p-ISSN: 2723-6609 e-ISSN: 2745-5254
Vol. 5, No. 12 Desember 2024 http://jist.publikasiindonesia.id/

User Management and Authentication of Hotspot Using Mikrotik Hotspot Monitor at A Coffee Shop

Gunawan Budi Sulistyo[1*], Pudji Widodo, Noor Hasan[2]
Universitas Bina Sarana Informatika, Yogyakarta, Indonesia[1.2,3]
Email: gunawan.gnw@bsi.ac.id[1*], pudji.piw@bsi.ac.id[2], noor.nhs@bsi.ac.id[3]

*Correspondence

Keywords: Mikrotik; Hotspot; Authentication; Management; Mikhmon

ABSTRACT

This research aims to analyze the effectiveness of using the Mikrotik Hotspot Monitor in user authentication management in hotspot networks. User authentication challenges that include security and ease of management motivate the use of Mikrotik to improve system efficiency. The research method used is a qualitative approach with a case study. Data collection is done through interviews with users and managers and direct observation. The results showed that Mikrotik Hotspot Monitor is able to improve the security and efficiency of authentication management. Users find this method more straightforward than other methods, such as Radius. In conclusion, Mikrotik Hotspot Monitor is an effective solution for authentication management on hotspot networks by offering features that are easy to use and efficient in supporting internet service business needs.

Introduction

User authentication management in hotspot networks is something that cannot be ignored, especially in the context of increasing internet usage in various sectors, including education, business, and the public. According to data from the Indonesian Internet Service Providers Association (APJII) (2022), the number of Internet users in Indonesia will reach 202.6 million, with penetration reaching 73.7% of the total population . In this situation, hotspots have become one of the solutions for providing widespread internet access. However, as the number of users increases, the challenges in managing authentication also increase. Without a strong authentication system, security risks such as misuse of access, data theft, and cyberattacks become higher.

Along with the development of technology, hotspot systems have evolved from simply providing internet access to more complex platforms that require efficient management. Various hotspot management software technologies, such as Mikrotik Hotspot Monitor (MIKHMON), offer solutions to address these challenges. The use of Mikrotik in hotspot network management can improve access speed and network security (Khairullah et al., 2024).

The main challenges in user authentication management in hotspots include security, scalability, and management complexity. Security is a significant concern as hotspots are often the target of attacks, such as hacking and data theft. In addition, as the

number of users increases, the system must be able to handle simultaneous authentication without degrading performance. Many service providers have difficulty managing user data and ensuring that only authenticated users can access the network (Wibowo & Triraharjo, 2023). This suggests the need for a more systematic approach to authentication management.

Mikrotik Hotspot Monitor offers a comprehensive solution to these challenges. With features such as bandwidth management, voucher systems, and usage reports, Mikrotik allows administrators to manage the network more efficiently. The voucher system allows users to access the internet in a more controlled manner and can also reduce the risk of misuse. Mikrotik's use in simulating authentication management can improve security and operational efficiency (Iskhaq et al., 2021). Therefore, the Mikrotik Hotspot Monitor is an attractive option for service providers who want to improve user authentication management.

The primary purpose of this research is to analyze the effectiveness of using the Mikrotik Hotspot Monitor in user authentication management. By conducting this analysis, it is hoped that the advantages and disadvantages of the system can be found, as well as how this system can be optimized to improve user experience. Previous research by Danang and Setiawan (2021) shows that implementing a sound management system can increase user satisfaction, which in turn can increase customer loyalty. Therefore, this research will provide valuable insights for service providers in designing better authentication management strategies.

In addition to analyzing effectiveness, this research also aims to provide recommendations for service providers in improving user authentication management systems. These recommendations will be based on the results of the analysis and relevant case studies, as well as the practices that have been implemented in the two sites. By providing clear and measurable recommendations, it is expected that service providers can implement the necessary changes to improve security and efficiency in authentication management. Research by Romauli Romauli et al. (2024) emphasizes the importance of developing systems that are responsive to user needs, which will be one of the focuses in providing recommendations at the end of this research.

Method

This research uses a qualitative approach, which aims to understand and explore the user experience and effectiveness of authentication management on hotspot systems using Mikrotik Hotspot Monitor. A qualitative approach was chosen because it can provide deep insights into how users interact with the system and the challenges they face. According to Wibowo and Triraharjo (2023), qualitative research is beneficial in the context of information technology to explore user perceptions and factors that influence system use. In this case, researchers conducted interviews with users and hotspot managers to obtain more comprehensive data.

The approach used in this research is a case study, where researchers will focus on a Coffee Shop that will use Mikrotik Hotspot Monitor. With case studies, researchers

can evaluate system implementations directly and identify best practices and issues that arise in managing user authentication. This approach allows researchers to collect relevant contextual information, such as hotspot usage policies and user satisfaction levels, which are important for further analysis (Pramudita et al., 2014; Verma et al., 2021).

The location of this research will be one of the coffee shops in Yogyakarta. Yogyakarta was chosen because it is one of the cities with a high level of hotspot usage, especially among students and tourists. The Yogyakarta City Government, through the Yogyakarta City Informatics and Communication Office (Kominfosan), continues to expand public access to the internet by increasing the number of free public wifi locations. As of February 3, 2021, this free public wifi access is spread across 356 points throughout the city of Yogyakarta (Adminwarta, 2021; Susilo et al., 2023).

The subject selection criteria in this study include a variety of hotspot users in terms of age, educational background, and frequency of use. The researcher will select subjects who have used the hotspot service for a minimum of three months to ensure that they have enough experience to provide valuable insights. In addition, hotspot managers will also be involved as subjects, as they have different perspectives on the challenges and solutions in authentication management. By involving a variety of subjects, it is expected that the research results can reflect a more representative condition (Ardianto et al., 2018; Widyatama et al., 2023).

The primary data collection technique used in this research is interviews. These interviews will be conducted with hotspot users and managers to gather information about their experiences using the Mikrotik authentication system. Questions will be designed to explore various aspects, including ease of use, problems encountered, and features considered important. These interviews are analyzed to find key themes that emerge from the data. According to Iskhaq et al., (2021), interviews are an effective method for collecting qualitative data

In addition to interviews, researchers will also conduct direct observations at the research location. This observation aims to understand how users interact with the authentication system and how the hotspot manager manages user access. The researcher will record various aspects, such as the time taken for authentication, the number of users connected at any given time, and the manager's response to problems that arise. This observational data will provide additional context for the analysis conducted through interviews and help researchers understand the dynamics that occur in the field (Tavory, 2020; Tenggario & Lukas, 2011).

This research also involves collecting secondary data from relevant sources, such as hotspot managers' annual reports, internet usage data in Yogyakarta, and previous studies related to user authentication management. This secondary data will complement the information obtained from interviews and observations. By combining primary and secondary data, researchers can provide a more comprehensive and in-depth analysis of hotspot user authentication management (Wibowo & Triraharjo, 2023).

The data analysis method used in this research is thematic analysis. After the data is collected through interviews and observations, the researcher will identify the main themes that emerge from the data. This process involves coding the data and categorizing the information based on the similarities and differences found. The thematic analysis allows researchers to highlight key issues and provide a better understanding of user experience and authentication management challenges (Ardianto et al., 2018).

To ensure the accuracy and reliability of the data, the researcher compares information obtained from interviews, observations, and secondary data. In addition, the researcher will also conduct member checking, where the results of the initial analysis will be shared with several research subjects to obtain feedback and ensure that the interpretations made are in line with their experiences. This validation process is important to increase the credibility of the research results and provide a solid basis for the conclusions drawn (Iskhaq et al., 2021).

User authentication is the process of ensuring that individuals accessing a system or network are who they claim to be. In the context of hotspot networks, authentication is a crucial first step to control user access. This process usually involves using a username and password but can also include other methods such as tokens, biometrics, or two-factor authentication (2FA). According to Wibowo and Triraharjo (2023), effective authentication not only protects sensitive data but also increases user trust in the services provided.

In a hotspot environment, where multiple users can access the network simultaneously, the importance of authentication becomes even more apparent. Without proper authentication, the network can be vulnerable to abuse, such as illegal access and uncontrolled bandwidth usage. Data from Pramudita et al. (2014) shows that more than 65% of hotspot service providers experience problems with unauthenticated users, which negatively impacts service quality. Therefore, implementing a strong authentication system is necessary to maintain network integrity and security.

A hotspot is a geographical area where users can access the internet through a wireless network, usually by using devices such as laptops, smartphones, or tablets. The primary function of a hotspot is to provide fast and easy internet connectivity so that users can connect without having to use cables. Ardianto et al. (2018) explain that hotspots are often used in public places such as cafes, airports, and libraries, which allow internet access for anyone in the area.

Mikrotik is one of the popular network devices for hotspot management, offering various features that support user authentication and management. Features such as User Manager allow administrators to manage user accounts, monitor bandwidth usage, and set access restrictions. Mikrotik also supports various authentication methods, including RADIUS and captive portals, which makes it easy to integrate with existing systems. Rahardi et al. (2022) noted that the use of Mikrotik in hotspot management has proven effective in improving service quality and user satisfaction.

The advantages of using Mikrotik in hotspot management include relatively low cost compared to other solutions and flexibility in configuration and setup. However,

there are also some drawbacks, such as a steep learning curve for new users and complexity in the initial setup. According to Tenggario and Lukas (2011), although Mikrotik offers many features, users must have sufficient technical knowledge to maximize the potential of this device.

Several studies have been conducted to explore the effectiveness of bandwidth management and authentication in hotspot networks. For example, research by Rahardi et al. (2022) showed that implementing a sound authentication system can reduce bandwidth abuse by 40%. This shows that effective management not only protects the network but also improves user experience by ensuring that all users get fair access to network resources.

The Mikhmon and User Manager methods are two popular approaches to hotspot management using Mikrotik. Mikhmon, as a web-based application, offers a user-friendly interface for user management and network monitoring. Meanwhile, User Manager provides more in-depth control over account settings and authentication. The implementation of these two methods in a laboratory environment showed satisfactory results, with significant improvements in management efficiency and user satisfaction.

The implementation of this research uses the Network Development Life Cycle (NDLC) method to evaluate the effectiveness of the Mikrotik Hotspot Monitor (MIKHMON) in hotspot user management and authentication. NDLC is a systematic approach involving planning, design, development, and evaluation stages to ensure that technology solutions meet identified needs efficiently and effectively.

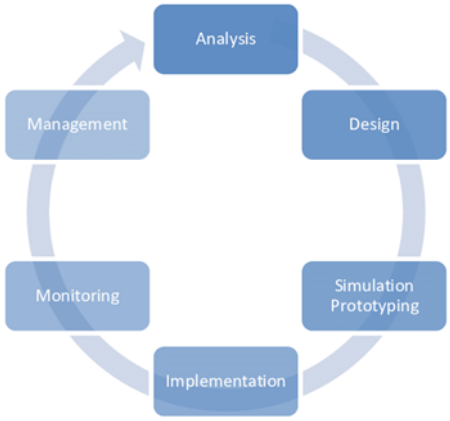

Figure 1. Network Development Life Cycle (NDLC)

1. Analysis and Planning

   At this stage, identification of system needs and mapping of existing problems in user management and authentication are carried out. The results of this need analysis are then used to design relevant evaluation criteria. A careful planning stage is critical to understand user needs and determine appropriate system specifications (Murtaji, 2022). Data was collected through interviews with hotspot managers and surveys of users to determine the main problems that need to be addressed.
2. Design

   The design stage involves creating a detailed plan for the implementation of MIKHMON, including technical specifications and monitoring schemes. The system design is based on the planning results and aims to ensure that the features of

MIKHMON can fulfill the identified management and authentication needs. The importance of a comprehensive design in facilitating system integration and performance optimization is well documented (Romauli et al., 2024).

3. Development

   In this phase, it is implemented according to the design that has been made. The development process includes system configuration, integration with existing hotspot infrastructure, and functionality testing. A practical development phase involves continuous monitoring and adjustments to address issues that may arise during implementation (Rizky et al., 2024).

4. Evaluation

   The final stage in the NDLC is evaluation, where the effectiveness of MIKHMON in user management and authentication is assessed based on the criteria established in the planning stage. Evaluation is conducted through analysis of usage data, user feedback, and system security testing. Evaluation results are used to provide recommendations for system improvements and upgrades. A comprehensive evaluation can identify the strengths and weaknesses of the system, and provide a basis for continuous improvement.

Results and Discussion

In this study, an analysis of the use of the Mikrotik Hotspot Monitor was carried out to evaluate the effectiveness and efficiency of the hotspot user authentication system. The Network Topology used in this research is as shown below:

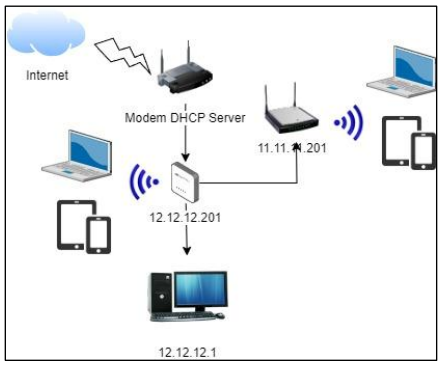

Figure 2. Network topology used

Mikrotik Hotspot Monitor is a tool that allows network administrators to manage user access to hotspot networks in a structured way.

The IP Address design used in the topology in Figure 2 is as follows.

Table 1. IP Address Design (Internet Protocol)

No.	Device Name	Port	IP Address
1	Mirotic RB951Ui-2HND Wireless Router	Eth1 (ISP Bridge)	192.168.0.21
		Eth1 Hotspot	12.12.12.1
		Mikhmon Server	11.11.11.1
		Hostspot Server	11.11.11.201
2	PC Admin	RJ45 NC	192.168.1.10

3.	Hand Phone /Laptop Client	wireless	192.168.2.10

Mikrotik Configuration

To configure the proxy to connect to the modem, it must be through a laptop/computer connected via a UTP cable with the following topology:

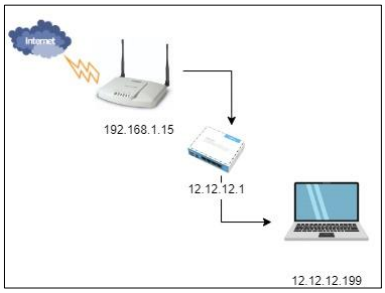

Figure 3. Initial topology configuration

After the UTP cable is connected from the modem to the proxy via Port 1 with IP 192.168.1.99, the Laptop can access/configure the proxy using the Winbox software, which is connected to the proxy via Port 2 with a UTP cable with IP 12.12.12.1. Then we configure from the beginning, namely for the client, through the IP Menu, DHCP Client, and just select ether1 on the interface, as shown below.

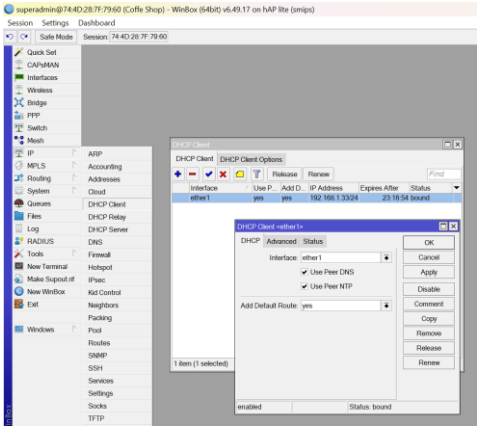

Figure 4. DHCP Client Configuration

Next, we need to complete the IP address for ether2 and bridge, as shown below:

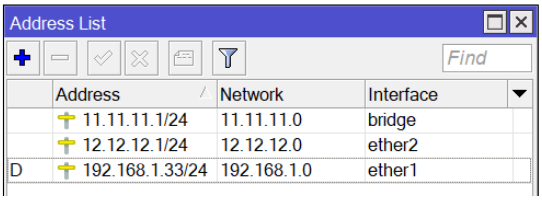

Figure 5. Ip Address Configuration

This configuration aims to set the client up to connect to the Internet via proxy with the rules we specify.

One of Richmond's advantages is that user authentication management can be done via Android or wireless mobile phones, provided that the proxy device is connected to the Internet.

Installing mikhmon using a mobile phone

Before installing Mikhmon on Android, it is necessary to prepare in advance, including AwebServer.apk, mikhmonv3-master.zip, PrinterShare.apk, and RAR.apk. First, we have to install Rar.apk to extract mikhmonv3-master.zip into cellphone storage. After it is successful, we can install AwebServer.apk and run it so that it appears like this:

Figure 6. Web server on mobile phone

The web server is used to run mikhmon, which is based on the PHP programming language. So after the web server is installed on the cellphone, the next step is to extract the mikhmon file to the root server or if it is in storage. Then, after starting the server, a link address will appear to direct to mikhmon.

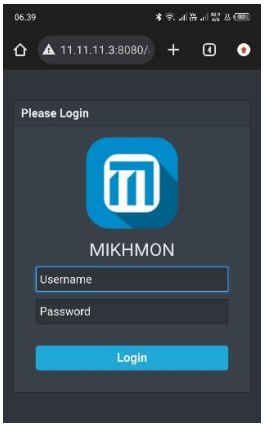

Figure 7. Login to mikhmon via Mobile

After successfully logging in, we will be faced with the mikhmon dashboard.

Figure 8. Mikhmon dashboard on mobile phone

Create a profile, where this is the character of the user for whom the password will be created. You can do this through the Hostspot-User Profile-Add Profile menu.

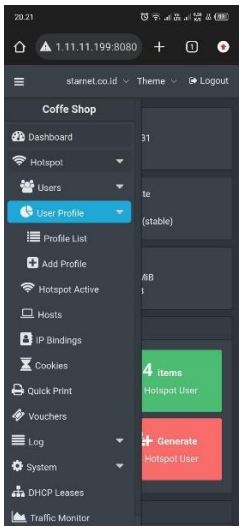

Figure 9. Adding User Profile

Next, we need to set the user's access rights after successfully logging in. Here, it is possible to make various settings, ranging from bandwidth speed to the price given. In this case, Coffe Shop will provide free internet vouchers to customers who come through the cashier. Every customer who orders drinks or food must pay first through the cashier, then get a free internet voucher for 6 hours, with an average internet speed of 2 Mbps.

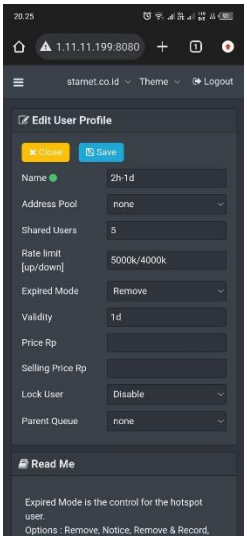

Figure 10. User Profile Configuration

The following table is inputted in the User Profile.

Table 2. User Profile

Name	Profile Name
Pool Address	none
Shared Users	The number of users who can access the Voucher code
Rate limit	The average speed is given.
Expired Mode	To have the Voucher code that has been used deleted by the proxy selected, Remove
Validity	Validity period
Price	The price is determined; if it is free, then enter 0.
Selling Price	Selling price
Lock User	Devices that have been logged in using the voucher cannot be used on other devices.
Parent Queue	none

Next, we need to print the generated voucher by going through the Hotspot-Users-Generate menu.

Figure 11. Generate User

The following description table is inputted in Generate User.

Table 3. Generate User

Qty	Number of Vouchers
Server	All
User Mode	Username = Password
Name Length	Character length
Prefix	null
Character	Random 1234
Profile	Please choose the one we have already created.

The sample results of the voucher generation are shown in the following table:

Table 4. Sample generate voucher

User	Passw	Profile	Time Limit	Data Limit	Comment
xss69	xss69	2h-1d	2h	5M/5M	vc-887-08.26.24-
sba76	sba76	2h-1d	Two h	5M/5M	vc-887-08.26.24-
vgk63	vgk63	2h-1d	2h	5M/5M	vc-887-08.26.24-
dga99	dga99	2h-1d	2h	5M/5M	vc-887-08.26.24-

Meanwhile, if it is printed, a QR code can be added in Richmond.

Figure 12. Mikhmon voucher

With the presence of Qrcode, users can choose either manual or scanned authentication.

Testing

At this stage, system testing will be carried out, covering aspects of Hardware, Software, and Brainware. This test aims to ensure that the configuration on Hardware and Software has functioned in accordance with the design that has been made. If an error is

found in the Hardware or Software, the problem can be immediately identified and corrected. The testing stages can be seen in the following figure:

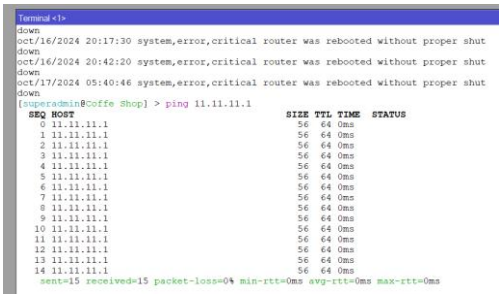

Figure 13. Ping Router to Modem test.

Next, test the connection using a cellphone to the login/authentication page.

Figure 14. Login/authentication page

The voucher code for authentication can be input manually through the voucher menu or QR code. The trial was conducted on ten people, with details of 5 people inputting the code manually and five people using the QRcode. To find out how much time is needed for authentication, the user is prepared in advance and distributed vouchers in a closed manner; after being divided, they are asked to authenticate together, both manually and with Qrcode. In this study, the speed results in authentication were obtained as follows:

Table 5. User Authentication Results

User	Methods	Authentication Time	SpeedTest
User 1	Qrcode	2,1	2 Mbps
User 2	Qrcode	3,5	1.8 Mbps
User 3	Qrcode	2,2	2 Mbps
User 4	Qrcode	2,5	1.8 Mbps
User 5	Qrcode	3,1	2.1 Mbps
User 6	Manual	3,2	2 Mbps
User 7	Manual	3,5	1.9 Mbps
User 8	Manual	3,6	2 Mbps
User 9	Manual	3,7	1.8 Mbps

User 10	Manual	2,9	1.9 Mbps

The table above shows that all users successfully authenticate using two methods: manual and QRcode. The speed obtained for the QRcode authentication method is faster than the manual, with an average internet speed of 2 Mbps.

Figure 15. Mikhmon traffic monitoring

Conclusion

Based on the results of the experiments that have been carried out, it can be concluded that user authentication management using Mikhmon is more straightforward, more effective, and more efficient than Radius. Mikhmon can easily manage Hotspot user management manually or automatically, as well as the voucher system, custom templates, and a more user-friendly display. Mikhmon offers desktop and website versions that you can upload to your hosting or server and later can be controlled remotely from a distance. In addition, Mikhmon also offers a mobile Android version, which will help run an internet voucher business for the neighborhood Net Coffee Shop and other public spaces, and it can be accessed from anywhere.

However, the effectiveness of MIKHMON implementation is highly dependent on the technical understanding of the staff in charge as well as the readiness of the network infrastructure. To support successful implementation, hotspot providers are advised to use a structured Mikrotik implementation guide, covering basic Mikrotik configuration, MIKHMON settings, and troubleshooting steps. This guide can be presented in the form of a manual document or an easy-to-understand video tutorial. In addition, technical training to staff responsible for network management also needs to be provided. This training should include a basic understanding of computer networks, Mikrotik configuration, and the use of MIKHMON to manage users and monitor network activity.

Hotspot providers should also conduct periodic evaluations of the authentication system to ensure that the configuration continues to meet user needs and evolving network challenges. This includes identifying potential issues, such as an increase in the number of users or new security threats. In addition, adequate technical support should be provided, both from within the hotspot provider and from the Mikrotik community. Extensive documentation needs to be prepared to support the staff's self-learning process, so that they can overcome obstacles on their own. With these steps, hotspot providers can optimize their MIKHMON implementation to improve the efficiency and quality of their network services.

Bibliography

Adminwarta. (2021). Kini Ada 356 lokasi Wifi Publik Gratis di Kota Yogyakarta. https://warta.jogjakota.go.id/detail/index/13353

APJII. (2022). No Title. APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Ardianto, F., Alfaresi, B., & Yuansyah, R. A. (2018). Jaringan Hotspot Berbasis Mikrotik Mengunakan Metode Otentikasi Pengguna (User). Jurnal Surya Energy, 2(2), 166–171.

Danang, D., & Setiawan, K. (2021). Pengaturan Billing Hotspot pada Sistem Jaringan RT/RW Net dengan Mikrotik Router OS. Jurnal Publikasi Teknik Informatika, 1(1), 12–22. https://doi.org/10.55606/jupti.v1i1.94

Iskhaq, G. M., Triyono, J., & Kusumaningsih, R. Y. R. (2021). Simulasi Manajemen Dan Autentikasi User Hotspot Menggunakan Mikhmon Server Pada Lab Basis Data Institut Sains & Teknologi Akprind Yogyakarta. Jurnal Jarkom, 9(2), 105–116.

Khairullah, K., Yoan Joupin, M., Marhalim, M., & Mahfuzhi, A. R. W. (2024). Perancangan Sistem Keamanan Jaringan Hotspot Mikrotik Router Os Login Menggunakan One-Time Password (OTP). JATI (Jurnal Mahasiswa Teknik Informatika), 8(5), 10953–10957. https://doi.org/10.36040/jati.v8i5.11059

Murtaji, A. (2022). Implementasi dan Modifikasi Data Rate di Wireless Mikrotik untuk Mengoptimalkan serta Menstabilkan Akses Jaringan Internet pada SMA Negeri 9 Banda Aceh. Karya Ilmiah Fakultas Teknik (KIFT), 2(4), ., 2(4), 153–168.

Pramudita, D. C., Pinandito, A., Eko Sakti, P., Kom, S., & Kom, M. (2014). Otentikasi dan Manajemen Pengguna Hotspot Router Mikrotik Menggunakan RADIUS dan PHP-MySQL. Universitas Brawijaya.

Rizky, M. A. H., Solehudin, A., & Nurkifli, E. H. (2024). Optimalisasi Bandwidth pada Jaringan Internet Menggunakan Metode Simple Queue dan Peer Connection Queue. JATI (Jurnal Mahasiswa Teknik Informatika), 8(4), 7856–7863. https://doi.org/10.36040/jati.v8i4.10497

Romauli, R., Subagja, I. K., Hakim, A., Ermanto, C., & Ali, A. (2024). Analisis Dampak Layanan Jak-Wifi dalam Rangka Meningkatkan Kepuasan Warga di Kelurahan Tanjung Priok Jakarta Utara. Mutiara: Multidiciplinary Scientifict Journal, 2(6), 422–431.

Susilo, R. M., Kusumaputra, F. R., Adiwijaya, M. H., Mayasari, R., Negara, R. M., & Astuti, S. (2023). Integration of Software-Defined Networking with Named Data Network for Implementing Forwarding Strategies in Wireless Networks. 2023 6th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 335–340. https://doi.org/10.1109/ISRITI60336.2023.10467947

Tavory, I. (2020). Interviews and Inference: Making Sense of Interview Data in Qualitative Research. Qualitative Sociology, 43(4), 449–465. https://doi.org/10.1007/s11133-020-09464-x

Tenggario, R. P., & Lukas, J. (2011). Manajemen Jaringan Wireless Menggunakan Server Radius. J. Tek. Komput, 19(1), 80–87.

Verma, P., Alam, A., Sarwar, A., Tariq, M., Vahedi, H., Gupta, D., Ahmad, S., & Shah Noor Mohamed, A. (2021). Meta-Heuristic Optimization Techniques Used for Maximum Power Point Tracking in Solar PV System. Electronics, 10(19), 2419. https://doi.org/10.3390/electronics10192419

Wibowo, A., & Triraharjo, B. (2023). Implementasi Manajemen dan Autentikasi Pengguna Hotspot Menggunakan Mikrotik Hotspot Management Mikhmon di Kedai Kopi Legalita. Sienna, 4(1), 27–39. https://doi.org/10.47637/sienna.v4i1.805

Widyatama, A., Agustia, D., Ardianto, A., & Soewarno, N. (2023). Effect of integrated reporting and environmental reputation on comprehensive decision-making non-professional Investors. Business: Theory and Practice, 24(2), 488–500. https://doi.org/10.3846/btp.2023.18537