Progress in Engineering Application and Technology Vol. 3 No. 1 (2022) 571-579

PEAT

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/peat
e-ISSN : 2773-5303

Wifi Security at Edu Hub

Nur Amalia Zamros[1], Azlina Bahari[1]*

[1]Department of Electrical Engineering Technology, Faculty of Engineering Technology, Universiti Tun Hussein Onn Malaysia, 84600 Pagoh, Johor, MALAYSIA

*Corresponding Author Designation

DOI: https://doi.org/10.30880/peat.2022.03.01.057
Received 17 January 2022; Accepted 11 April 2022; Available online 25 June 2022

Abstract: Many people can use Wi-Fi without a password or permission in today's world of globalization and modernity. This is due to the widespread use of open Wi-Fi in public places such as universities, businesses and more [1]. Network security is a growing concern among domestic as well as industrial computer users. Security has become a key worry as the internet has grown and dedicated to the study of security will help anyone fully comprehend how security technology evolved [4]. Several methods of assessment were employed, including enlisting the assistance of UTHM students, conducting research, conducting a poll on the Wifi connection and intensity at UTHM, and soliciting supervisor feedback. This study demonstrates the progression of an evaluation, including changes in assessment instruments and methodology, by describing the evaluation methods and procedures for each phase of the study in detail. This project will assist in network security by requiring a password to log in to the WIFI. Aside from that, it is also required to establish a private network to connect and share data without fear of being tracked, as well as to set a specific restriction for broadcasting videos on YouTube so that scholars may concentrate on their academics rather than waste time watching irrelevant movies. Students at UTHM were asked to log in to the Internet access with the specified password to collect data. Furthermore, can utilize the point-to-point tunnelling protocol (PPTP) beneath a virtual private network (VPN) then configure the application restriction through using 7-layer protocol. The MikroTik Rb4011 and Winbox software were used in this study. The consequences were discussed during a discussion of the procedure taken to achieve the study's objectives.

Keywords: MikroTik, Firewall, VPN

1. Introduction

Many people can use Wi-Fi without password or permission in today's world of globalization and modernity. This is due to widespread use of open Wi-Fi in public places such as universities, businesses, and so on. We can safeguard our Wi-Fi from being utilized by strangers or hackers thanks to this effort, Wi-Fi security in Edu Hub. It assists the Wi-Fi owner in keeping their Wi-Fi and data secure because

*Corresponding author: lina@uthm.edu.my

strangers are unable to access the Wi-Fi without a password, and each device has its own IP address, which can only be accessed by your IP address.

It appears that in today's society, functioning without connection to the wireless internet would be practically impossible. Wi-Fi is used by people all over the world for everything from enjoyment to reaching their goals. However, with the internet's widespread use comes an underlying threat in the form of hackers looking to exploit security weaknesses in order to obtain access to our personal data and information. In essence, wireless security is the protection of unauthorized users from accessing a wireless network. Furthermore, wireless security, often known as Wi-Fi security, tries to ensure that only the people you permit have access to your data. The Wireless Alliance designed authentication security protocols such as Wired Equivalent privacy (WEP) and Wi-Fi protected Access (WPA) that are used to assure wireless security. There are four wireless security protocols currently available which are Wired Equivalent Privacy (WEP, Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA 2) and Wi-Fi Protected Access (WPA 3).

2. Methodology

MikroTik Router OS is a Linux -based operating system Installed on the MikroTik's proprietary hardware (Router Board), or on standard x-86- based computer which is our personal computers [3], it turns the computer into a network router and implements various additional features such as firewalling, Virtual Private Network (VPN) service and client, bandwidth shaping and quality of service, wireless access point functions and other commonly used features when interconnecting networks. The system is also able to serve as a captive-portal -based hotspot system. The operating system is licensed in increasing service levels, each releasing more of the available Router OS features. An application programming interface is available for direct access from applications for management and monitoring. This Router OS supports many applications used by internet service providers, for example OSPF, BGP, Multiprotocol Label Switching (VPLS/MPLS). The Router OS also supports Internet Protocol Version 4(IPV4) as well as Internet Protocol Version 6 (IPV6).

2.1 Block Diagram

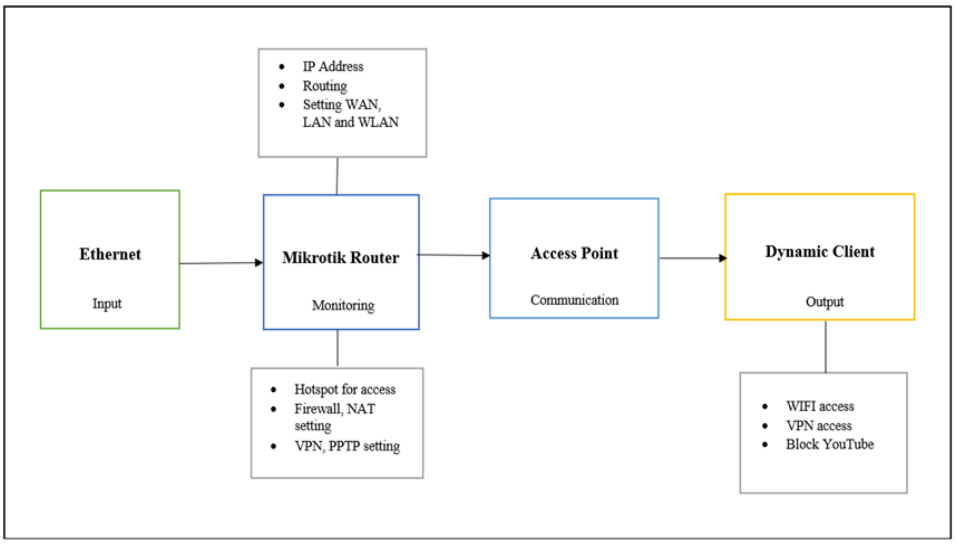

Figure 1: Block diagram of project

Based on the Figure 1, The Mikrotik wireless router serves as both a wireless access point and a LAN gateway. There is one WLAN interface and two ethernet interfaces on this wireless router. For the input, the ethernet will connect to the Mikrotik Router so that the Mikrotik Router can Monitoring the Ip Address. For this project, Mikrotik Router will setting local area network (LAN), wide area

network (WAN) and wireless local area network (WLAN). Other than that, the Mikrotik also will being set with hotspot, network address translation (NAT) and firewall. The Mikrotik also being set that it can have virtual private network (VPN) which specify more to point to point tunnelling protocol (PPTP) so that can have our own network. The Mikrotik also have been set a firewall to block YouTube so that no student can access to YouTube, and it is one of the final products of this project other than having own Wi-Fi access and VPN access.

2.2 Project Flowchart

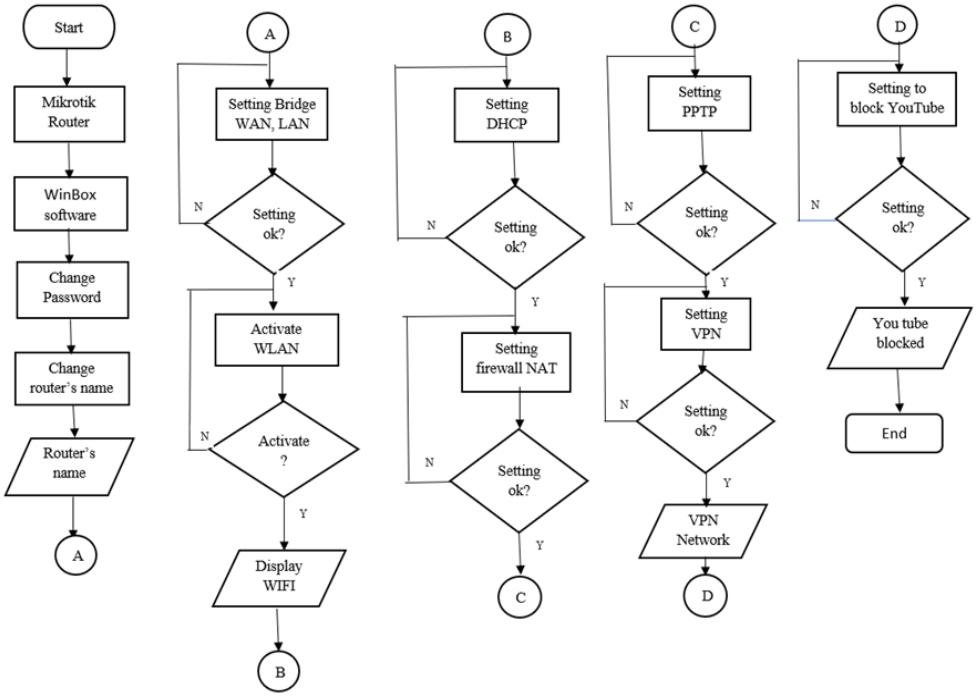

Figure 2: Project flowchart

Based on Figure 2 which is the project flowchart. First and foremost, the Mikrotik have to be able to connect with the ethernet so that it can conduct our project smoothly. After being able to connect with the internet, the Mikrotik router will detect the internet and start functioning and can connect with Winbox software It is reasonable to presume that using Mikrotik to manage network traffic increases user prosperity. After that, the password and the router's name can be changed to access the WinBox software. Next, set WAN, LAN, WLAN and HOTSPOT bridge. After all the setting have been completed, WLAN can be activated so that the Wi-Fi from the Mikrotik which named before can be found in Wi-Fi connection list and can be used as long as it has the username and password of the Wi-Fi. Set the dynamic host configuration protocol after that (DHCP). DHCP is a client or server that automatically sends information to an IP host. After that, set the NAT and firewall which is the most important part to secure the network. Next, PPTP should be set as the part to secure data before access the VPN network. Finally, the router has to set on blocking YouTube on the 7-layer protocol firewall to achieve the project's aim.

2.3 Network Design

The tunnelling PPTP (Point-to-Point Tunneling Protocol) is a set of communication protocols that govern the secure implementation of virtual private networks (VPNs), which allow businesses to extend their private networks across the public Internet via "tunnels". By utilising the infrastructure of a wide area network (WAN), such as the network of a public Internet service provider (ISP) or telecom, a large

organization with distributed offices can create a large local area network (LAN) – essentially a VPN – by utilizing the infrastructure of a wide area network (WAN) (WAN). It is less expensive to do this than to set out a network infrastructure over such long distances [6].

By creating a VPN over TCP/IP-based networks, such as the Internet, PPTP allows for the secure transmission of data from a remote client to a server in a private company network. It enables remote users to securely connect to business networks via the Internet, just as if they were physically present on the network. As in Figure 3 shows that it is a schematic of PPTP tunnel that have been used in this project. The place taken in Block B of UTHM which Office A is a server located on the third floor while Office B is a client who is located on the second floor. As Figure 4, it is also about PPTP configuration but with the different cases which is the router will connect to a computer which will be a Server and a mobile client which we connect to another PC without router.

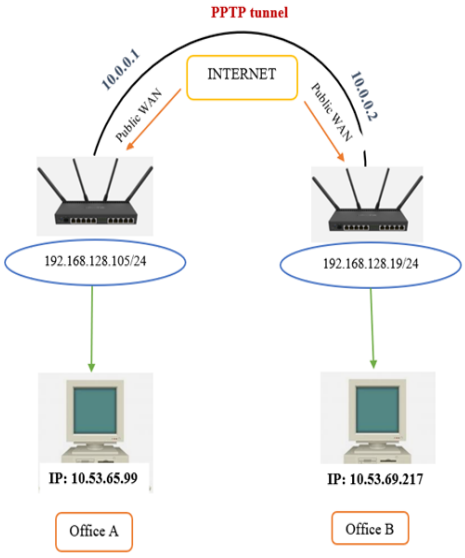

Figure 3: Connection Diagram of Office A and Office B

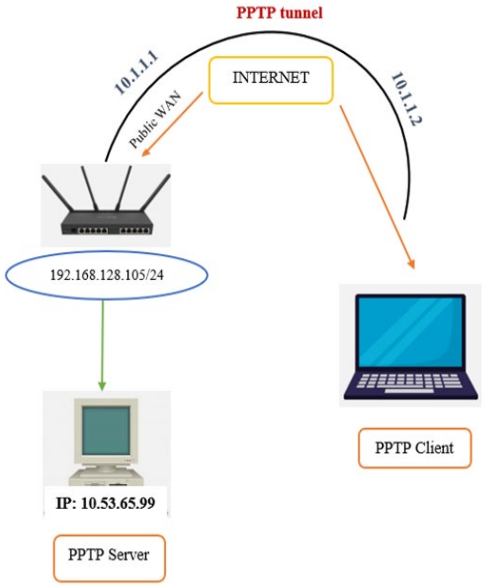

Figure 4: Connection diagram of PPTP Server and PPTP Client

3. Results and Discussion

Figure 5: Two devices connected to Wi-Fi (MikroTik ama)

To be able to get as shown in the figure above the router has to set the interface of the WLAN connection to be able to make our own Wi-Fi connection. First, after connecting the Winbox software with MikroTik router and also after do the basic configuration of MikroTik such as change the name of router to MikroTik-Ama, setting router's username and password and not to forget on setting the WAN and LAN bridge. Next, the router has activated the WLAN on wireless section. After activated, it has to go to the interface list and set to ap bridge mode with band of 2 GHz-B/G/N and frequency of 2437. Later, the SSID and security profile must also be configured. Following the configuration of the WLAN interfaces, the mode of the WLAN is R, indicating that it is operational and reachable, and that the configuration was successful. To connect to Wi-Fi, make sure that both the WLAN on interfaces list and the wireless list are in the running and reachable mode. The figure 5 above depicts two distinct devices that can access to the MikroTik Router's Wi-Fi network. The Wi-Fi network is reliable and smooth.

3.1 Result of VPN (PPTP) setting on Office A and Office B

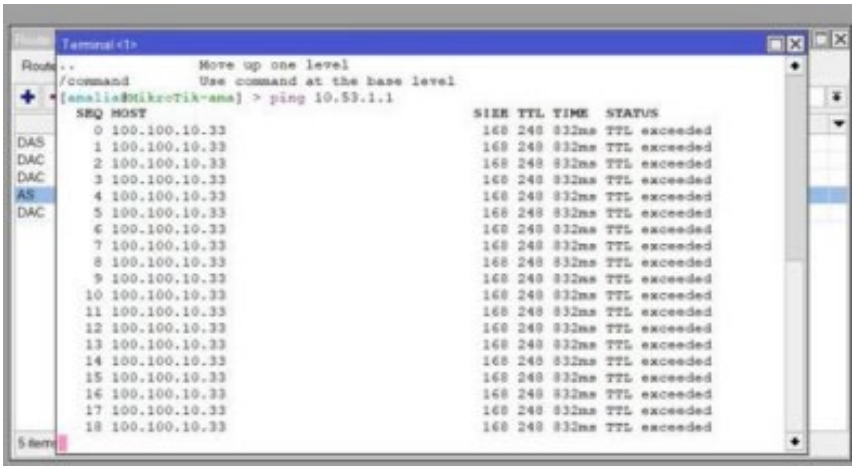

Figure 6: New Terminal result after connecting Office A and B

To begin, the router must enable the PPTP server in the PPP menu of the Winbox software, as shown in the figure 6 above, by clicking the enable sign to activate the server and modify the default profile to default encryption, as highlighted before in chapter 3. Go through the secrets area, which is

also in the PPP menu, after enabled the PPTP server. Set the name, password, service, profile local and remote addresses throughout this area to pptp, 12345, and default encryption. Set 10.0.0.1 and 10.0.0.2 as your local and remote addresses, respectively.

Next, set up for Office B which is the second floor of Block B of UTHM. First, open another Winbox software with the different MikroTik router and set the PPP menu with PPTP client setting and names it as <pptp-out 1> on the general setting. As for the dial out setting on the interfaces, connect the PPTP client to the PPTP server which is Office A (10.53.65.99) and also set the user and password with default- encryption as the profile and apply it. to make the gateway reachable on the route list of Office A, required to set the route by clicking the '+' on the list. To find the route list, go to the IP menu and click on the route section. As to make it reachable, set the Dst. Address which is the destination address and put the IP of Office B which is 10.53.69.217. Other than that, setting on to fill in the gateway. There are two option which are <pptp-pptp> or can fill in it with 10.0.0.1 – 10.0.0.2. The setting for the Office B is also the same way as Office A but have slightly different which are Dst. Address for Office B is 10.53.65.99 with the gateway of pptp-out 1or also can put 10.0.0.2 -10.0.0.1.

The figure 6 show that the result of the new terminal of Office A. Open Winbox of Office A, we have to ping to Ip of office B to identify if the network is connected or not. As the figure above shown, it appears that it has been successfully connected. Then, do the same thing on Office B router. As it successfully connected, the peer-to-peer case is complete with the step that we make it first for PPTP service and also activate the PPTP server then make secrets and continue with settings in Office B to dial up of PPTP client and if it is connected between PPTP server and PPTP client, make static routing in order to communicate between LANs in each office and if it is, then do a Ping test from each office to check if is it really connected or not.

3.2 Result of VPN (PPTP) setting on PPTP Client without MikroTik

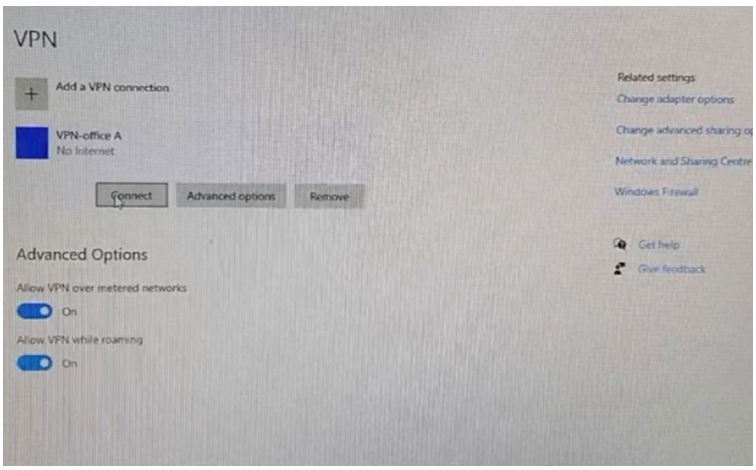

Figure 7: VPN connection on Client

This section, a configuration of PPTP client for mobile client by starting with making configuration on the PPTP server side were made. For PPTP Server, make Office A as a server with the same IP which is 10.53.65.99. Due to have activated it earlier, it doesn't need to make or activate the new PPTP service and just need to edit the part of the secret for accounts that are used to dial upside to side and can also differentiate the mobile client. Next, used the IP pool settings which required us to enter the IP menu. Then enter into the pools submenu and add the name for the new IP Pool which have been set with poolVPN with IP range of 10.1.1.2 - 10.1.1.100. It will be added a new rule or new pools named poolVPN. Then it needs to be modified in the profile sections because it will differentiate for accounts used by remote clients and also side to side connection. Named the profile as profileVPN. Then, for a local address, fill in the allocation of the IP address for PPTP server which supposedly 10.1.1.1 and

remote address poolVPN due to the use IP pools. To make sure that the use encryption in profile section has been activated and not to forget that limits tab. It is very important parameters. For only one parameter required to select or activate “no” for the choice on only one due to if choose “yes” or “default” later who can use an account that are made earlier in Secrets only one client and for the current case, one account can be used by many remote clients. After applied all of them, on the profiles tab, create a new profile for remote client.

On the profile tab that have created a new profile for remote client connection, make a new Secret on the Secret tab and add one new account for remote client connection. The name parameter is the same as before. Fill in the username as pptp2 with remote12345 as the password. Then for service parameter, choose pptp because it will create a new profile for remote client connection and choose profileVPN as the profile which direct it to the profile that have created earlier. Then, for Local Address parameters and the Remote Address in the secret, there’s no need to fill in because already made and set on the profileVPN. Next, do testing with dial up from the client side. In this section, try to dial up to pptp server that have created before. For the Windows operating system, first step is open the menu in “Control Panel”, then go to the “Network and Sharing Centre” menu and select the “set up a new connection or network”. Next, choose to create a new connection and then have to select “use my internet connection (VPN)”. To dial up on a Windows operating system, the column is provided and have to fill in the Internet Address parameter which can fill in with the Public IP of PPTP Server. Then for the destination name, fill in to name the interface that will be made on this device which have filled as VPN- office A. Later, referring to what have been made before on PPTP Server, enter the parameters for the username which have created by name “pptp2” and “remote12345” as the password. On the next step, automatically the system will dial up to PPTP Server

3.3 Result on Limiting Time using YouTube

Figure 8: Blocking YouTube on L7 Protocol

Based on the Figure 8, this is the step on how to block YouTube for a limit user. So, the first thing that need to do is to go to IP menu and select firewall and will create a layer seven region. Next, click on the symbol of ‘+’ and add the code as in the figure 8 above under the name of YouTube [10]. For the next step, which is to set and create Mangle rule for parties are used for YouTube traffic that will mark all the traffic that will be going to YouTube. To make it have only limited user, go to user’s menu item, and click on user’s tab and the double click on any user who will be restricted and not. In this section, set that the time for user can browse and streaming to YouTube are only for 30 minutes for 50 users to create the setting just like the figure 8 above, add the configuration by setting with forward chain on the general side while for the advance part, put YouTube on the layer 7 protocol which have named it before. And finally on the action site, put as mark connection with youtube_conn as the new connection mark by clicking the button ‘+’ on filter rules side, create a new rule to block the traffic. On the general setting, put forward on the chain choice and the connection mark should be youtube_conn

as have been set them before and change the protocol to TCP. Then the action part, change the action to reject and on the reject with part section, put with TCP reset and put a comment of "Block Youtube" as a comment for the new firewall rule.

3.4 Analysis

To analyse, as can be seen when doing all these settings, ensure that our profile security has WPA2 PSK is a security protocol developed by the World Wide Web Consortium (W It is a technique of safeguarding the network using WPA2 with the optional Pre-Shared Key (PSK) authentication, which was developed for home users without a corporate authentication server. It is also known as WPA or WPA2 Personal. To encrypt a network with WPA2-PSK, confirmed that to give our router a plain-English password between 8 and 63 characters long, rather than an encryption key. That passcode TKIP (Temporal Key Integrity Protocol) is used to generate unique encryption keys for each wireless client, and the encryption keys are changed on a regular basis, along with the network SSID.WEP also supports passphrases, but mainly to make it easier to construct static keys, which are often made up of the hex digits 0-9 and A-F.

Other than that, besides WPA2 PSK, PPTP also playing a big role as a security which only connected server and client with secure where this network protocol allows us to send data package or make a connection via the internet which is safe and secure. Tunnelling is the process of sending packets from a computer on a private network to another network, such as the Internet. Other network routers are unable to connect to the private network's PC. The routing network, on the other hand, can deliver the packet to a computer that is connected to both the routing network and the private network, such as a PPTP server, through tunnelling. Tunnelling is used by both the PPTP client and the PPTP server to securely route messages to a computer on the private network using routers that only know the private network intermediate server's address. There are few tips to do PPTP VPN configuration. The first is for the PPTP path, it will be more stable and much easier on the server side in particular have dedicated internet connection or use public IP that is static. Second, for client devices that use Operating System Windows 7 or above, make sure that on the PPTP Server we choose the profile parameter with default-encryption so when we activate PPTP Server for profile parameters.

MikroTik RouterOS provides a fantastic functionality that allows us to restrict user access to specified IP addresses. Users will only be able to connect from specified IP addresses if IP-based user access restrictions are implemented. As a result, users will be safe, and hackers will have a hard time logging in using their credentials. Moreover, by using MikroTik, it also can be set that on the User setting to have a limit time access. As for the limit user and blocking YouTube, the setting for limit user that have been done in this project is only for UTHM students. At one session, there are only 50 students that can stream to YouTube for 30 minutes and after 30 minutes the YouTube will be automatically blocked. The next session, the 50 early birds' students can access to YouTube and yet still can be used only for 30 minutes. This will make the traffic flow smoothly

4. Conclusion

In a word, this project will make an internet connection in UTHM Pagoh more secure, particularly for UTHM students, allowing them to share data while utilizing Wi-Fi with the look of a PPTP tunnel. Furthermore, by using WPA2 PSK on our router settings, it is possible to keep our password private. In the future, it is recommended that UTHM adopt a MikroTik router as their primary Wi-Fi connection because it is simple to set up but still secure. Aside from that, we have YouTube blocked at limited time to prevent students from watching videos online and to encourage them to concentrate on their studies.

Furthermore, the approaches used in this project have been carefully considered and planned, such as determining the most effective processes or techniques, which are critical in producing precise outcomes. In addition, with a solid network, this project can provide customers with convenience and benefits for an extended period of time. Apart from that, it has uncontrolled access to vast volumes of

information. The network can manage effectively with high internet network security assurance for this project.

Acknowledgement

The authors would like to thank the Faculty of Engineering Technology, University of Tun Hussein Onn Malaysia for its support.

References

[1] A. M. Saliu, M. I. Kolo & M. K. Muhammad, "Internet Authentication and Billing (Hot Spot) System Using MikroTik Router Operating System," International Journal of Wireless Communications and Mobile Computing, vol. 1, no. 1, pp. 51-57, 2013.

[2] P. Mollick, S. Biswas, A. Halder & M. Salmani, "Mikrotik Router Configuration using IPv6," International Journal of Innovative Research in Computer, vol. 4, no. 2, pp. 2001-2007, 2016.

[3] M. D. Lesmana Siahaan, M. Sari Panjaitan & A. P. Utama Siahaan, MikroTik bandwidth management to gain the users prosperity prevalent. International Journal of Engineering Trends and Technology, 42(5), 218–222 (2016)

[4] MONDAY, I. D. A. H. O. S. A. P. A. U. L. (n.d.). Network security using MIKROTIK Router Operating System. Scribd. Retrieved May 2012, from https://www.scribd.com/document/126896407/NETWORK-SECURITY-USING-MIKROTIK-ROUTER-OPERATING-SYSTEM

[5] A. Koujalagi, Network Security Intelligence for small and medium scale industry 4.0 design and implementation. International Journal of Computer Sciences and Engineering, 6(10), 475–485 (2018)

[6] B. Usmonov, A. Iskhakov, A. Shelupanov, A. Iskhakova, and R. Meshcheryakov, "The cybersecurity in development of IoT embedded technologies," 2017 Int. Conf. Inf. Sci. Commun. Technol., pp. 1–4, 2017.G. Veruggio, "The EURON roboethics roadmap," in Proc. Humanoids '06: 6th IEEE-RAS Int. Conf. Humanoid Robots, 2006, pp. 612–617, doi: 10.1109/ICHR.2006.321337 (Example for conference paper or proceedings with doi number)

[7] J. Charles, Kolodgy Christian A. Christiansen, ―Network Security Over watch Layer: Smarter Protection for the Enterprise‖, Sponsored by: Trend Micro, November 2009.

[8] O., Adeyinka "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008.

[9] B. Daya, "Network Security: History, Importance, and Future ,"University of Florida Department of Electrical and Computer Engineering , 2013. http://web.mit.edu/~bdaya/www/Network%20Security.pdfJ. O. Williams, "Narrow-band analyzer," PhD dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993 (Example for a thesis)

[10] Author, author. (2018, September 18). Mikrotik tutorials. TKSJA. Retrieved January 25, 2022, from http://tksja.com/