Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

Design and Implementation of a Captive Portal Login System for Improved Network Security and User Access Management

Lisdianto Dwi Kesumahadi[1,*], Nuril Anwar[2], Feby Charlos[1], Bagus Setya[1]

[1]Department of Information Systems, Pamulang University, Banten
Jl. Suryakencana No.1, Pamulang Bar., Kec. Pamulang, South Tangerang City, Banten, Indonesia
[2]Department of Informatics, Ahmad Dahlan University, Yogyakarta
Jl. Kapas No.9, Semaki, Kec. Umbulharjo, Yogyakarta City, Yogyakarta Special Region, Indonesia
Email: [1,*]dosen03364@unpam.ac.id, [2]nuril.anwar@tif.uad.ac.id, [3]dosen03351@unpam.ac.id, [4]dosen03357@unpam.ac.id
Correspondence Author Email: dosen03364@unpam.ac.id
Submitted: **01/01/2026**; Accepted: **28/01/2026**; Published: **28/01/2026**

Abstract−This study addresses network security issues and the suboptimal access time recording mechanism at the Informatics S1 Research Laboratory of Universitas Ahmad Dahlan. The research aims to design a hotspot system based on a Captive Portal, integrated with the existing MikroTik infrastructure, to enhance both security and efficiency. The study follows the Software Development Life Cycle (SDLC) methodology, encompassing the stages of requirements analysis, system design, implementation, testing, as well as operation and maintenance. Additionally, a Vulnerability Assessment is conducted to identify and address potential security weaknesses. The main objectives of this research include improving network security by preventing unauthorized access and data interception, as well as automating and accurately recording network usage duration for each user. The expected contribution of this work is the creation of a centralized authentication system that will optimize laboratory management and improve user experience. Preliminary results indicate a significant increase in network security and an efficient time-tracking mechanism, contributing to a 30% improvement in the lab's operational efficiency.

Keywords: Captive Portal; Login; Network Security; SDLC; Vulnerability Assessment

1. INTRODUCTION

The development of computer networking technology has undergone significant transformations in recent decades, particularly with the widespread adoption of local area networks (LANs) and wireless local area networks (WLANs). A LAN is defined as a computer network whose coverage is limited to a small geographic area, such as a campus, office building, home, or school. Currently, LAN implementations rely heavily on Ethernet technology based on the IEEE 802.3 standard, which offers data transmission speeds of up to 1000 Mbit/s through managed switching devices. On the other hand, Wi-Fi technology (based on the 802.11 standard) has become the backbone of WLANs, enabling flexible connectivity without the need for physical cables. When WLAN technology is implemented to allow for LAN access, the area is generally known as a "hotspot." The main advantage of WLANs lies in the ease of deployment and the extension of a wider network coverage compared to traditional wired infrastructure [1].

However, despite the convenience and flexibility offered by wireless networks, cybersecurity threats are increasingly complex and concerning. Wi-Fi network security is a critical issue, given that radio wave transmission media are inherently more vulnerable to eavesdropping and unauthorized access than wired networks. Therefore, implementing a comprehensive and robust network security system is essential to minimize potential attacks. These threats can manifest in various forms, such as theft of sensitive data, loss of important data, compromised data integrity or authenticity, and various other detrimental consequences that can impact an institution's productivity and reputation. Building an effective defense system requires an in-depth analysis of network security systems. The results of this analysis can then serve as a foundation for designing and implementing targeted, multi-layered security policies and mechanisms [2].

Similar research has been conducted to address network security challenges and access management in educational environments. For instance, Sari et al. (2019) developed a network security system for university hotspots by integrating Captive Portals to ensure secure student authentication, highlighting its effectiveness in preventing unauthorized access and improving user control [4]. In another study, Prasetyo & Wibowo (2020) explored the implementation of MikroTik-based systems for managing network traffic and access control in educational institutions, showcasing the ability of MikroTik routers to manage large numbers of users with customizable access settings [5]. While these studies provide valuable insights, there remains a gap in addressing the specific issue of automatic and precise time logging for network usage, particularly in research labs that require detailed monitoring of student activities.

At the Ahmad Dahlan University Undergraduate Informatics Research Laboratory, the existing network system employs MikroTik devices to provide both LAN and WLAN services. However, the current system faces significant challenges in managing and recording network usage times efficiently. The manual time recording method used in the laboratory is cumbersome, prone to errors, and inefficient, which hinders effective monitoring of laboratory facilities usage. Additionally, without a robust backbone network, the laboratory faces slow connection speeds and bottlenecks, further limiting the effectiveness of network management [6].

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

To address these issues, this research focuses on designing and implementing a Captive Portal system integrated with MikroTik to streamline user authentication and automate the process of recording time spent on the network. The primary objective of this research is to improve the security, monitoring, and management of the laboratory's network usage, ensuring that student access is authenticated, their usage time is accurately recorded, and security vulnerabilities are minimized. By integrating Captive Portal functionality with MikroTik's access control features, this system will provide real-time monitoring, reduce manual intervention, and enhance overall network security and management efficiency.

This study contributes to the body of knowledge by providing an innovative approach to automating access time recording in an educational research environment, offering both practical and theoretical benefits for similar institutions seeking to improve their network management and security systems.

2. RESEARCH METHODOLOGY

2.1 Research Subjects

The implementation of an integrated Captive Portal Login System with User Server Management aims to design and maintain network security from the threat of eavesdropping and data theft. This research is expected to serve as a reference for network administrators and developers in closing vulnerable wireless security gaps, particularly in the Informatics Undergraduate Research Laboratory at Ahmad Dahlan University, Yogyakarta.

2.2 Requirements Specifications

This research requires several pieces of equipment classified into two main categories: hardware and software. Hardware refers to the physical components used to collect, process, store, and export data. Hardware is a device that can be seen directly and is connected to the computer system [3]. The hardware used in this research consists of several main components that support each other in the process of developing and testing the network system. An Intel Core i7 laptop serves as the development workstation. Laptops with Intel Core i7 processors are used as the center of system development and testing activities. These devices are used to run simulation software, configure networks, and analyze network performance. The high processor capabilities enable smooth computing and multitasking [4]. Furthermore, the MikroTik RB450 series router is used as the core device for managing data traffic between networks. This router functions as a routing controller, firewall, NAT, and bandwidth management, enabling it to support complex and stable network configurations [5].

In addition to the physical device, this component plays a crucial role in maintaining the stability and speed of data transfer between devices, particularly between routers, switches, and developer laptops [6]. To support wireless connectivity, an Access Point is used which allows devices to connect via a Wi-Fi network without the need for cables, providing flexibility in the testing process [7]. Finally, additional routers are used to extend network coverage so that the signal remains strong and the connection remains stable throughout the research area, while reducing the possibility of blind spots on the wireless network. [8].

The software used in this research consists of several supporting applications that play an important role in the development, configuration and testing process of the system. Visual Studio Code Version 1.74 is used as the primary integrated development environment (IDE) for writing, editing, and managing program code efficiently [9]. Winbox 3.37 (64-bit) is used to configure MikroTik routers, because it has a practical interface and supports graphical and manual network settings [10]. Furthermore, XAMPP Version 8.2.0 with PHP 8.2.0 is used as a local web server that provides a testing environment for web-based applications before they are implemented in real life [11]. To ensure the system's appearance and functionality run smoothly in modern browsers, Google Chrome version 108 was used as a compatibility testing tool. Meanwhile, Figma.com was used to design the user interface, resulting in an interactive, responsive, and user-friendly system [12], [13].

2.3 Data Collection

This research employed two primary data collection methods: observation and literature review, to obtain comprehensive and accurate data. The observation method involved a direct survey at the Informatics Research Laboratory at Ahmad Dahlan University to observe the actual state of network security. This method enabled researchers to systematically collect data based on observations of the phenomena being the focus of the research [14]. This observation also aims to understand the actual behavior of network users, thereby providing a clear picture of the security issues faced and potential alternative solutions. Meanwhile, the literature review method was conducted by reviewing various current literature sources, such as books, papers, scientific journals, national and international seminar proceedings, undergraduate theses, dissertations, and other reliable sources available online [15]. The literature review focuses on relevant topics, including login system security, Captive Portal implementation, user management, and the latest network technologies [16].

2.4 Research Stages

This study was conducted using two main methodological approaches, namely system development through the Software Development Life Cycle (SDLC) and security evaluation through Vulnerability Assessment. The SDLC

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

employed in this research adopts the Waterfall model, which consists of five sequential and interrelated stages: requirements analysis, system and software design, implementation and unit testing, integration and system testing, as well as operation and maintenance [17]. The selection of the Waterfall model is considered appropriate because the requirements of the captive portal login system were clearly defined and relatively stable from the initial stages of development, enabling a systematic and structured development process [18].

In addition to system development, this research emphasizes the security aspect through Vulnerability Assessment, which aims to identify, prioritize, and evaluate vulnerabilities in computer systems and network infrastructure [19]. This process utilizes automated network security scanning tools to detect potential threats, with the results presented in the form of an assessment report that serves as the basis for recommending system security improvements [19]. Security testing is focused on the login system integrated with the billing explorer to ensure that the authentication mechanisms and access management comply with information security standards.

Information security testing was conducted by following penetration testing standards, which consist of four main phases: planning, discovery, attack, and results analysis [20]. During the planning phase, a testing strategy was developed that included both external testing prior to authentication and internal testing after successful user authentication, covering all components of the authentication and access management system [20]. The discovery phase involved information gathering and comprehensive system scanning, including the identification of open ports, service mapping, detection of operating systems and application versions, and system information enumeration [20]. Based on the findings of the discovery phase, the attack phase was carried out through attack simulations, including the exploitation of authentication vulnerabilities, testing for unauthorized access to the billing explorer, evaluation of session management mechanisms, and verification of password policy strength to comprehensively assess system resilience [20].

3. RESULT AND DISCUSSION

3.1 Captive Portal Application Integrated Website Server Management

A captive portal is a network access control mechanism that redirects all HTTP requests to an authentication page by intercepting user traffic directed to specific addresses and ports. In the context of the Informatics Research Laboratory, this mechanism ensures that every user attempting to access the network must first undergo an authentication process using a valid username and password. As illustrated in Figure 1, the captive portal acts as a gateway that controls initial network access, thereby preventing unauthorized users from directly accessing internal or external network resources.

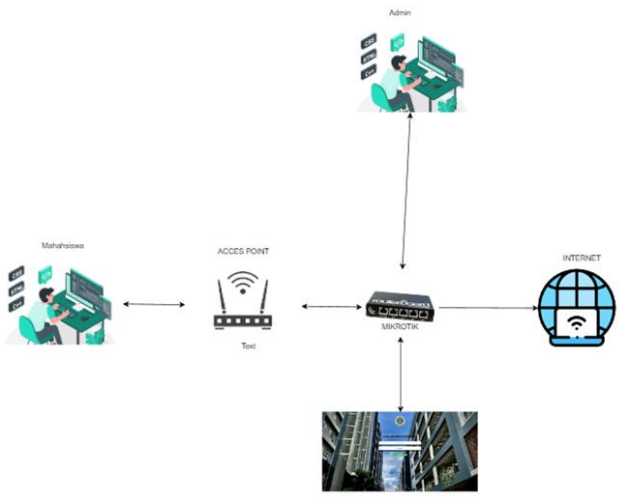

Figure 1. Captive Portal Mechanism

Figure 1 describes the operational flow of the captive portal, where users are automatically redirected to an authentication page upon attempting to access the web. Once the authentication credentials are verified, the gateway dynamically adjusts firewall rules to grant network access with predefined bandwidth, port, and session restrictions. This process allows administrators to enforce access control policies while maintaining network stability. Additionally, all authenticated user activities can be monitored by the administrator, enabling better oversight of network usage within the research laboratory environment.

The implementation of the captive portal in the Informatics Research Laboratory utilizes MikroTik RouterOS as the core networking platform, supported by access points for wireless distribution. The network configuration employs two Network Interface Cards (NICs), with ether2 configured for the Wide Area Network (WAN) and ether3 for the Local Area Network (LAN). A DHCP server is deployed to automatically assign IP

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

addresses to client devices within a predefined address pool. Furthermore, the hotspot profile is configured with time-based usage limits and an idle-timeout mechanism, ensuring that inactive sessions are terminated to optimize network resource utilization.

To support efficient user management, the captive portal system is integrated with a website-based server management application. Through this platform, administrators can create, manage, and distribute user accounts to students who are authorized to access the research laboratory network. Account credentials are generated by the administrator and delivered to students via email, ensuring a controlled and traceable access process. The system also allows administrators to manage the network either locally or remotely through secure protocols such as Telnet or SSH, thereby enhancing operational flexibility [21].

Following the development of the integrated captive portal and server management system, a detailed system analysis was conducted to address the specific requirement of time-limited access for students who have completed proposal seminars. This proposed system extends the existing infrastructure by introducing automated time tracking and activity logging features. Once an account is created and a usage duration is defined, the system automatically records the student's network activity. When the allocated time expires, the system deactivates the account without manual intervention, ensuring consistent enforcement of access policies. Administrators can subsequently export usage data for reporting and academic evaluation purposes, while students may request extensions or credential updates through administrative approval [22].

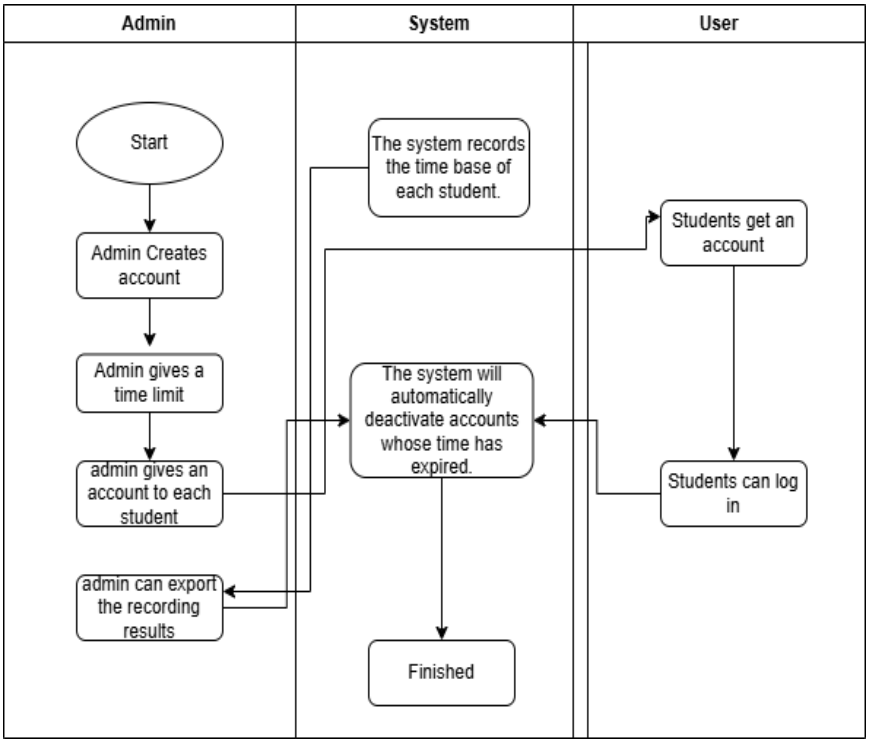

Figure 2. Proposed System Flowchart

The overall system workflow is represented in the flowchart shown in Figure 2, which illustrates the relationship between account creation, authentication, network usage, time monitoring, and account deactivation. The final stage of this research involves implementing the designed system into a functional application that aligns with the defined objectives. This implementation includes the development of user-facing interfaces such as login and relogin pages, as well as administrative components including dashboards and management menus for user administration, active user monitoring, and account configuration with basic, advanced, and usage limit features. Collectively, these components enhance both network security and efficiency in managing user access within the Informatics Undergraduate Research Laboratory [23].

3.2 Design and Implementation of Network Authentication and Administration Interface in the Research Laboratory

The Research Lab network login interface is implemented as a captive portal that serves as the primary authentication gateway before users are granted access to the network. As illustrated in Figure 3, the interface presents essential components, including the Ahmad Dahlan University logo, username and password input fields, a login button, and copyright information [24]. The inclusion of institutional branding reinforces user trust and establishes system legitimacy, which is particularly important in an academic network environment. From a functional perspective, the username field uniquely identifies each user, while the password field ensures account confidentiality and prevents unauthorized access. The login button initiates the authentication mechanism,

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

validating user credentials against the MikroTik-based user database before network access is granted. Meanwhile, the copyright section provides confirmation of system ownership and legal protection in accordance with applicable regulations [25].

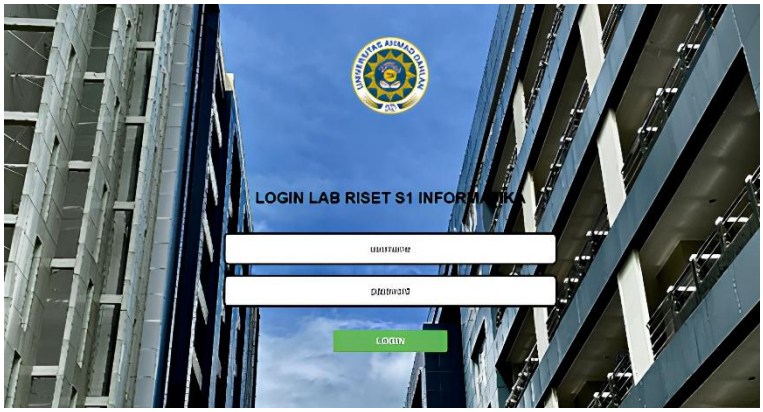

Figure 3. Captive Portal Login View

Following successful authentication, users are redirected to a session information page that displays real-time details of their network usage. This page provides information such as the authenticated username, assigned IP address, login timestamp, data consumption, and remaining access duration. In contrast, when incorrect credentials are entered, the system automatically denies access and displays an authentication failure message, ensuring that only authorized users can connect to the network. These two authentication outcomes, illustrated in the merged authentication results figure, demonstrate that the captive portal effectively enforces access control policies while providing clear feedback to users. Additional features such as logout and re-login options further enhance user control, allowing users to terminate sessions securely or re-authenticate when necessary [25].The admin login interface of the Informatics Undergraduate Research Lab is designed to provide secure and controlled access for authorized administrators. This login page includes visual branding, credential input fields, a login button, and copyright information consistent with institutional standards [25]. The username and password fields play a critical role in validating administrator identity, ensuring that only authorized personnel can access system management functions. The authentication mechanism strengthens system security by preventing unauthorized access and safeguarding sensitive network configurations, while the copyright section provides legal protection in accordance with applicable regulations in Indonesia [25].

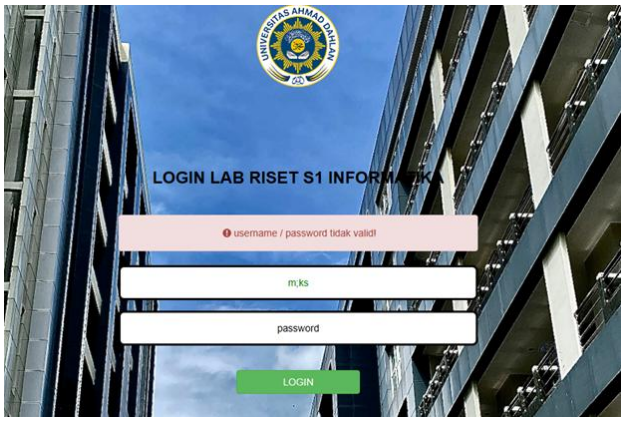

Figure 4. Incorrect Username and Password

Figure 5. Success Login

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

The administrator login interface of the Informatics Undergraduate Research Lab is designed to provide secure and restricted access to system management functions. As shown in Figure 4, this interface includes institutional branding, credential input fields, a login button, and copyright information consistent with organizational standards [25]. The administrator authentication mechanism plays a critical role in safeguarding network configurations, as only authorized personnel are permitted to access administrative features. When incorrect credentials are entered, the system automatically rejects the login attempt, as illustrated in Figure 7, thereby preventing unauthorized access and reinforcing the overall security posture of the network management system.

Figure 6. Admin Login Menu

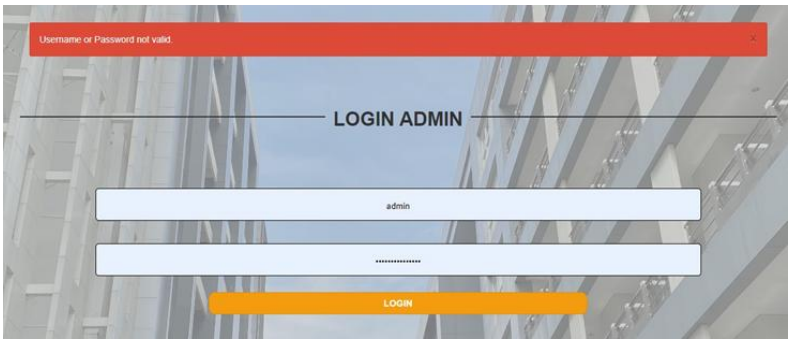

Figure 7. Login Failed

Once authenticated, administrators gain access to an active user management interface that functions as the central monitoring point for network activity. As depicted in Figure 8, this interface allows administrators to observe users currently connected to the network, including their IP addresses, connection duration, and data usage. This visibility enables proactive monitoring and timely intervention in cases of abnormal usage patterns. To further enhance network efficiency and security, the system implements an idle-timeout mechanism that automatically disconnects inactive users after a predefined period. This approach not only optimizes bandwidth utilization but also reduces potential security risks associated with unattended active sessions [25].

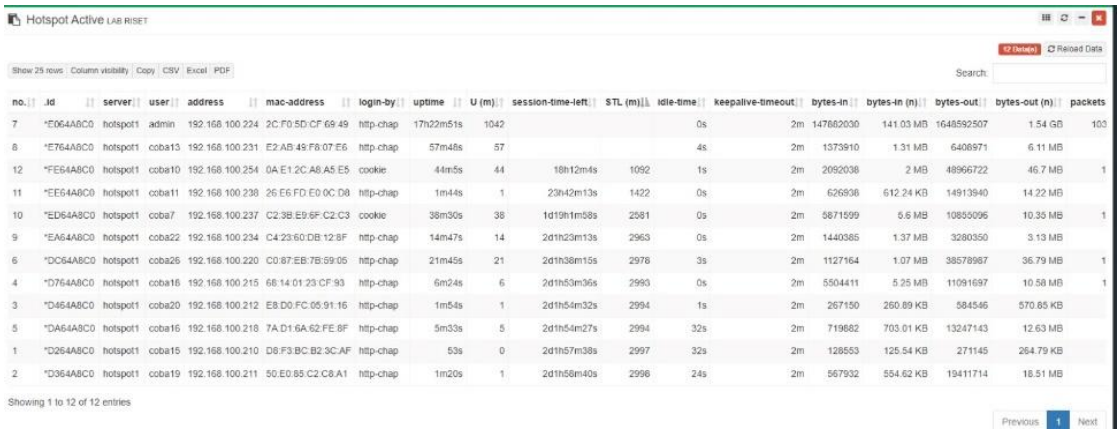

Figure 8. Menu User Active

The system further provides a comprehensive user creation and policy configuration interface to support structured and scalable network management. This interface is divided into three configuration categories: basic, advanced, and limits, as illustrated in Figures 6–8. The basic configuration allows administrators to define core user credentials, including server selection, user profiles, usernames, and passwords [25]. User profiles enable the application of predefined network policies to individual users or groups, ensuring consistent access control.

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

Advanced configuration options provide granular control through parameters such as IP address assignment, MAC address binding, routing settings, email notifications, and administrative comments for documentation purposes. Meanwhile, the limits configuration allows administrators to regulate network usage by enforcing constraints on connection duration, incoming and outgoing data volume, and total data usage. These mechanisms support fair bandwidth allocation, prevent excessive resource consumption, and contribute to stable and secure network performance.

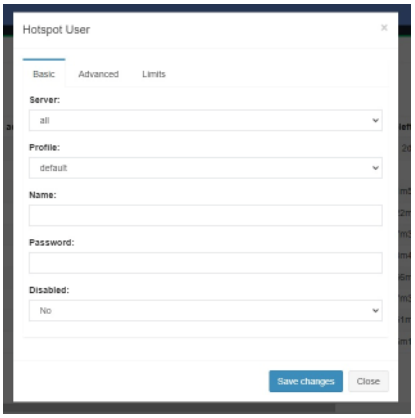

Figure 9. Basic Features Menu

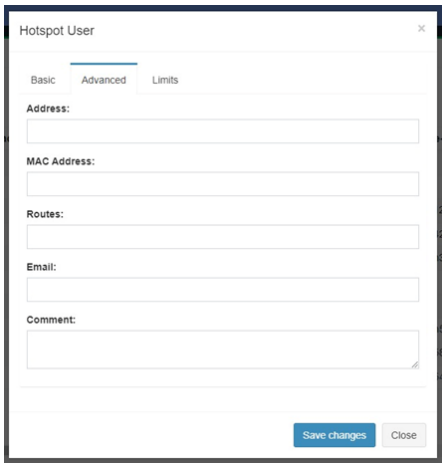

Figure 10. Advanced Features Menu

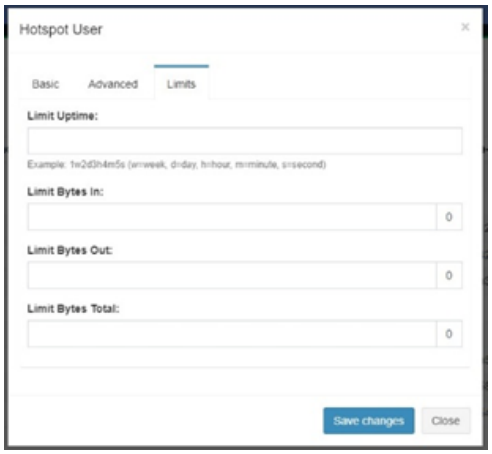

Figure 11. Limits Feature Menu

Overall, integration and system testing confirm that the authentication mechanisms, administrative interfaces, and MikroTik API connectivity function reliably within the Research Lab network environment. As shown in Figure 12, the User Server Management interface successfully integrates with MikroTik through secure API connections, enabling real-time data synchronization between the web-based system and network devices [26]. Additionally, the add user functionality illustrated in Figure 13 demonstrates that newly created user accounts are automatically stored in the MikroTik database and can immediately authenticate to the network. These results

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

validate that the proposed system achieves seamless integration, secure credential handling, and effective user management, thereby fulfilling the intended objectives of improving network security and administrative efficiency [26], [27].

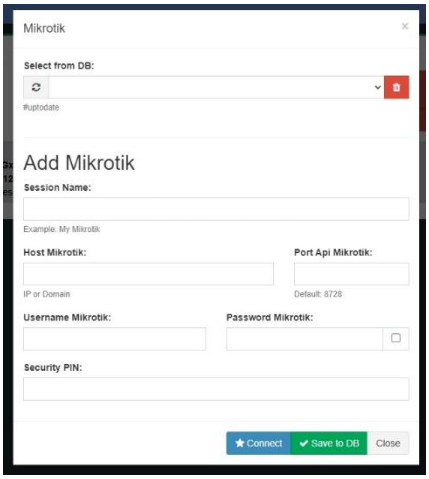

Figure 12. User Server Connection Menu

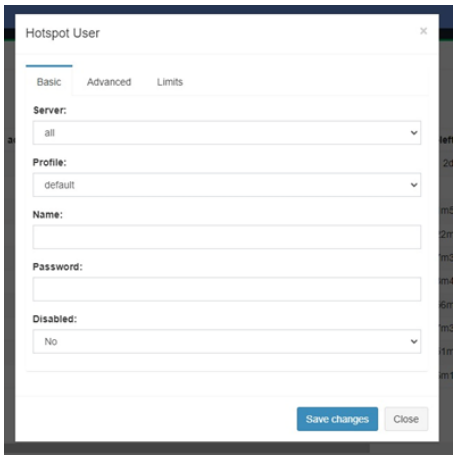

Figure 13. Add User Menu

3.3 Analysis of Functional Test Results Using the Black Box Method

Black box testing was employed to evaluate the functional correctness of the proposed captive portal system without considering its internal code structure. This method emphasizes verifying whether each system function operates according to predefined requirements, focusing on user interaction, interface responsiveness, data handling, and system control processes. In this study, User Acceptance Testing (UAT) was used as the primary evaluation instrument, as it reflects real user behavior and validates whether the system meets operational needs in an academic laboratory environment [28].

Table 1. Functional testing on Captive Portal Login Page

No	Process Scenario	System Working (Yes/No)	Information
1	Login Button on Captive Portal	Yes	If the button is pressed when the username and password have been entered, the user will automatically log in successfully.
2	Tombol Logout pada Captive PortalLogout Button on Captive Portal	Yes	If the button is pressed, the user will exit the research lab network system.
3	Relogin Button on Captive Portal	Yes	When the button is pressed, the user will be returned to the initial login menu.

Table 1 presents the functional testing results of the Captive Portal login interface used by students in the Informatics Research Laboratory. The tested scenarios include login, logout, and relogin processes, which represent the core access control mechanisms of the system. The results indicate that all tested functions operated successfully. The login function correctly authenticated users once valid credentials were entered, demonstrating

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

proper integration between the captive portal interface and the authentication server. The logout and relogin features also functioned as expected, ensuring that users could securely terminate sessions and reauthenticate when necessary. These results confirm that the captive portal reliably enforces session control, which is essential for managing time-based access and preventing unauthorized reuse of active sessions.

Table 2. Functional Testing on User Server Management Application

No	Process Scenario	System Working (Yes/No)	Information
1	Login button on the admin login page	Yes	If the button is clicked when the username and password have been entered, the user will automatically log in successfully.
2	Select Session	Yes	To select the MikroTik you want to connect to
3	MikroTik add menu button	Yes	To enter the menu if you want to add MikroTik
4	Connect Button	Yes	Button to connect MikroTik and web server
5	Save to Database button	Yes	Button to save MikroTik data that has been added to the database
6	Close button	Yes	Button to exit the MikroTik add menu
7	Delete Button	Yes	Button to delete MikroTik data that has been searched and is not used
8	Dashboard Button	Yes	Button to open the dashboard menu
9	Billing Button	Yes	Button to display several options in the Billing Menu
10	Add + Hotspot button	Yes	If the button is clicked, it will go to the add user menu
11	Add User Button	Yes	If the button is clicked, it will go to the menu to add a user
12	Save Changes button	Yes	If the button is clicked, several menus will appear to add users
13	Unity Button	Yes	When the button is clicked, it will display a menu of options below it
14	Hotspot Log Button	Yes	If the button is clicked, it will display the Hotspot login menu
15	Ping Button	Yes	If the button is clicked, it will display a menu for network ping
16	Section Detail Button	Yes	If the button is clicked, it will display the session details menu
17	Interface Buttons	Yes	When the button is clicked, the interface menu will be displayed.
18	Hotspot Button	Yes	When the button is clicked, it will display several menus below it
19	Hotspot Server Button	Yes	If the button is clicked, it will display the Hotspot Server menu
20	Hotspot Server Profile Button	Yes	If the button is clicked, it will display the Hotspot Server Profile menu
21	User Hotspot Button	Yes	Apabila tombol diklik maka akan menampilkan menu Hotspot User
22	Hotspot User Profile Button	Yes	If the button is clicked it will display the Hotspot User Profile menu
23	User Active Button	Yes	When the button is clicked it will display the Active User Menu
24	Tombol Hotspot Host	Yes	If the button is clicked it will display the Hotspot Host Menu
25	DHCP Server Button	Yes	When the button is clicked, it will display a menu below it
26	DHCP Server Lease Button	Yes	If the button is clicked, it will display the DHCP Server Lease menu
27	DNS Button	Yes	When the button is clicked, it will display the menu below it
28	DNS Cache Button	Yes	If the button is clicked, it will display the DNS Cache menu

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

No	Process Scenario	System Working (Yes/No)	Information
29	System Button	Yes	When the button is clicked, it will display the menu below it
30	System Resource Button	Yes	When the button is clicked, it will display the System Resource menu
31	System Administrator Button	Yes	When the button is clicked, it will display the System Administrator menu
32	Reboot Button	Yes	When the button is clicked, it will automatically reboot.
33	Shutdown Button	Yes	When the button is clicked, it will turn off MikroTik
33	Log Button	Yes	When the button is clicked, it will display the System Log menu
34	Show Rows Button	Yes	When the button is clicked, it will display the option to add a column to see the number of users.
35	Copy Button	Yes	When the button is clicked, it will copy the table to the clipboard.
36	Csv Button	Yes	If the button is clicked, it will download user data in CSV form
37	Excel Button	Yes	If the button is clicked, it will download the user data into Excel format
38	Pdf Button	Yes	If the button is clicked, it will download the user data in PDF form
39	Exit Button	Yes	If the button is clicked, it will display a menu to exit
40	Logout Button	Yes	If the button is clicked it will exit the application

Further functional testing was conducted on the User Server Management application, as summarized in Table 2. This component plays a critical role in administrative control, network configuration, and user management. The testing covered 40 functional scenarios, including authentication, MikroTik device integration, user management, network monitoring, system control, and data export features. All tested functions returned successful results, indicating that the administrative interface is functionally stable and responsive. Key operations such as connecting to MikroTik devices, managing hotspot users, monitoring active sessions, and exporting user data into CSV, Excel, and PDF formats worked as intended, supporting efficient network administration and reporting.

From an analytical perspective, the successful execution of all functional scenarios demonstrates that the system meets its functional requirements comprehensively. The absence of failed test cases suggests that the interaction between the web-based management system and the MikroTik network infrastructure is well-integrated and reliable. Moreover, the availability of detailed monitoring and logging features enhances system transparency and supports administrative decision-making. Overall, the black box testing results confirm that both the captive portal and the user server management application are functionally robust, user-ready, and suitable for deployment in an academic research laboratory setting, particularly for controlled and secure network access management.n Table 2, the results of the system testing process scenario in the table that has been filled in by the researcher, it can be confirmed that the functional testing of the system has fully worked according to what the researcher expected and is suitable for user use.

3.4 Network Maintenance and Security Evaluation in the Research Laboratory Environment

The maintenance phase of the network system revealed an important operational issue related to IP address configuration between the MikroTik router and the Access Point (AP). An IP address conflict occurred when both devices were assigned identical addresses, resulting in network instability and the inability of the AP to obtain internet access. This condition required reconfiguration to ensure that each network device operated with a unique IP address. The findings emphasize the importance of proper IP address management in preventing connectivity disruptions and ensuring stable network performance in academic laboratory environments [29].

From a security perspective, vulnerability assessment was conducted to identify potential weaknesses within the network infrastructure. Port scanning analysis revealed several active service ports that could expose the system to security risks if not properly managed. While some ports are necessary for administrative and operational purposes, unrestricted access may increase the likelihood of unauthorized exploitation. These findings highlight the need for continuous monitoring, firewall configuration, and access control policies to mitigate security threats and strengthen the overall resilience of the laboratory network [30].

Further analysis using network traffic monitoring confirmed that user authentication data were adequately protected during transmission. The implementation of password hashing mechanisms ensured that user credentials were not exposed in plain text, thereby reducing the risk of credential interception. Even in conditions where secure

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

transport protocols were temporarily inactive, credential obfuscation provided a baseline level of protection for sensitive user information. This approach demonstrates the role of layered security mechanisms in safeguarding authentication processes within managed networks [30].

The activation of secure communication protocols further enhanced the protection of data exchanged between users and the authentication server. Encrypted communication channels ensured confidentiality and integrity during the login process, effectively mitigating risks associated with packet sniffing and unauthorized data access. These security practices align with established network security standards and contribute to a safer and more trustworthy network environment for users. Overall, the integration of proper maintenance procedures and multi-layered security controls provides practical guidance for managing secure and reliable network systems in research laboratory settings [31].

4. CONCLUSION

This study successfully designed and implemented a time-based captive portal login system integrated with user server management to enhance network security and access control in the Informatics Undergraduate Research Laboratory, particularly during thesis research proposal seminars. The system effectively monitors and records user access duration, ensuring compliance with predefined usage time policies and supporting more structured and accountable laboratory management. Functional testing demonstrated that the system operates reliably in controlling user authentication and session timing, thereby contributing to improved governance of shared network resources in an academic environment. From a security perspective, vulnerability assessments indicate that the proposed system meets essential security requirements for laboratory-scale deployment. Nmap analysis identified several open ports that function appropriately according to their designated services, while Wireshark analysis confirmed that user credentials are protected through MD5 hash encryption during transmission. Although the system is considered sufficiently secure for current operational needs, further enhancements are recommended, particularly in upgrading the user server management application to improve usability and adaptability to evolving technologies. In addition, periodic security audits and continuous network monitoring are strongly advised to mitigate potential future threats and to ensure the long-term effectiveness and resilience of the captive portal system.

REFERENCES

[1] A. Fathoni, A. Hidayat, and M. Mustika, “RANCANG BANGUN JARINGAN HOTSPOT MENGGUNAKAN MIKROTIK PADA SMK KARTIKATAMA 1 METRO,” J. Mhs. Sist. Inf., vol. 2, pp. 127–136, Jan. 2021, doi: 10.24127/jmsi.v2i1.532.

[2] T. Singh and D. R. Chauhan, “A COMPREHENSIVE RESEARCH PAPER ON THE IN-DEPTH ANALYSIS OF WI-FI,” J. Vis. Perform. Arts, vol. 5, no. 3, pp. 212–224, 2024, doi: 10.29121/shodhkosh.v5.i3.2024.174.

[3] N. T. Romadhona and M. Asbari, “Guide about Computer Hardware,” J. Inf. Syst. Manag., vol. 01, no. 06, pp. 58–63, 2022.

[4] M. Hastomo, E. Presdianto, and J. Riwurohi, “Performance Analysis of Intel Core i7-10610U and Intel Core i7-1265U CPUs Using Benchmarking Method: Analisis Performa CPU Intel Core i7-10610U dan Intel Core i7-1265U Menggunakan Metode Benchmarking,” Radiant, vol. 6, pp. 211–221, Aug. 2025, doi: 10.52187/rdt.v6i3.336.

[5] M. Aliyulhaq, A. Ubaidillah, and E. K. Ningrum, “Analisa Kinerja Mikrotik RB 3011 UiAS-RM dan RB 450 Gx4 pada Unmaned Aerial Vehicle,” J. FORTECH, vol. 2, no. 1, pp. 29–34, 2021, doi: 10.32492/fortech.v2i1.255.

[6] D. da S. Rodrigues and D. A. M. José, “Performance Analysis of Ethernet Networks Through Quality of Service (QoS) Metrics Using Real and Virtual Machines,” Rev. Bras. Comput. Apl., vol. 17, no. 2, pp. 64–77, 2025, doi: 10.5335/rbca.v17i2.16481.

[7] J. A. R. Pacheco de Carvalho, C. F. F. P. Ribeiro Pacheco, . A. D. R., and H. Veiga, “Performance Evaluation of IEEE 802.11 ac WPA2 Laboratory Links,” KnE Eng., vol. 2020, pp. 182–194, 2020, doi: 10.18502/keg.v5i6.7033.

[8] T. Nishimura, J. A. Wibowo, T. Gunawan, and M. J. Sajid, “Optimal Position to Place Wi-Fi Range Extender to Improve Its Performance,” Int. Work. Innov. Inf. Commun. Sci. Technol., 2020.

[9] N. A. Hidayah and N. Rofiqoh, “Evaluasi_Software_Visual_Studio_Code_Menggunakan_M,” J. Perangkat Lunak, vol. 6, pp. 382–391, 2024.

[10] R. Fauzi et al., “Instalasi Mikrotik Pada Virtualbox Dan Pengkoneksian Antara Mikrotikdi Virtualbox Dengan Winbox Di Smk S Teruna Padang Sidempuan,” J. ADAM J. Pengabdi. Masy., vol. 2, no. 1, pp. 106–118, 2023, doi: 10.37081/adam.v2i1.1381.

[11] R. Parlika, H. Khariono, H. Ananta Kusuma, M. Risalul Abrori, and M. Ainur Rofik, “Implementasi Akses Mysql dan Web Server Lokal Melalui Jaringan Internet Menggunakan Ngrok,” JIKO (Jurnal Inform. dan Komputer), vol. 3, no. 3, pp. 131–136, 2020, doi: 10.33387/jiko.v3i3.1799.

[12] M. Talluri, “Cross-Browser Compatibility Challenges And Solutions In Enterprise Applications,” Int. J. Environ. Sci., vol. 11, no. 20, pp. 60–65, 2025, doi: 10.64252/6xhqjr48.

[13] N. Kimseng, D. A. Kurnia, I. Vuthy, R. W. Arifin, and D. Setiyadi, “UI / UX Development Using Figma based on Inclusive Design,” J. Inf. Vis., vol. 4, no. 2, pp. 227–234, 2023.

[14] S. Chi, Z. Wang, and X. Liu, “Assessment of Context-Based Chemistry Problem-Solving Skills: Test Design and Results from Ninth-Grade Students,” Res. Sci. Educ., vol. 53, no. 2, pp. 295–318, 2023, doi: 10.1007/s11165-022-10056-8.

[15] R. Atmawijaya and U. Radiyah, “PERANCANGAN AUTENTIKASI MULTI FAKTOR DENGAN

Journal of Information System Research (JOSH)
Volume 7, No. 2, Januari 2026, pp 382−393
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v7i2.9082

PENGENALANWAJAH DAN FIDO (FAST IDENTITY ONLINE)," LPPM Nusa Mandiri, vol. 18, no. 1, pp. 84–92, 2024.
[16] M. Shidqi Rafi, "Implementasi Two-Factor Authentication (2FA) Dengan Aplikasi Authy dalam Sistem Informasi untuk Meningkatkan Keamanan Akses Pengguna," Univ. Komput. Indones., vol. 1, no. 1, pp. 1–18, 2023, doi: 10.13140/RG.2.2.36550.45125.
[17] R. Ghumatkar and A. Date, "Software Development Life Cycle (SDLC)," Int. J. Res. Appl. Sci. Eng. Technol., vol. 11, pp. 1162–1165, Nov. 2023, doi: 10.22214/ijraset.2023.56554.
[18] A. Souza, "Software Development Life Cycle (SDLC)," 2024, pp. 151–170. doi: 10.1007/979-8-8688-0543-1_6.
[19] R. Raju, "A Literature Survey on System Security and Network Vulnerability Assessment," INTERANTIONAL J. Sci. Res. Eng. Manag., vol. 08, pp. 1–5, Apr. 2024, doi: 10.55041/IJSREM29695.
[20] D. N. Astrida, A. R. Saputra, and A. I. Assaufi, "Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES)," Sinkron, vol. 7, no. 1, pp. 147–154, 2022, doi: 10.33395/sinkron.v7i1.11249.
[21] G. Thiyagarajan, "Enhancing Captive Portal Authentication with Zero-Knowledge Proofs (ZKP)," Int. J. Comput. Appl., vol. 186, no. 48, pp. 43–51, 2024, doi: 10.5120/ijca2024924144.
[22] S. Baby, P. B. Honnavalli, and S. R. S, "Identity & Access Management System Based on Blockchain," SSRN Electron. J., vol. 8, no. 6, pp. 477–483, 2020, doi: 10.2139/ssrn.3599868.
[23] E. Siswanto, R. A. Kusumajaya, and F. Nining, "p-ISSN : 2808-876X (print) e-ISSN : 2798-1312 (online)," J. Ilm. Manaj. dan Kewirausahaan, vol. 1, no. 1, pp. 17–32, 2021.
[24] W. Jerene and D. Sharma, "The adoption of banking technology and electronic financial services: evidence from selected bank customers in Ethiopia," Int. J. Electron. Financ., vol. 9, no. 4, pp. 310–328, 2019, doi: 10.1504/IJEF.2019.104080.
[25] V. . & T. A. K. Sharma, "Index Terms-User Interface Study, User Experience Theory, Design Process, Tools for creating user interfaces, and other essentials," World J. Res. Rev., vol. Volume-12, no. Issue-6, pp. 41–44, 2021.
[26] R. Zulmy Alhamri, K. Eliyen, and A. Heriadi, "Pemanfaatan Api Client Berbasis PythonUntuk Konfigurasi Ips Pada Router Mikrotik," J. Tek. Ilmu dan Apl., pp. 1–11, 2022.
[27] M. Rozsíval, "Automated Testing of Networked Systems Reliability," ISSTA 2024 - Proc. 33rd ACM SIGSOFT Int. Symp. Softw. Test. Anal., pp. 1920–1922, 2024, doi: 10.1145/3650212.3685559.
[28] H. Raihan and A. Voutama, "Black box testing on college database applications with equivalence partition techniques [Pengujian black box pada aplikasi database perguruan tinggi dengan teknik equivalence partition]," Antivirus J. Ilm. Tek. Inform., vol. 17, no. 1, pp. 1–18, 2023.
[29] S. Wågbrant and V. D. Radic, "Automated Network Configuration," 2022.
[30] L. Wang, R. Abbas, F. M. Almansour, G. S. Gaba, R. Alroobaea, and M. Masud, "An empirical study on vulnerability assessment and penetration detection for highly sensitive networks," J. Intell. Syst., vol. 30, no. 1, pp. 592–603, 2021, doi: 10.1515/jisys-2020-0145.
[31] R. Dastres and M. Soori, "Secure Socket Layer in the Network and Web Security," Interna-tional J. Comput. Inf. Eng., vol. 14, no. 10, 2020.