

## Wi-Fi Login Authentications System Using MikroTik

Azraei Khairuddin<sup>1</sup>, Azlina Bahari<sup>1\*</sup>

<sup>1</sup>Department of Electrical Engineering Technology, Faculty of Engineering Technology,  
University Tun Hussein Onn Malaysia, 84600 Pagoh, Johor, MALAYSIA

\*Corresponding Author Designation

DOI: <https://doi.org/10.30880/peat.2023.04.01.042>

Received 15 January 2023; Accepted 11 February 2023; Available online 11 February 2023

**Abstract:** The Wi-Fi Login Authentications System Using MikroTik aims to create a customized login portal for users accessing a MikroTik hotspot. MikroTik hotspots are a popular and widely used solution for providing wireless internet access in public places such as coffee shops, hotels, and airports [10]. The current login process for MikroTik hotspots is often viewed as a cumbersome and unappealing process for users. The login page will be providing a user-friendly and intuitive interface that simplifies the login process. The page will be designed with a focus on usability and accessibility, with the goal of making it easy for users to access the internet through the hotspot. The custom log-in page will include various features that are not present in the standard MikroTik hotspot log-in process [10]. The Wi-Fi Login Authentications System Using MikroTik project will be developed using web technologies such as HTML, CSS, and JavaScript to ensure compatibility with a wide range of devices and browsers. The project will be implemented on a MikroTik router, which will serve as the gateway for all incoming and outgoing traffic. Overall, the project aims to provide a seamless and efficient user experience for those accessing the hotspot, by creating a customized log-in portal that is easy to use and offers useful features. The custom log in page will not only improve the user experience but also help to increase the number of users that sign up to the hotspot, ultimately resulting in increased revenue for the hotspot operator [10].

**Keywords:** Mikrotik Hotspots, Wi-Fi Login Authentications System, Wireless Internet

### 1. Introduction

In today's world, internet access has become a necessity for both personal and professional use. However, providing secure and controlled access to a wireless network can be a challenging task for network administrators [1]. This is where MikroTik comes in. MikroTik is a Latvian company that designs and manufactures computer network equipment [8]. Their router hardware and software provide various features that can be used to create a secure and efficient login system for Wi-Fi networks. In

---

\*Corresponding author: [lina@uthm.edu.my](mailto:lina@uthm.edu.my)

2023 UTHM Publisher. All rights reserved.

[publisher.uthm.edu.my/periodicals/index.php/peat](http://publisher.uthm.edu.my/periodicals/index.php/peat)

this project, it will be utilizing MikroTik's hotspot feature to create a login portal for users to access the Wi-Fi network. Additionally, the authentication methods such as user login credentials and vouchers for added security [2]. The use of vouchers allows the network administrator to provide temporary access to guests or visitors without the need to create a new user account. This system will not only provide secure access to the network but also give network administrators the ability to monitor and control the network usage. I believe that this project will serve as a valuable resource for anyone looking to implement a similar system in their organization or community [10].

In this project, we will be providing an overview of MikroTik RouterOS, the features and capabilities that will be utilized in the project, and how it will be used to create a login portal and authenticate users. We will also be discussing the different authentication methods that will be implemented, such as user login credentials and vouchers, and how each method will be configured and used in the system. Additionally, we will be detailing the network configuration and setup, including the hardware and IP addressing used in the project, as well as the steps required to set up and configure the MikroTik router for the login system. We will then discuss the testing and evaluation methods used to test the functionality and performance of the system and explain how the system will be monitored and maintained once it is deployed. Lastly, we will be providing a conclusion, summarizing the project's goals and objectives, discussing the potential benefits and limitations of the system, and providing future directions for improvements and enhancements [10].

## 2. Materials and Methods

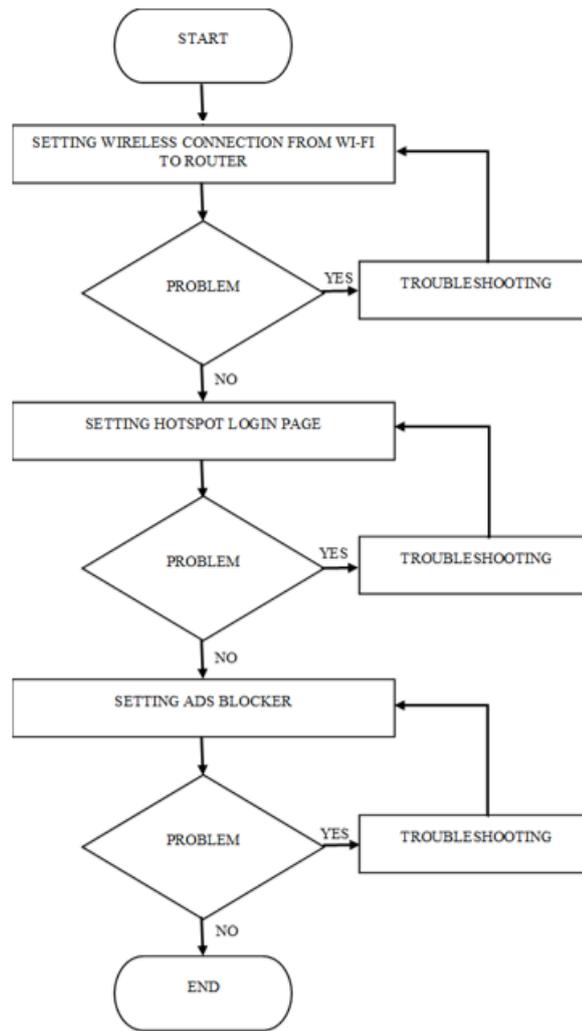
In this project, we will be utilizing the features of MikroTik HAP Lite RB941-2nD router, WinBox software and Visual Studio Code to create a login portal for users to access the Wi-Fi network. MikroTik HAP Lite RB941-2nD is a small wireless access point that provides an easy and affordable way to create wireless networks. The Ethernet network cable RJ45 will be used to connect the router to other network devices. WinBox is a software that will be used to remotely manage the MikroTik Router, and Visual Studio Code will be used for programming and scripting purposes in the project.

### 2.1 Materials

**Table 1: MikroTik HAP Lite RB941-2nD router specification**

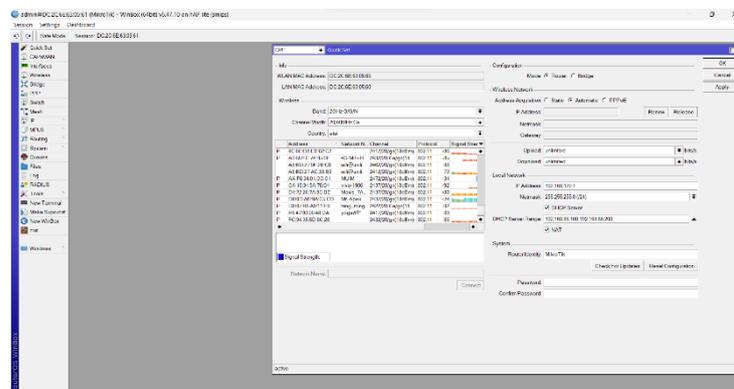
Product code	RB941-2nD
CPU nominal frequency	650 MHz
CPU core count	1
Size of RAM	32 MB
10/100 Ethernet ports	4
Wireless chip model	QCA9533
Wireless standards	802.11b/g/n
Power Jack	1
Supported input voltage	5 V - 5 V
Operating System	RouterOS
License level	4
Antenna gain DBI	1.5
CPU	QCA9533
Max Power consumption	3.5W
Storage type	FLASH
Storage size	16 MB

## 2.2 Methods



**Figure 1: Flowchart of the project**

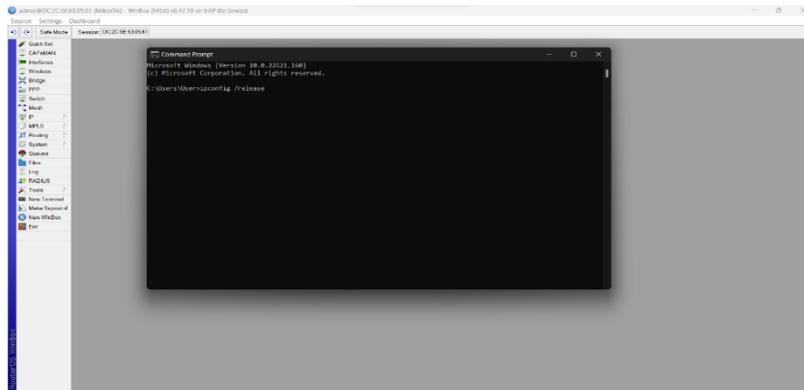
This project is split into some phases to as to realize the objectives. It is for guaranteeing the project development can be allotted with efficiency. The flowchart diagram shows the procedure to be enforced in keeping with the requirement of the project. Setting up a network security for the MikroTik router is the main half for this project.



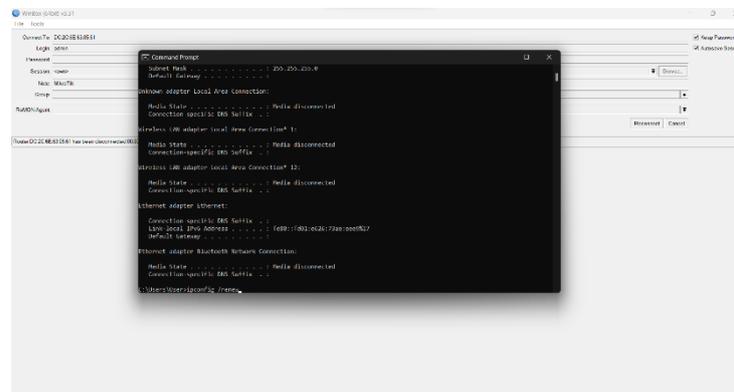
**Figure 2: Quick Set Tools**



specified IP address. This will prevent the ads server from being able to serve ads to devices connected to the network.



**Figure 6: Command prompt IP release**



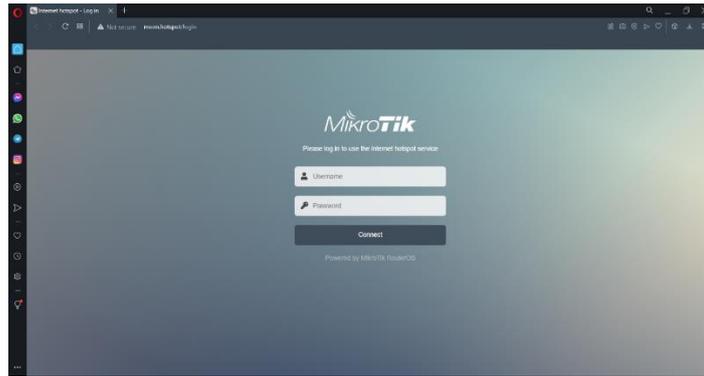
**Figure 7: Command prompt IP renew**

For troubleshooting, if there is still no internet connection, use the command prompt to release and renew the IP address. The command `ipconfig / release` and `ipconfig / renew` is used as shown in figure 6 and figure 7. After release and renew the IP address, `ping google.com` is used to check if there is internet connection. The Ookla speed test used to check internet connection on smartphone.

### 3. Results and Discussion

In this section of the project, it will be presenting the results of the implementation and evaluating the performance of Wi-Fi login system using MikroTik HAP Lite RB941-2nD router. The discussion of the test scenarios that were carried out and present the data and observations that were collected. Furthermore, this section will be providing a detailed analysis of the results and how they align with the project's goals and objectives.

#### 3.1 Results

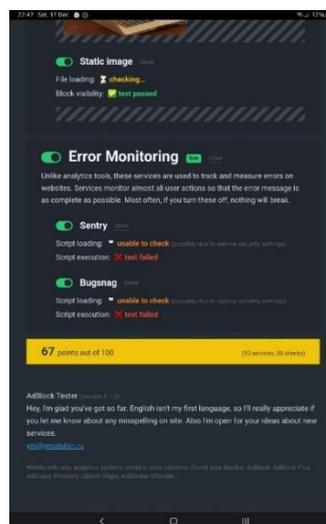


**Figure 8: Login page in computer browser**



**Figure 9: Login page in smartphone browser**

As shown in figures 4 and 5, the login page appears on the screen immediately after the device establishes a connection to the wireless network. After successfully connecting to the wireless network, the login page may not open immediately. However, a notification about this will appear in the top corner of the screen. Username and password can be registered in the winbox software.



**Figure 10: Ad Blocker Test**

Figure 6 indicates that the ad blocker successfully banned some of the adverts, but not all of them. Ads blockers provide a simple and effective way to limit the number of online ads you see. By blocking ads, the user will no longer be shown any ads when accessing websites or applications. This can significantly reduce data usage and prevent ads from distracting users. Ads blockers can also help protect the user’s personal data and browsing activity from being tracked by third-party websites and services.

### 3.2 Figures and Table

**Table 2: Internet Usages During Day and Night**

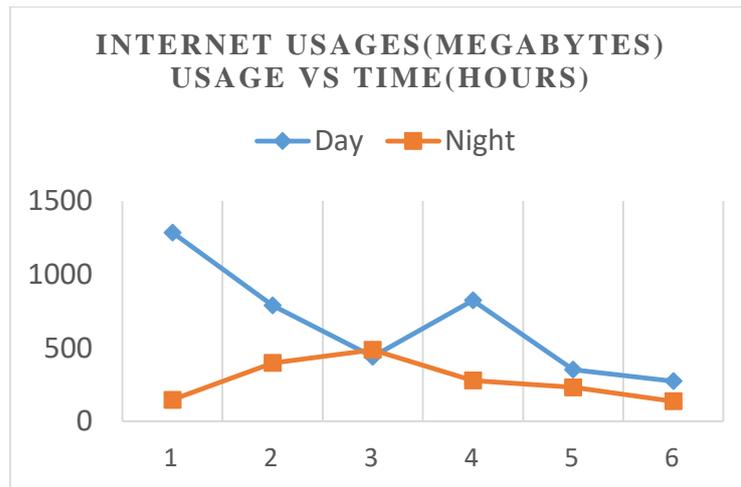
Hours	Day	Night
1	1285.4	146.23
2	789	397.4
3	439.8	486.56
4	823	278.39
5	351.72	231.48

**Table 3: Internet Usages During Weekday**

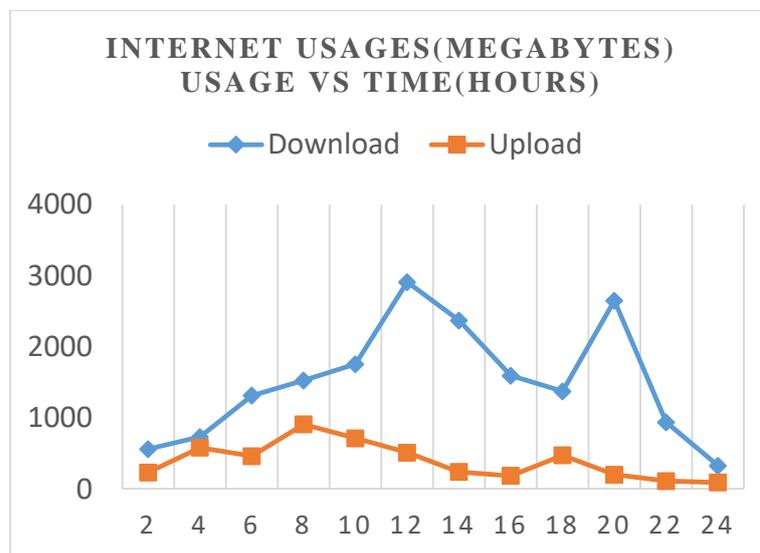
Hours	Download	Upload
2	561.27	232.1
4	731.98	581.5
6	1312.32	460.3
8	1525.2	908.9
10	1754.72	713.54
12	2909.5	511.28
14	2371.22	239.1
16	1593.8	185.6
18	1374.1	472.7
20	2648.9	201.3
22	937.8	111.7

**Table 4: Internet Usages During Weekend**

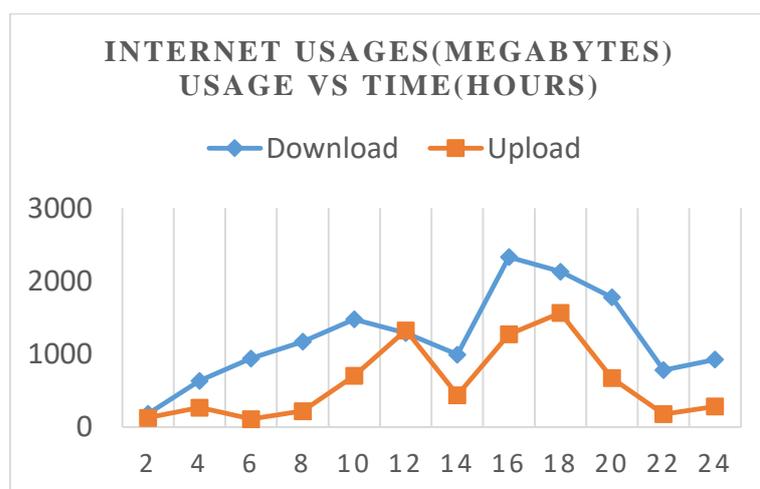
Hours	Download	Upload
2	182.96	128.3
4	636.48	268.11
6	942.17	110.4
8	1172.45	220.7
10	1477.3	703.8
12	1290.15	1326.79
14	993.6	437.9
16	2331.09	1271.37
18	2132.53	1564.3
20	1780.03	672.5
22	783.1	178.09



**Figure 11: Internet usage during day and night**



**Figure 12: Internet usage during weekdays**



**Figure 13: Internet usage during weekend**

Figure 11, 12 and 13 shows the internet usage for day and night, weekdays, and weekend. The graph displays the amount of data (megabytes) that is being used on a network over time (hours). Understanding how internet usage changes over time can provide valuable insights into usage trends and anomalies.

The graph shows a steady increase in internet usage during the daytime hours, when people are awake and using the internet for work or entertainment. Usage decreases during the night when most people are asleep. Additionally, the usage patterns change during the week and weekends. On weekdays, usage spikes at a particular time, indicating that people are using the internet for work-related activities during that time, however this trend does not occur on weekends.

The analysis of internet usage versus time provides valuable insights into how usage patterns change over the course of a day, week, and weekends. This information can be useful for network administrators in optimizing network performance and identifying and troubleshooting usage-related issues. The spike in usage during work hours suggests that most internet usage is likely related to work or school activities. Further research could be done to confirm this and to delve deeper into specific usage patterns.

#### 4. Conclusion

For the conclusion, the network security for MikroTik router is focusing on the safety for people to use the public Wi-Fi that been provided at any place. This network security configuration can be used at any version of MikroTik router because mostly all the MikroTik router are using RouterOS as their operating system. The main objective of this project is to create a public Wi-Fi network that are safe to use by any registered users has been achieved. The login authentication page that was designed using Visual Studio code can be used without any error. The network that has been configure will block all unnecessary and unsafe Ads with the Ads Block system. The network also has a user limit so that the internet speed will not drop drastically. The internet speed limit that has been set also work perfectly. The automatic cookie removal will ensure that all user information is removed. From the result, it can be concluded that the configuration of the MikroTik router will keep the user safe. Future modifications can be added to the configuration to increase the network security of the public Wi-Fi network.

#### Acknowledgement

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

#### References

- [1] A. Pratama, Agussalim, and F. Muhammad Reza, "Point-to-multipoint implementation on mikrotik router-based warehouses networks," in *Proceeding - 6th Information Technology International Seminar, ITIS 2020*, Oct. 2020, pp. 87–91. doi: 10.1109/ITIS50118.2020.9321045.
- [2] A. M. Khasanova, "Detection of Attacks on Wi-Fi Access Points," in *Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021*, Jan. 2021, pp. 28–31. doi: 10.1109/ElConRus51938.2021.9396420.
- [3] J. M. Ceron, C. Scholten, A. Pras, and J. Santanna, "MikroTik Devices Landscape, Realistic Honey pots, and Automated Attack Classification," Apr. 2020. doi: 10.1109/NOMS47738.2020.9110336.
- [4] F. Zhu, L. Liu, W. Meng, T. Lv, S. Hu, and R. Ye, "SCAFFISD: A Scalable Framework for Fine-grained Identification and Security Detection of Wireless Routers", doi: 10.1109/TrustCom50675.2020.00160/20/\$31.00.

- [5] R. Sharma, "Integration of Software Router with Wi-Fi for Enhanced Security," 2017 IEEE 7th International Advance Computing Conference (IACC), 2017, doi:10.1109/IACC.2017.14.
- [6] R. Ajami and A. Dinh, "Design a hardware network firewall on FPGA," in Canadian Conference on Electrical and Computer Engineering, 2011, pp. 000674–000678. doi: 10.1109/CCECE.2011.6030538.
- [7] Young-Ho Kim and Jeong-Nyeo Kim "Design of firewall in router using network processor". Electronic and Telecommunications Research Institute. (Accessed Jan. 7, 2023)
- [8] Mollick, P., Biswas, S., Halder, A., & Salmani, M. (2016). Mikrotik Router Configuration using IPv6. International Journal of Innovative Research in Computer, 4(2), 2001-2007.
- [9] Siahaan, M. L., Panjaitan, M. S., & Siahaan, A. U. (2016). MikroTik bandwidth management to gain the users prosperity prevalent. Int. J. Eng. Trends Technol, 42(5), 218-222.
- [10] Adam, M. S., Mohammed, I. K., Muhammad, K. M., & Abiodun, N. L. (2013). Internet authentication and billing (hotspot) system using MikroTik router operating system.