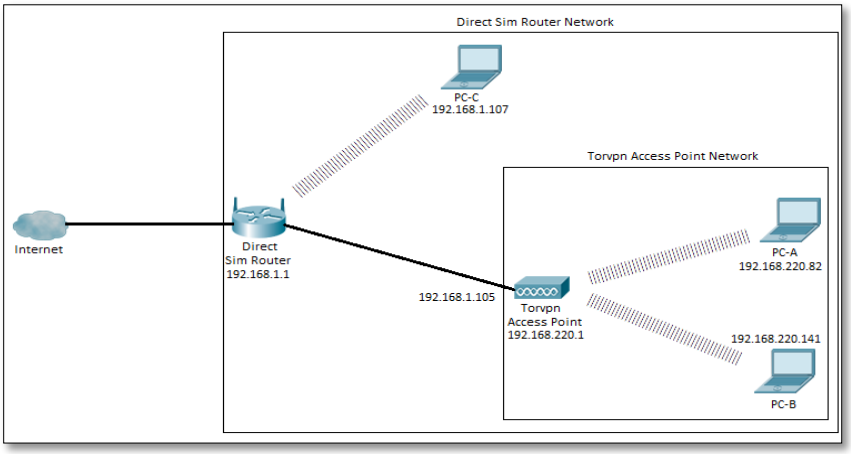


Figure 3: Logical Design for the Network

Implementation for Developing a Secure Network Architecture using Raspberry Pi

i. Raspberry Pi TorVPN Access Point

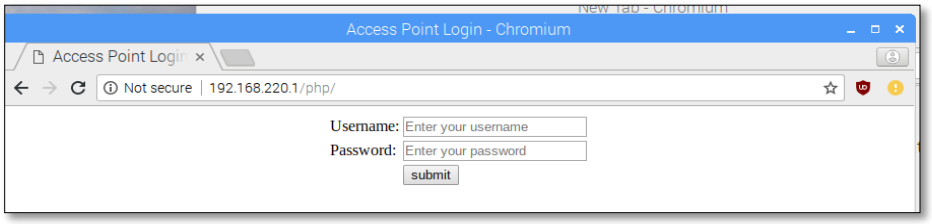
Raspberry Pi was used in this proposed work as a microprocessor device and for TorVPN access point system to work accordingly. Raspberry Pi generally used to optimize system, application and IoT device due to it is able to have its own operating system and capable to get connected with the Internet and allow system or application to be run wirelessly. In this proposed work, it is used to receive the Internet connection from direct sim router and share the connection to users wirelessly. Due to the Raspberry Pi 3 B+ has a build in function of Wi-Fi, so it does not need an external wireless adapter in order to work as an access point. To connect the Raspberry Pi with direct sim router, RJ45 or LAN cable was used, and it supported up to 100Mbps of transfer rate between devices. In addition, power supply was used for power on direct sim router and booting up the Raspberry Pi.

Then, some software, services and tools were installed on the Raspberry Pi accordingly. For instance, Raspbian OS is the operating system which is free to use on Raspberry Pi equipment. Its system was based on the enhanced Debian and included the basic programs, tools, and utilities to ensure Raspberry Pi run and

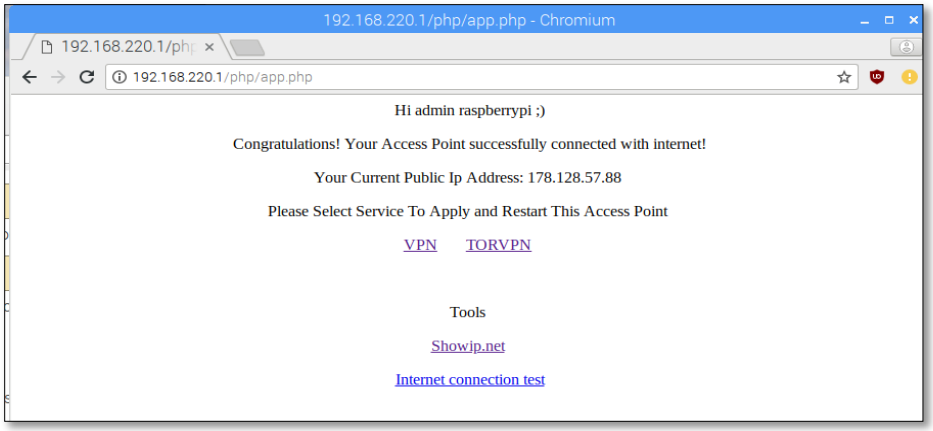
works. Thus, Raspbian OS was officially supported operating system, which used to develop and maintain the system. To make Raspberry Pi as an access point and able to forward the data packet from its clients to the Internet, an appropriate installation and configuration are needed. Then, the OpenVPS was used and implemented in the Virtual Private Server (VPS) and a VPN server and Raspberry Pi as VPN client. The OpenVPN server was configured to establish the connection to the Tor service. Finally, the Tor installation package was installed, which will establish the connection from VPN server to the Tor network service which VPN server was act as a bridge for VPN client to send and route the connection and data packet into Tor network through several of Tor servers.

ii. Raspberry Pi TorVPN Access Point Web Interface

The web interface of Raspberry Pi access point was designed after hardware and necessary software was successfully installed. This web interface is able to view the connection's details, access an additional tool and perform some configurations. Figure 4 (a) and (b) show the login and main web page of TorVPN access point. This web page only can be accessed by authorize users of this access point.



(a) Login Page



(b) Main Page

Figure 4: TorVPN Access Point Interface (a) Login Page and (b) Main Page

This web page contains the details about the current Internet connection and where the TorVPN access point was routed the user's data packet either to VPN network or Tor network. Besides, this page also views the current IP address of an access point. Moreover, it provides the clicking button for user to choose the services, either to use and tunnel the TorVPN access point connection into VPN or Tor network.

FINDINGS AND DISCUSSIONS

This section analyses the result of experiments. Two experiments were performed in this study. First experiment objective was to analyses the encryption of the data packet which going out from both direct sim router network and TorVPN access point network. The second experiment objective was to measure the performance of Internet connectivity while the Raspberry Pi access point was tunneling its connection to the VPN server with configured and connected to Tor network.

Experiment 1: Analyses the Encryption of Data Packet which Going Out from Direct Sim Router and TorVPN Access Point

Two situations were investigated in this experiment. Firstly, sniff data packets that were come from PC-C, which was a client for direct sim router. Secondly, sniffed a user's data packet that came from TorVPN access point network. Figure 5 shows the logical design of area network that has been tested which include direct sim router area network and TorVPN access point network. PC-D was added in direct sim router and act as a sniffer to perform Man in The Middle (MiTM) attack.

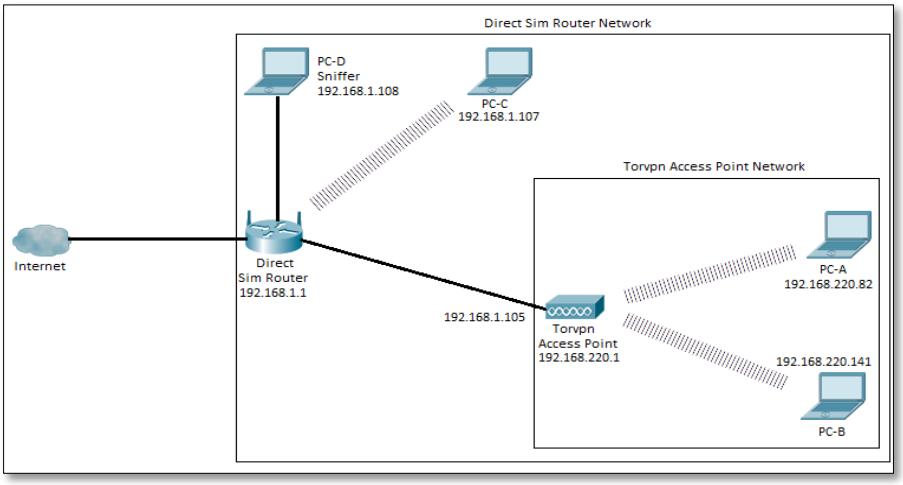


Figure 5: Logical Design Network with Sniffer

PC-D was operated the Kali Linux OS and executed several tools to perform MiTM attack and replace it IP address as a main router which is direct sim router. In other names, it called as IP Spoofing. Spoofing process has been done by running the Ettercap and performs the ARP Poisoning. After that, all clients which connected to direct sim router will assume the current gateway in the network was PC-D IP address and send all packets to the attacker. Then, PC-D captures all user data packets by using Wireshark before it releases the data packet over the Internet.

The purpose of this experiment is to verify the confidentiality in terms of encryption of the data packet that travelled to the Internet by suing direct sim router network and TorVPN access point network. Both packets from both networks were sniffed and analysed. The packet that has been filtered was HTTP packet. Table 1 shows the results on tested packet.

Table 1: Result for Sniffing Test

Data Packet's Origin	Password Sniff	Encryption
PC-C (Direct sim router)	Success	No
PC-A & B (TorVPN access point)	Failed	Yes

Based on Table 1, the data packet that comes from client in direct sim router network was more likely to be intercept by the sniffers. Therefore, the users that used public network to access an unencrypted website such as HTTP website was easily targeted as a victim for MiTM attack. The password or any other surfing information that contains in the data packet can be captured and analysed by an unauthorized person easily. However, if the packet was coming from clients in a TorVPN access point network, the data packet was fully encrypted and password or surfing information in the data packet was not sniffed by another unauthorized person.

Experiment 2: To Measure the Performance of Internet Connectivity from TorVPN Access Point

The main objective was to measure the performance of Internet connectivity while tunnelling to VPN server, which connected with Tor network. The elements that had been considered were based on ping, download, and upload speed. This experiment was repeated three times on every ten minutes with different IP address of TorVPN access point. The IP address were 178.32.147.150, 185.220.102.7, and 185.234.217.242. These IP addresses were the exit node's IP address from Tor relay.

In this experiment, the Internet connectivity performance test was measured by using speedtest-cli which has been provided by speedtest.net for Linux system. Table 2 shows the results of average value for ping, download and upload speed.

Table 2: Average for ping, download, and upload speed

IP Address	Average Ping (ms)	Average Download Speed (Mbps)	Average Upload Speed (Mbps)
178.32.147.150	846.782	2.23	2.9
185.220.102.7	744.962	2.17	2.2
185.234.217.242	1007.298	3.28	2.94

Based on Table 2, there were three types Internet connectivity performance test, which are ping, download, and upload. The results show that the Tor network which has been connected from TorVPN access point had unstable performance as it changes the IP address of the last node or in another name called exit relay. Moreover, it also happened because of Tor service itself route the data packet through a different path of server in Tor relay. The average for ping, download, and upload was decreased as the IP address 178.32.147.150 changed to 185.220.102.7 and the percentage of drops were 12.02% for ping, 2.69% for download, and 24.14% for upload accordingly. However, after TorVPN access point got a new IP address, which is 185.234.217.242, the performance of the Internet connectivity was increased drastically. The percentage of the increments were 35.21% for ping, 51.15% for download, and 33.64% for upload. Therefore, it can be concluded that Tor service does not ensure the stability of Internet connectivity, but its connection can be more stable if the data packet was routed through the Tor server, that had a better Internet connection performance because it has less distances between servers in Tor relay.

CONCLUSION AND RECOMMENDATIONS

This paper presents the design and implementation of TorVPN access point using Raspberry Pi, which contains the combination of Tor and VPN service, that was reduced the difficulty to use the Tor and VPN service when connecting to the Internet. The client which connected with TorVPN access point can easily use the Tor and VPN services without bounded with the complexity of configuration or installation to any particular software needed. There were two experiments involved in this study, which is confidentiality test and the Internet connectivity performance test. All experiments were successfully applied and gave the positive and encouraging results.

In conclusion, based on the analysis of the experiments implemented in VPN and Tor network, the performance of Internet connectivity was unstable as the IP address of TorVPN access point changed from the previous IP address because the path and route of the data packet inside Tor relay was not same, and it also depends on the distance between the Tor server. Meanwhile, the confidentiality of TorVPN access point network was also proved fully encrypted and secured. Thus, the combination of VPN and Tor service was suitable to implement in the normal network for user who needs a better security and privacy of Internet connection. Hence, Tor and VPN service is important to improve the privacy protection, anonymity, and security over the internet. Furthermore, this study can be enhanced by improvising any part of hardware or software such as using a real router as an access point.

REFERENCES

Bian, J., Cao, C., Wang, L., Ye, J., Zhao, Y., & Tang, C. (2021). Tor Hidden Services Discovery and Analysis: A Literature Survey. *Journal of Physics: Conference Series*, *1757*(1), 1-6.

Islam, Md. M., Rahaman, A., & Islam, Md. R. (2020). Development of Smart Healthcare Monitoring System in IoT Environment. *SN Computer Science*, *1*(3), 185.

Jamal, A., Kumar, D., Helmi, R. A. A., & Fong, S. L. (2019). Portable Tor Router with Raspberry Pi. *Proceedings of the 2019 8th International Conference on Software and Computer Applications*, 533–537.

Kadir, M. M. A., Osman, M. N., Othman, N. A., & Sedek, K. A. (2020). IoT based Car Parking Management System using IR Sensor. *Journal of Computing Research and Innovation*, *5*(2), 75–84.

Kutukian, G. (2016). *Raspberry PI 3 Home Network Monitoring Tool* [Thesis, California State Polytechnic University, Pomona]. http://dspace.calstate.edu/handle/10211.3/179269

Lales, C., & Carranza, A. (2013). *Using the Raspberry Pi to Establish a Virtual Private Network (VPN) Connection to a Home Network.*

Osman, M. N., Zulrahim, M. S. A. M., & Maghribi, M. (2016). RaspyAir: Self-Monitoring System for Wireless Intrusion Detection using Raspberry Pi. *Journal of Computing Research and Innovation*, *1*(1), 14–21.

Phobos. (2010, June 1). *Plaintext Over Tor is Still Plaintext | Tor Blog*. https://blog.torproject.org/plaintext-over-tor-still-plaintext

Sheik, F., & Xinrong, L. (2014). Wireless Sensor Network System Design Using Raspberry Pi and Arduino for Environmental Monitoring Applications. *Procedia Computer Science*, *34*, 103–110.

Stokkink, Q., Treep, H., & Pouwelse, J. (2015). Performance Analysis of a Tor-like Onion Routing Implementation. *ArXiv - Computer Science*, *abs/1507.00245*, 1–6.

Sumanth, R., & Bhanu, K. N. (2020). Raspberry Pi Based Intrusion Detection System Using K-Means Clustering Algorithm. *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, 221–229.

Syverson, P. F., Goldschlag, D. M., & Reed, M. G. (1997). Anonymous Connections and Onion Routing. *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097)*, 44–54.

Syverson, P., Reed, M., & Goldschlag, D. (2000). Onion Routing Access Configurations. *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*, *1*, 34–40.

Syverson, P., Tsudik, G., Reed, M., & Landwehr, C. (2001). Towards an Analysis of Onion Routing Security. In H. Federrath (Ed.), *Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability Berkeley, CA, USA, July 25–26, 2000 Proceedings* (pp. 96–114). Springer.

Thakur, D., Kumar, Y., & Vijendra, S. (2020). Smart Irrigation and Intrusions Detection in Agricultural Fields Using IoT. *Procedia Computer Science*, *167*, 154–162.

Tiwari, S., Arora, D., & Singh, V. (2015). *Implementation of Routing Protocol for Network and Data Security using Onion Routing with Salt Method*. *5*(7), 3.

Tripathi, S., & Kumar, R. (2018). Raspberry Pi as an Intrusion Detection System, a Honeypot and a Packet Analyzer. *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*, 80–85.

Vitosinschi, A. (2016). *Protecting Privacy using TOR*. Turku University of Applied Sciences.

Younglove, R. (2000). Virtual Private Networks—How They Work. *Computing & Control Engineering Journal*, *11*(6), 260–262.