Green Intelligent Systems and Applications

Research Article
Volume 6(1), 2026, 147−160
https://doi.org/10.53623/gisa.v6i1.1215

Implementation of a Centralized Cloud-Based Hotspot Voucher Management System and Network Traffic Monitoring Using MikroTik Virtual

Cristovani Ari Wibowo Lohonauman*, Christopel Hamonangan Simanjuntak, Maksy Sendiang, Herry Setiawan Langi, Venny Vita Ponggawa

D4 Informatics Engineering Study Program, Department of Electrical Engineering, Politeknik Negeri Manado, Indonesia

*Correspondence: cristo.lohonauman01@gmail.com

SUBMITTED: 24 May 2026; REVISED: 12 June 2026; ACCEPTED: 16 June 2026

ABSTRACT: Hotspot voucher services became one of the most widely adopted solutions among local Internet Service Providers (ISPs) because they facilitated user access control, usage duration management, and bandwidth allocation. In the existing network environment, hotspot voucher sales were operated at two different locations. However, the management of these locations was still performed independently using separate MikroTik routers. This condition created several challenges, including decentralized voucher data, standalone user authentication processes, inefficient voucher administration, and the inability to perform comprehensive network traffic monitoring. This study implemented a centralized hotspot voucher management system using a MikroTik Cloud Hosted Router (CHR) to integrate two hotspot voucher sales locations into a unified management platform. The MikroTik CHR was deployed in a cloud computing environment and functioned as the central server for voucher management, user authentication, and network traffic monitoring. Each MikroTik router at the voucher sales locations was connected to the MikroTik CHR through a VPN tunnel. Furthermore, a web-based application was developed as a management interface and was integrated with the MikroTik CHR through an Application Programming Interface (API). The application enabled administrators to generate vouchers, monitor voucher status, manage users, and observe network traffic through a centralized dashboard. The research adopted the Network Development Life Cycle (NDLC) methodology, which consisted of the stages of analysis, design, simulation, implementation, monitoring, and management. The implementation results demonstrated that the centralized system successfully integrated voucher management across two different locations, simplified administrative processes, supported centralized user authentication, and provided unified network traffic monitoring through a single platform. Therefore, the implementation of MikroTik CHR in a centralized hotspot voucher system improved management efficiency and supported the expansion and sustainability of hotspot services across multiple locations.

KEYWORDS: Centralized hotspot; cloud computing; mikrotik CHR; network traffic monitoring; hotspot voucher

1. Introduction

Public demand for internet access continued to increase for communication, work, education, and business activities. This trend made hotspot-based internet services increasingly popular because they provided network access in a practical manner and were easily accessible to users. One common system applied in hotspot services was the use of vouchers [1]. Through a voucher system, users could access the internet using a username and password according to the selected service package, such as usage duration, active period, quota allocation, or specific speed limits. In the existing network environment, hotspot voucher sales were carried out at two different locations. Both locations used MikroTik routers to manage hotspot services and generate vouchers for customers [2]. Although the service was already operational, voucher management at each location was still performed separately. Each router stored voucher data, user profiles, and active user information independently. As a result, administrators had to perform administrative tasks on each router when creating vouchers, modifying service packages, or viewing active users.

This separate management created several operational challenges. The voucher creation process became less efficient because it had to be performed on different routers. In addition, voucher data from the two locations were not stored in a centralized management system, making it difficult for administrators to view overall service information directly. If changes to service packages or service settings were required, the configurations also had to be applied individually on each router [3]. This condition complicated management, particularly when the number of voucher sales locations increased. In addition to voucher management issues, network traffic monitoring was also limited. Network usage information could only be viewed through the router at each location. Administrators did not have a unified interface that displayed traffic conditions from both locations simultaneously. However, information such as the number of active users, bandwidth consumption, connection duration, and upload and download traffic was essential for understanding the operational condition of hotspot services [4]. Without a centralized monitoring system, network supervision became less practical and more time-consuming.

Based on these conditions, a system was needed to connect voucher management from two locations into a single management center. A centralized management system could assist administrators in creating vouchers, managing service profiles, authenticating users, and monitoring network traffic through a single platform [5]. Therefore, hotspot service management no longer needed to be performed separately on each router. MikroTik Cloud Hosted Router (CHR) could be used as a solution for developing a centralized hotspot voucher management system. MikroTik CHR is a RouterOS platform that runs in a virtualized or cloud computing environment [6]. By utilizing CHR, MikroTik routers at two hotspot voucher sales locations could be connected to a central server through a VPN tunnel [7], [20]. The CHR could then function as the central platform for voucher management, user authentication, and network traffic monitoring [8]. To simplify the management process, this system also utilized a web-based application. The application functioned as an interface for administrators to create vouchers, view voucher lists, monitor voucher status, manage active users, and observe network traffic. The web application was integrated with MikroTik CHR through an Application Programming Interface (API), allowing management activities to be performed through a single system without requiring direct access to each router individually [9].

Several previous studies have discussed voucher-based hotspot systems, MikroTik-based hotspot management, VPN implementation, and web-based network monitoring [1], [2], [7], [14], [20]. These studies contributed to improvements in hotspot services, network connectivity, and monitoring capabilities. However, most previous studies focused on hotspot deployment and management within a single location, where voucher data, user authentication, and network monitoring were handled independently by local routers. Furthermore, limited research had integrated centralized voucher management, centralized user authentication, multi-location hotspot administration, and network traffic monitoring within a single cloud-based platform. Therefore, this study proposed a centralized hotspot voucher management system utilizing MikroTik Cloud Hosted Router (CHR) deployed in a cloud computing environment as the central server for voucher management and user authentication. The proposed system integrated multiple hotspot locations through VPN tunnels and provided a web-based management application connected via an Application Programming Interface (API). This approach enabled centralized administration, unified traffic monitoring, and easier service expansion for additional hotspot locations, thereby offering a more scalable and efficient solution than conventional standalone hotspot management systems.

This study aimed to implement a centralized hotspot voucher management system using MikroTik CHR. The system was designed to integrate two hotspot voucher sales locations that had previously been managed separately. Through the centralized system, voucher management was expected to become more efficient, user authentication could be performed through a single management center, and network traffic monitoring could be conducted through a unified platform [10]. This study focused on the implementation of MikroTik CHR as the central platform for cloud-based hotspot voucher management. The developed system was not only used to generate vouchers but also to integrate management functions across two hotspot voucher sales locations. In addition, the system was expected to serve as a foundation for future service expansion if additional voucher sales locations were established.

2. Materials and Methods

This study employed the Network Development Life Cycle (NDLC) approach as the network system development methodology. NDLC was selected because it provides systematic stages for designing, developing, testing, and managing network infrastructure. The stages applied in this study included analysis, design, simulation, implementation, monitoring, and management [11]. The selection of this methodology was aligned with the requirements of developing a centralized hotspot voucher management system involving the integration of multiple network devices, a cloud-computing-based server, and a web-based management application. The developed system focused on integrating two hotspot voucher sales locations that had previously been managed independently. The integration was achieved by utilizing MikroTik Cloud Hosted Router (CHR) as the central platform for user authentication, voucher management, and network traffic monitoring [12]. The MikroTik routers at each location were connected to the MikroTik CHR through VPN tunnels [13], while a web-based application was developed as the management interface and integrated with the CHR through an Application Programming Interface (API) [14].

2.1. Analysis.

The analysis stage was conducted to identify the initial condition of hotspot voucher management at the two voucher sales locations. Previously, each location had utilized a MikroTik router to provide hotspot services, generate vouchers, configure user profiles, and authenticate internet access [15]. However, the management process was still performed independently on each router. This management model resulted in voucher data, service profiles, active user information, and network traffic being stored in separate systems. Administrators were required to access each router individually to create vouchers, modify service profiles, monitor active users, and observe bandwidth utilization. This condition indicated that service management was not yet efficient because no centralized management system was available to integrate the two voucher sales locations. Based on this analysis, the required system needed to support centralized voucher management, user authentication through a central server, secure connectivity between routers, and unified network traffic monitoring across both locations through a single platform. To meet these requirements, MikroTik Cloud Hosted Router (CHR) was utilized as the cloud-computing-based management center, while a web-based application was developed as the user interface to support voucher administration and network traffic monitoring.

2.2. System specifications.

The implementation of the proposed centralized hotspot voucher management system required both hardware and software components to support hotspot services, centralized authentication, voucher management, and network traffic monitoring. The system consisted of two MikroTik routers deployed at separate hotspot service locations, a MikroTik Cloud Hosted Router (CHR) hosted on a Virtual Private Server (VPS), and a web-based management application integrated through the MikroTik Application Programming Interface (API). The hardware and software specifications utilized in this study are presented in Table 1.

Table 1. Hardware and software specifications.

Component	Specification
Router Location 1	MikroTik RB750Gr3
Router Location 2	MikroTik RB750Gr3
CHR Server	MikroTik Cloud Hosted Router (CHR)
VPS Storage	10 GB Disk Space
VPS Processor	1 vCPU
VPS Memory	1 GB RAM
VPS Bandwidth	Up to 10 Mbps (Unlimited Bandwidth)
Operating System	MikroTik RouterOS CHR
VPN Protocol	L2TP Tunnel
ISP Connection	Starlink
Front-End Technology	HTML
Back-End Technology	PHP
Database Management System	MySQL
Management Interface	Web-Based Application

As shown in Table 1, the centralized hotspot management system utilized two MikroTik RB750Gr3 routers connected to a MikroTik Cloud Hosted Router (CHR) hosted on a cloud-based Virtual Private Server (VPS). The CHR functioned as the central server for user authentication, voucher management, and network traffic monitoring. Communication between the hotspot locations and the CHR server was established through an L2TP VPN tunnel over a Starlink internet connection. Furthermore, a web-based application developed

using HTML and PHP was integrated with the MikroTik API, enabling administrators to manage vouchers, monitor user activity, and observe network traffic through a centralized platform [16].

2.3. Security considerations.

Security was an important aspect of the proposed centralized hotspot voucher management system because user authentication, voucher management, and network communication were performed through a public internet connection. To ensure secure communication between the hotspot locations and the centralized server, an L2TP VPN tunnel was implemented between each MikroTik router and the MikroTik Cloud Hosted Router (CHR). The VPN tunnel provided a dedicated communication channel that isolated management traffic from public network traffic and reduced the risk of unauthorized access or data interception during transmission [13, 17]. In addition to VPN-based communication, the web-based management application communicated with the MikroTik CHR through the MikroTik Application Programming Interface (API). Access to the API was restricted through authentication credentials configured on the CHR server. Furthermore, only authorized administrators were permitted to access the management application, ensuring that voucher creation, user management, and network monitoring activities could be performed securely. The implementation of VPN connectivity and controlled API access contributed to improving the overall security of the centralized hotspot management system [7, 19].

2.4. Design.

The design stage was conducted to develop the architecture of a voucher-based hotspot system with centralized management using a cloud-computing approach [17]. The designed system architecture consisted of three main layers: the application layer, the VPN/RADIUS server layer, and the access layer. As shown in Figure 1, the application layer contained the voucher management website, which functioned as the interface for hotspot voucher management and network monitoring. The website was integrated with the MikroTik Cloud Hosted Router (CHR) through an API, enabling administrators to create, delete, and centrally manage voucher profiles. In the VPN/RADIUS server layer, the MikroTik CHR functioned as both an L2TP server and a RADIUS server responsible for hotspot user authentication. The CHR was assigned a public IP address and established L2TP VPN tunnels with each router at the service locations using the 10.3.3.0/24 tunnel network. The RADIUS mechanism enabled centralized authentication, eliminating the need to store user data locally on each router. In the access layer, two service locations utilized Starlink ISP connections as the primary internet source. Each location was equipped with a MikroTik router that functioned as the gateway and hotspot manager, using local networks 192.168.10.0/24 and 192.168.20.0/24, respectively. The router at each location established a VPN connection to the CHR to support user authentication and data synchronization.

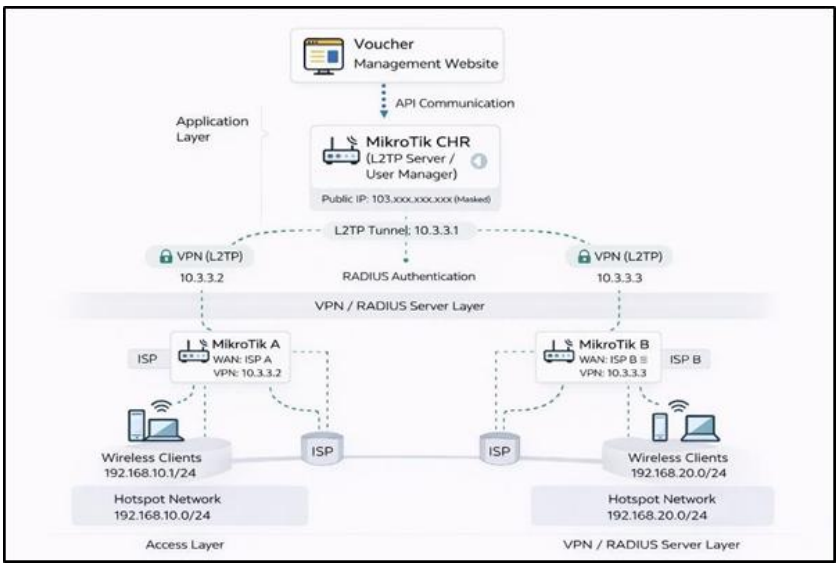

Figure 1. Cloud-based centralized hotspot network topology.

2.5. Simulation.

The simulation stage was conducted to validate the proposed system design before its deployment in the operational environment. Testing at this stage focused on two main aspects: centralized network connectivity through a VPN tunnel and the integration of the web-based voucher management application with MikroTik CHR as the central authentication and management server. During this stage, the MikroTik routers deployed at the two hotspot voucher sales locations were configured as L2TP clients to establish tunnel connections with the MikroTik CHR through the public network [18]. The MikroTik CHR functioned as the central server that received and managed connections from both local routers. The simulation results demonstrated that the VPN tunnels were successfully established and operated in an active state. As shown in Figure 2, communication between the MikroTik routers at the two hotspot voucher sales locations and the central server operated according to the designed system architecture.

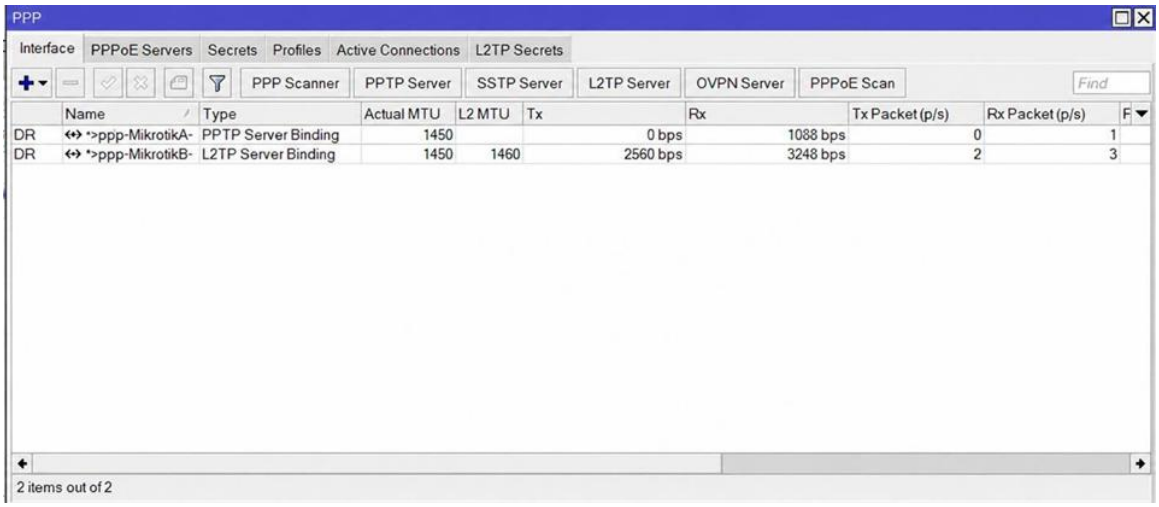

Figure 2. L2TP VPN tunnel status on mikrotik CHR in active condition.

In addition to VPN connectivity testing, a simulation was also conducted at the application layer. The voucher management system was developed as a web-based application

integrated with the MikroTik Cloud Hosted Router (CHR) through an Application Programming Interface (API). The application was designed to manage hotspot vouchers, configure service profiles, record voucher usage history, and monitor network device parameters in real time. The dashboard interface used for centralized management is presented in Figure 3.

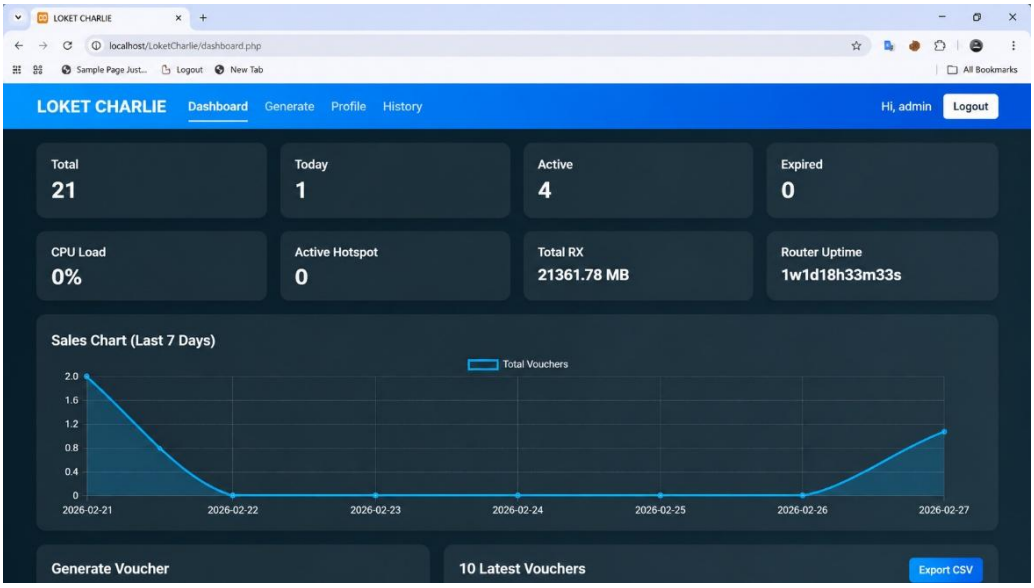

Figure 3. Web-based voucher management system dashboard display.

Testing was carried out by generating several vouchers through the voucher generation feature in the system. The generated vouchers were stored in the database and automatically synchronized with MikroTik CHR as the centralized authentication server. The voucher status displayed in the system indicates that the synchronization process ran properly, as shown in Figure 4. Based on the testing results in the simulation stage, VPN connectivity, API integration between the system and MikroTik CHR, and the voucher data synchronization mechanism were able to operate according to the system design. These results indicate that the developed system can support centralized authentication and voucher management processes, allowing the system to be implemented in an operational environment.

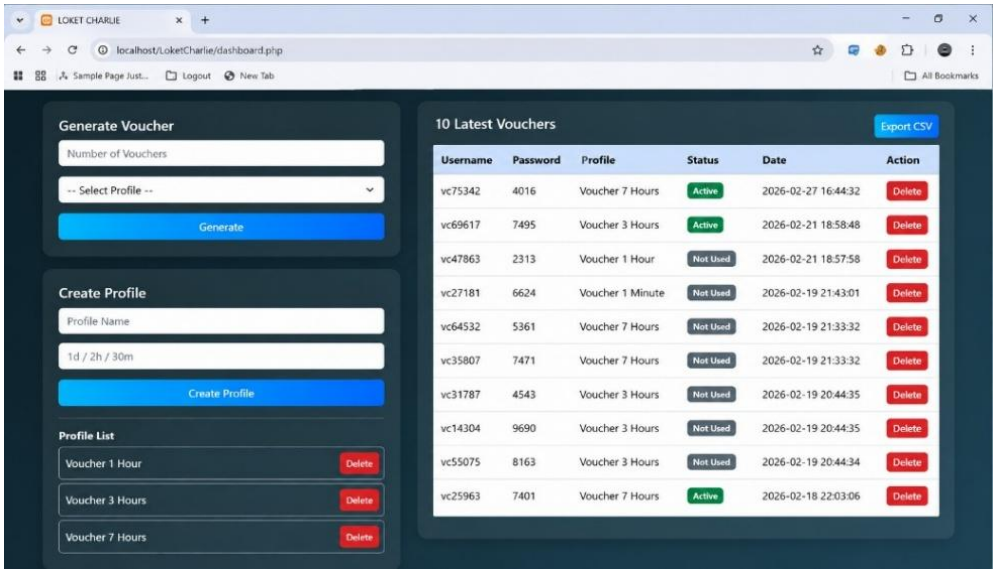

Figure 4. Voucher creation and synchronization results.

2.6. Implementation.

The implementation stage was carried out by deploying the system architecture developed in the previous stage within the operational environment. The implementation process included router configuration at each service location, centralized authentication integration using MikroTik Cloud Hosted Router (CHR) [19], and the deployment of a web-based voucher management system connected through an Application Programming Interface (API). The voucher generation and authentication processes were successfully tested through the web-based management application integrated with the MikroTik CHR. Administrators were able to generate hotspot vouchers automatically based on predefined service profiles. The generated vouchers were subsequently used for hotspot login testing, during which user credentials were authenticated centrally through the MikroTik CHR via the established L2TP VPN tunnel. Following successful authentication, the voucher status changed from unused to active, indicating that the system correctly recognized and validated user credentials. These results confirmed that the centralized voucher management and authentication mechanisms functioned as designed. After a user session ended, the system displayed a logout page containing detailed session information, including the username, IP address, MAC address, connection duration, and the volume of uploaded and downloaded data during the session. The information was obtained from user session logs recorded on the MikroTik device and synchronized with the MikroTik Cloud Hosted Router (CHR). The logout information page is presented in Figure 5. The implementation results demonstrated that the cloud-computing-based centralized hotspot voucher management system operated in accordance with the designed architecture. The integration among the routers at the service locations, the MikroTik CHR as the authentication center, and the web-based application for voucher management and network traffic monitoring functioned successfully as a unified and centralized system.

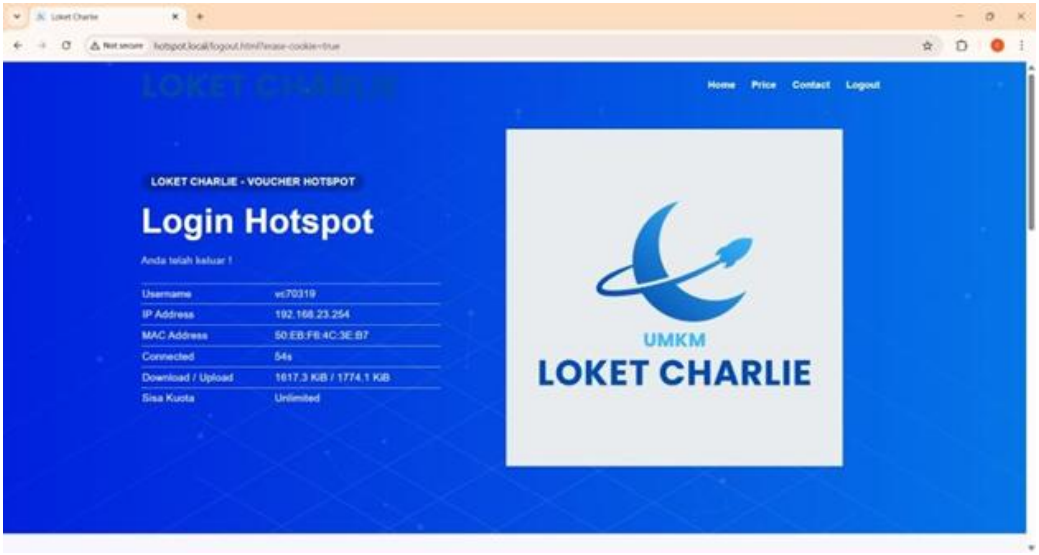

Figure 5. Logout information page.

2.7. Maintenance and backup strategy.

To ensure the reliability and continuity of the centralized hotspot management system, regular maintenance and backup procedures were implemented. Configuration backups of the MikroTik CHR server and hotspot routers were performed periodically to prevent data loss and facilitate system recovery in the event of hardware or software failures. The web application

database was also backed up regularly to preserve voucher data, user information, and monitoring records. In the event of a service disruption, the backup configuration files could be restored to the CHR server or hotspot routers to recover system functionality. Furthermore, the centralized architecture simplified troubleshooting and maintenance activities because administrators could monitor and manage the system through a single platform. These maintenance and recovery mechanisms contributed to improving system availability and operational reliability.

3. Results and Discussion

The implementation of the centralized hotspot voucher management system was carried out by connecting two MikroTik routers located at hotspot voucher sales locations to the MikroTik Cloud Hosted Router (CHR) through a VPN tunnel. The MikroTik CHR functioned as the central server for user authentication and voucher management, while the web-based application served as the interface for voucher generation, user management, and network traffic monitoring. Before implementation, voucher management was performed independently on each MikroTik router. Each location maintained its own voucher data, service profiles, and active user information. This condition required administrators to manage each router separately, including creating vouchers, modifying service profiles, and monitoring network usage. After implementation, the voucher management process could be performed through a web-based application integrated with the MikroTik CHR. Vouchers generated through the application were used as authentication credentials for hotspot users. When users logged in, the local MikroTik router forwarded the authentication request to the MikroTik CHR. If the voucher credentials matched the stored authentication data, users were granted internet access according to the predefined service profile [8, 13, 20]. A comparison of the system before and after implementation is presented in Table 2.

Table 2. Comparison of the system before and after implementation.

Aspect	Before Implementation	After Implementation
Voucher Management	Vouchers were managed on each router.	Vouchers are managed centrally through MikroTik CHR.
User Authentication	Authentication was performed locally on each router.	Authentication is performed through MikroTik CHR as the authentication center.
Traffic Monitoring	Traffic was monitored from each router.	Traffic is monitored through a single management platform.
Service Administration	The administrator had to access each router individually.	The administrator manages the service through a web application.

Based on Table 2, a clear difference was observed between the system before and after implementation. Prior to the implementation of the centralized system, voucher management was performed locally on each MikroTik router. After implementation, voucher management, user authentication, and network traffic monitoring were centralized through the MikroTik Cloud Hosted Router (CHR), which functioned as the primary management server [8, 10]. This centralized architecture simplified administrative tasks, improved management efficiency, and enabled unified monitoring across multiple service locations. The differences between the system architectures before and after implementation are illustrated in Figures 6 and 7. Figure 6 shows the system architecture before the implementation of the centralized hotspot voucher management system. In this architecture, each hotspot voucher sales location operated

independently using its own MikroTik router and locally stored voucher database. Voucher generation, user authentication, and network monitoring were performed separately at each location. Consequently, administrators were required to access and manage each router individually, resulting in increased administrative complexity and limited visibility of overall network operations [1, 2].

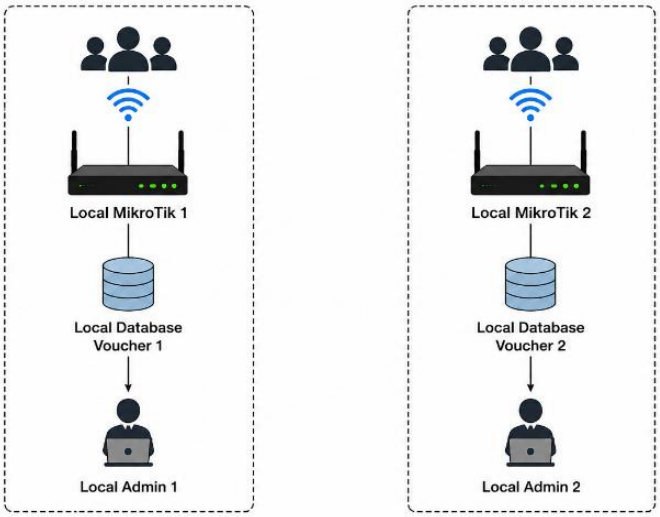

Figure 6. System architecture before implementation.

Figure 7 presents the system architecture after the implementation of the proposed centralized management system. In this architecture, the two hotspot voucher sales locations are connected to MikroTik Cloud Hosted Router (CHR) through L2TP VPN tunnels. The web-based management application communicates with CHR through an Application Programming Interface (API), enabling centralized voucher management, user authentication, and network traffic monitoring. Through this architecture, hotspot services from multiple locations can be administered through a single management platform, improving operational efficiency and simplifying service administration [10, 13, 14].

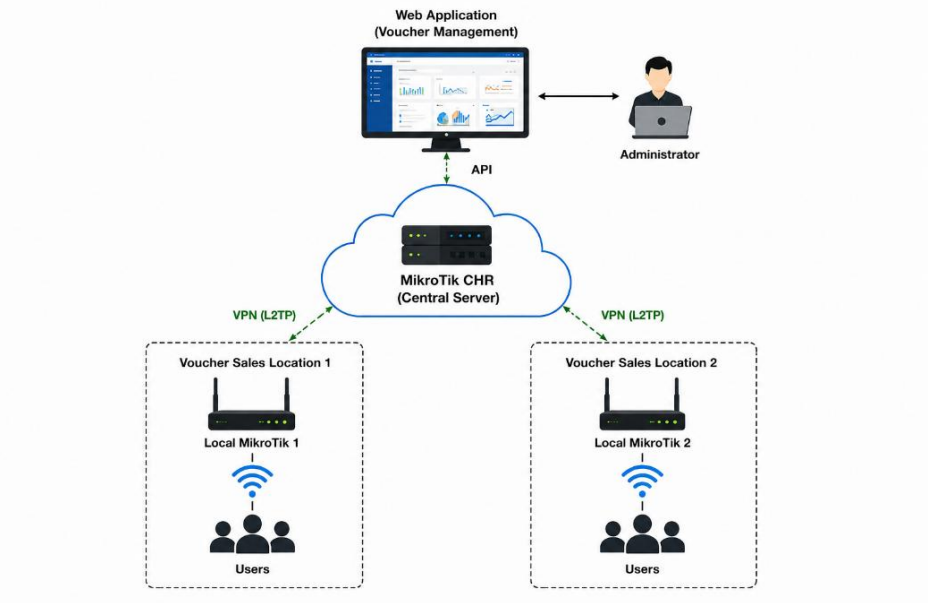

Figure 7. System architecture after implementation.

The test results demonstrated that vouchers generated through the web-based management application could be successfully used for hotspot authentication. User credentials were verified centrally through the MikroTik CHR, and voucher status was automatically updated following successful login. In addition, network traffic information, including active users, connection duration, IP addresses, MAC addresses, and uploaded and downloaded data, could be monitored through the centralized management interface. These results indicated that the proposed system successfully integrated hotspot voucher management, user authentication, and network traffic monitoring across multiple hotspot service locations [8, 10].

The operational performance of the proposed system was evaluated using several network performance indicators, including latency, authentication response time, bandwidth utilization, and throughput. During system operation, communication between the hotspot routers and the MikroTik CHR server through the L2TP VPN tunnel remained stable, with an average latency of approximately 25 ms. The authentication process required an average response time of approximately 1.5 seconds, enabling users to access hotspot services without noticeable delays. Bandwidth utilization at the hotspot locations ranged from 8 Mbps to 10 Mbps, while the average throughput achieved during operation was approximately 9 Mbps. These results demonstrated that the proposed centralized architecture was capable of supporting hotspot services while maintaining stable performance and efficient resource utilization.

To further evaluate the contribution and advantages of the proposed system, a comparison was conducted with several previous studies related to hotspot voucher management and network administration. The comparison focused on key features, including centralized management, user authentication, multi-location integration, VPN connectivity, cloud deployment, and monitoring capabilities. By comparing these features, the proposed system could be evaluated in terms of functionality and scalability relative to existing approaches. The results of the comparison are presented in Table 3.

Table 3. Comparison of the proposed system with previous studies.

Feature	[1]	[2]	[10]	Proposed System
Voucher-Based Hotspot Service	Yes	Yes	No	Yes
Centralized Voucher Management	No	No	Yes	Yes
Centralized User Authentication	No	No	No	Yes
Multi-Location Integration	No	No	No	Yes
VPN-Based Interconnection	No	No	No	Yes
Cloud-Based Deployment (CHR)	No	No	No	Yes
Network Traffic Monitoring	Limited	Limited	Yes	Yes
Web-Based Management Interface	No	No	No	Yes

As shown in Table 3, previous studies primarily focused on hotspot deployment, voucher generation, and local network management. Hidayatulloh et al. [1] and Awaliyani [2] implemented voucher-based hotspot services using MikroTik devices; however, voucher management and user authentication were performed independently at each location. Damanik and Anggraeni [10] proposed a centralized network management approach, but their study did not specifically address hotspot voucher management, centralized user authentication, or multi-location hotspot integration. In contrast, the proposed system integrated centralized voucher management, centralized user authentication, VPN-based interconnection, cloud-based MikroTik CHR deployment, and web-based monitoring within a single platform. These capabilities improved administrative efficiency, simplified network management, and provided

a scalable architecture capable of supporting future expansion to additional hotspot service locations.

The proposed architecture also provided scalability for future service expansion. Since the MikroTik CHR operated as a centralized authentication and management server, additional hotspot locations could be integrated by establishing VPN connectivity between new MikroTik routers and the CHR server. This approach allowed administrators to extend hotspot services without significantly modifying the existing system architecture. The web-based management application continued to provide centralized monitoring and voucher management across all locations. Therefore, the proposed solution was capable of supporting multiple hotspot locations while maintaining centralized management, traffic monitoring, and operational efficiency.

4. Conclusions

Based on the implementation and testing results, the centralized hotspot voucher management system utilizing MikroTik Cloud Hosted Router (CHR) successfully integrated two hotspot voucher sales locations that had previously been managed independently. The system enabled voucher creation, user authentication, and network traffic monitoring to be performed through a single management center. The MikroTik routers at each location were connected to the MikroTik CHR through a VPN tunnel, while the web-based application served as the interface for voucher management and network activity monitoring. The results demonstrated that the centralized system reduced repetitive administrative tasks on individual routers, simplified the monitoring of voucher status and active users, and enabled administrators to observe network traffic information through a unified platform. Furthermore, the system successfully integrated voucher management, centralized authentication, and network monitoring across multiple locations. Therefore, the implementation of MikroTik CHR in a centralized hotspot voucher management system improved operational efficiency and provided a scalable foundation for future service expansion when additional hotspot voucher sales locations are introduced. Despite the successful implementation of the proposed system, several limitations should be acknowledged. The performance and availability of the centralized hotspot management system depended on the stability of the Starlink internet connection and the accessibility of the cloud-hosted CHR server. Any disruption to the internet connection or VPN tunnel could affect the authentication process and centralized management functions. In addition, this study was conducted using only two hotspot service locations; therefore, the scalability of the system for a larger number of locations was not extensively evaluated. Future research may focus on scalability testing involving multiple hotspot locations, performance evaluation under higher network loads, and the implementation of additional security mechanisms, redundancy strategies, and backup systems to further improve service reliability and availability.

Acknowledgments

The author would like to express sincere gratitude to Manado State Polytechnic for its support in the implementation of this research. Appreciation is also extended to UMKM Loket Charlie for providing the opportunity and facilities for conducting this study. The author would further like to thank Christopel H. Simanjuntak, S.T., M.Eng., and Maksy Sendiangan, S.S.T., M.I.T., as journal supervisors, as well as Herry S. Langi, S.S.T., M.T., and Venny V. Ponggawa, S.S.T.,

M.T., as final project supervisors, for their guidance, supervision, and valuable suggestions throughout the preparation and implementation of this research. Their support and contributions were invaluable to the successful completion of this study.

Competing Interests

The author declares that there are no competing interests regarding the publication of this paper.

Data Availability Statement

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

References

[1] Hidayatulloh, M.F.; Santi, I.H.; Febrinita, F. (2023). Implementasi Jaringan Hotspot Dengan Sistem Voucher Menggunakan Mikrotik Di Jaringan RT/RW Net. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*, 2652–2659. https://doi.org/10.36040/jati.v7i4.7808.

[2] Awaliyani, I. (2023). Pengembangan Konfigurasi Jaringan Hotspot dan Voucher WiFi Menggunakan Mikrotik CCR1009-7G-1C-1S+ pada Jalurdata.net. *Aisyah Journal of Informatics and Electrical Engineering*, *5*, 218–226. https://doi.org/10.30604/jti.v5i2.233.

[3] Mehmood, F.; Ahmad, S.; Kim, D. (2019). Design and Implementation of an Interworking IoT Platform and Marketplace in Cloud of Things. *Sustainability*, *11*, 5952. https://doi.org/10.3390/su11215952.

[4] Sandova, D.; Prihantoro, C. (2021). Analisis Traffic pada Jaringan LAN Menggunakan MikroTik. *Journal of Scientific and Applied Informatics*, *4*, 329–337. https://doi.org/10.36085/jsai.v4i3.2011.

[5] Ray, P.P.; Skala, K. (2022). Internet of Things Aware Secure Dew Computing Architecture for Distributed Hotspot Network: A Conceptual Study. *Applied Sciences*, *12*, 8963. https://doi.org/10.3390/app12188963.

[6] Arfind, R.; Supendar, H.; Fahlapi, R. (2023). Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan Mikrotik. *Jurnal Komputer dan Antar Sistem*, *1*, 108–116. https://doi.org/10.70052/jka.v1i3.28.

[7] Gentile, A.F.; Macrì, D.; Greco, E.; Fazio, P. (2024). Overlay and Virtual Private Networks Security Performances Analysis with Open-Source Infrastructure Deployment. *Future Internet*, *16*, 283. https://doi.org/10.3390/fi16080283.

[8] Sembiring, F.G.; Ashillah, S.; Nasution, A.K.; Kiswanto, D. (2025). Analisis Kinerja Routing Dinamis Pada Jaringan Virtual Menggunakan Mikrotik CHR. *Jurnal Informatika dan Teknik Elektro Terapan*, *13*. https://doi.org/10.23960/jitet.v13i3.6516.

[9] Safikri, Y.A.; Prehanto, D.R. (2022). Aplikasi Payment Voucher RT/RW Net Mikrotik Berbasis Android Flutter dengan Metode Payment Gateway pada Dusun Jomblang Desa Puncu Kabupaten Kediri. *Journal of Informatics and Computer Science*, *3*, 462–470. https://doi.org/10.26740/jinacs.v3n04.p462-470.

[10] Damanik, H.A.; Anggraeni, M. (2025). Manajemen Jaringan Terpusat untuk Konfigurasi dan Otomatisasi Pemulihan Menggunakan Paramiko dan Django Framework. *Jurnal Teknik Informatika dan Sistem Informasi*, *11*, 369–382. https://doi.org/10.28932/jutisi.v11i3.11431.

[11] Ariyadi, T.; Purwanto, T.D.; Fajar, M.M. (2023). Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Dengan Metode NDLC (Network Development Life Cycle) Pada PT Kirana Permata. *Jurnal Ilmiah Informatika*, *11*, 189–195. https://doi.org/10.33884/jif.v11i02.8032.

[12] Nirmalsari, P.; Fahmi, H.; Fadli, S. (2023). Implementasi Metode Network Development Life Cycle Pada Rancang Bangun Jaringan Wireless Berbasis Mikrotik. *Jurnal Teknik Mesin, Industri, Elektro dan Informatika*, *2*, 72–87. https://doi.org/10.55606/jtmei.v2i3.2107.

[13] Wardana, M.A.; Nusri, A.Z.; Juliandika, J. (2022). Jaringan Virtual Private Network (VPN) Berbasis Mikrotik Pada Kantor Kecamatan Marioriawa Kabupaten Soppeng. *Jurnal Ilmiah Sistem Informasi dan Teknik Informatika*, *5*, 107–116. https://doi.org/10.57093/jisti.v5i2.135

[14] Sobah, N.; Amrulloh, M.F. (2023). Perancangan dan Implementasi Sistem Monitoring Jaringan di MA Darut Taqwa Berbasis Web yang Mengintegrasikan dengan API MikroTik. *BIOS: Jurnal Teknologi Informasi dan Rekayasa Komputer*, *4*, 42–53. https://doi.org/10.37148/bios.v4i2.75.

[15] Samalukang, I.P.; Liando, O.E.S.; Paat, W.R.L. (2022). Pengembangan Media Pembelajaran Praktikum Jaringan Komputer di Jurusan PTIK Universitas Negeri Manado. *Edutik: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, *2*, 594–602. https://doi.org/10.53682/edutik.v2i4.5827.

[16] Novianto, D.; Japriadi, Y.S.; Tommy, L. (2022). Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik. *Jurnal Ilmiah Informatika Global*, *13*. https://doi.org/10.36982/jiig.v13i2.2308.

[17] Lim, K.S.; Ooi, S.Y.; Sayeed, M.S.; Chew, Y.J.; Ahmad, N.M. (2025). Securing the Internet of Things: Systematic Insights into Architectures, Threats, and Defenses. *Electronics*, *14*, 3972. https://doi.org/10.3390/electronics14203972.

[18] Pamungkas, A.P.; Putra, M.R.; Hafizh, M. (2021). Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis Mikrotik pada Diskominfo Kabupaten Muko-Muko. *Jurnal KomtekInfo*, *8*, 189–194. https://doi.org/10.20895/infotel.v9i3.274.

[19] Rahayu, T.B.; Suharjo, I. (2024). Implementasi BGP dengan RPKI Pada Jaringan PT. Bintang Mataram Teknologi Menggunakan Mikrotik Router OS. *Jurnal Fasilkom*, *14*, 293–300. https://doi.org/10.37859/jf.v14i2.6968.

[20] Nugraha, F.; Nurhayati, Y.; Yusup, A.M. (2025). Application of VPN Technology Using L2TP and AAA Radius as an Authentication Protocol on Hotspot Networks. *AIP Conference Proceedings*, *3141*, 020003. https://doi.org/10.1063/5.0261258.