

## PERANCANGAN SISTEM AUTENTIKASI WIRELESS *HOTSPOT* BERBASIS RADIUS MENGGUNAKAN MIKROTIK

Ahmad Sa'di<sup>1)</sup>, Ria Andriani<sup>2)</sup>, Taufikurrahman<sup>3)</sup>

<sup>1)</sup> Informatika Universitas AMIKOM Yogyakarta

<sup>2,3)</sup> Teknik Informatika Universitas AMIKOM Yogyakarta

email : [ahmadsa@amikom.ac.id](mailto:ahmadsa@amikom.ac.id)<sup>1)</sup>, [ria@amikom.ac.id](mailto:ria@amikom.ac.id)<sup>2)</sup>, [taufikurrahman.2000@students.amikom.ac.id](mailto:taufikurrahman.2000@students.amikom.ac.id)<sup>3)</sup>

### Abstraksi

Penggunaan jaringan WLAN (wireless Local Area Network) pada layanan hotspot sudah menjadi layanan umum yang disediakan oleh pemilik usaha café, toko dan lainnya. Terbatasnya pengetahuan jaringan komputer bagi pengelola café memberikan dampak pada keamanan WLAN. Ditemukan banyaknya penggunaan keamanan dasar pada layanan *hotspot* berdampak adanya isu kekhawatiran bagi pengguna layanan hotspot terhadap keamanan dirinya saat beraktivitas di internet. Penelitian ini bermaksud untuk menguji implementasi sistem autentikasi jaringan WLAN pada layanan *hotspot* menggunakan network access server dengan memanfaatkan radius server yang telah tersedia di Router Mikrotik dan Radius (*Remote Authentication Dial-In User Service*) berbasis sumber terbuka yang difungsikan sebagai autentikasi pengguna di jaringan WLAN pada layanan *hotspot*. Hasil penelitian yaitu implementasi keamanan pada layanan *hotspot* dengan memanfaatkan radius server dapat menaikkan tingkat pengaman jaringan WLAN (*security*) tepat guna, dibuktikan setiap pengguna yang akan menggunakan layanan hotspot mengharuskan datang ke petugas barista (dicatat) dan pengguna mengharuskan login dengan akun yang telah tervalidasi serta keamanan awal pengguna dalam menginputkan username dan password telah terenkripsi dengan protocol SSL (*Secure Sockets Layer*)

### Kata Kunci :

WLAN, Layanan Hotspot, Radius, Autentikasi

### Abstract

The use of WLAN (wireless Local Area Network) networks for hotspot services has become a typical service provided by cafes, shops and other business owners. The limited knowledge of computer networks for café managers has an impact on WLAN security. It was found that many uses of basic security in hotspot services have an impact on the issue of concern for users of hotspot services for their own safety when doing activities on the internet. This study intends to examine the implementation of the WLAN network authentication system on hotspot services using a network access server by utilizing the radius server available on Mikrotik and Radius (*Remote Authentication Dial-In User Service*) based open source routers that function as user authentication on WLAN networks on hotspot service. The research results show that the implementation of security in hotspot services by utilizing a radius server can increase the level of security for effective WLAN (*security*) networks, it is proven that every user who will use the hotspot service must come to the barista officer (recorded) and the user requires to log in with a validated account. as well as the initial security of the user in entering the username and password encrypted with the SSL (*Secure Sockets Layer*) protocol.

### Keywords:

WLAN, Hotspot Service, Radius, Authentication

### Pendahuluan

Layanan hotspot pada café disediakan untuk akses internet yang membuat pelanggan cafe mudah melakukan pekerjaan ataupun melakukan kegiatan yang menggunakan fasilitas internet [1], di cafe ini mempunyai satu router utama untuk mengakses internet seperti wifi atau *hotspot*, untuk mendapatkan akses internet, cafe ini akan memberikan 10 menit pertama gratis selanjutnya akan dikenakan biaya. Jaringan internet yang digunakan dalam café merupakan jaringan berskala kecil yang hanya terdiri dari ISP, Router, Switch, Server, hingga *End-User*.

Pada prinsipnya, jaringan tersebut sudah memenuhi kebutuhan penggunaan akses internet. Namun, ada beberapa kendala yang dihadapi seperti lambatnya akses jaringan internet yang dikarenakan pembagian *bandwidth* yang tidak merata. Selain itu sering terjadi antrian akses karena tidak adanya pembagian *bandwidth* untuk masing-masing user[2].

Permasalahan yang umum di ditemui yaitu pada penggunaan layanan *hotspot* yaitu kerentanan pada jaringan WLAN. Sebab kerentanan tersebut, pengguna yang tidak legal, dapat mendapatkan akses ke jaringan WLAN pada layanan hotspot. Metode

keamanan yang cukup tepat digunakan pada jaringan WLAN di Layanan *Hotspot* adalah dengan menerapkan metode autentikasi berupa *username* dan *password* sesuai kaidah keamanan informasi, pengguna diharuskan melakukan validasi akun (autentikasi) ke *radius server* sebelum terkoneksi ke jaringan wireless LAN pada layanan hotspot[1].

Pada penelitian ini bermaksud untuk membuat autentikasi jaringan wireless LAN pada layanan *hotspot*, agar pengguna yang mengakses jaringan wireless LAN tervalidasi dengan tepat yaitu hanya pelanggan cafe, sekaligus memberikan keamanan bagi pengguna saat terhubung ke jaringan wireless LAN pada layanan *hotspot*. Di sisi lain berharap dapat memudahkan bagi administrator jaringan dalam mengelola jaringan wireless LAN pada layanan *hotspot*. Dalam implementasi jaringan wireless LAN pada layanan *hotspot* menggunakan metode *Remote Access Dial-in User Service* (RADIUS) merupakan suatu mekanisme akses kontrol untuk memvalidasi dan melakukan autentikasi (*authentication*) pengguna berdasarkan pada mekanisme autentikasi yang sudah banyak digunakan sebelumnya, yaitu menggunakan metode *challenge* atau *response*. Diharapkan dengan menggunakan metode autentikasi radius dapat mengatasi keamanan [3] dan pengaturan akun pengunjung yang akan menggunakan jaringan wireless LAN pada layanan hotspot[4].

### Tinjauan Pustaka

Beberapa penelitian yang terkait dan kemiripan obyek yang diteliti adalah sebagai berikut. Penelitian pertama dilakukan oleh Endang Pujiastuti, tahun (2019) dengan judul “Perancangan Manajemen *Hotspot* Menggunakan Autentikasi Radius Server Mikrotik Pada Kantor Walikota Administrasi Jakarta Barat”. Tujuan penelitian ini yaitu membatasi hak akses dalam penggunaan internet pada setiap pengguna dengan metode Radius Server pada Mikrotik. Hasil dari penelitian ini sangat berpengaruh dalam kelancaran akses pengguna dalam memanfaatkan layanan *Hotspot* di sebuah Kantor Walikota Administrasi Jakarta Barat dengan tetap memenuhi protocol keamanan jaringan [5].

Penelitian selanjutnya oleh Wayan Sukartayasa dan Putu Haryadi (2019), yang berjudul “Perancangan Keamanan Jaringan *Authentication Login Hostpot* Menggunakan Radius Server dan Protokol EAP-TTLS Pada Mikrotik di Idoop Hotel”. Penelitian ini bertujuan memberikan alternatif untuk kemudahan autentikasi jaringan WLAN, dibandingkan dengan protokol EAP yang berbasis sertifikat digital. Metode EAP-TTLS hanya memerlukan sertifikat digital pada sisi *authentication server*, sedangkan sertifikat digital pada sisi pengguna akan digantikan dengan menggunakan kombinasi *username* dan *password*. Hasil dari penelitian adalah dapat meningkatkan pengguna dalam mobilitas menggunakan jaringan WLAN, karena pengguna

tidak perlu menambahkan sertifikat digital untuk ketika menggunakan layanan *hotspot* (login) [6].

Penelitian berikutnya oleh Sulhan Qidri, Marsani Asfi, Ridho Taufiq S. dan Muhammad Hatta pada tahun (2020) yang berjudul “Manajemen Hak Akses bagi pengguna Jaringan Menggunakan FreeRADIUS yang difungsikan untuk validasi akun pengguna Jaringan”. Tujuan penelitian yaitu memvalidasi akun pengguna jaringan WLAN di SMK NU Kaplongan, Metode yang digunakan yaitu dengan memanfaatkan layanan FreeRADIUS. Hasil dari penelitian menunjukkan bahwa aplikasi web menggunakan bahasa PHP dapat diintegrasikan dengan FreeRADIUS server untuk single user dalam proses autentikasi aplikasi[7].

Penelitian selanjutnya oleh Arif Gumelar (2020) yang berjudul “Perancangan jaringan *hotspot* berbasis radius server untuk manajemen pengguna internet di SMK Negeri 3 Pekalongan” yaitu implementasi sistem autentikasi untuk pengguna layanan *hotspot* di jaringan wireless LAN menggunakan RADIUS dengan menerapkan kontrol pembatasan akses pengguna berdasarkan kuota dan waktu pemakaian. Hasil dari penelitian ini membantu network administrator atau pengelola jaringan dalam mengatur layanan *hotspot*. Sistem manajemen *hotspot* ini dapat melakukan berbagai skema pembatasan akses [4].

Penelitian berikutnya oleh Eko Agus Darmadi pada tahun (2018) “Perancangan sistem otentikasi radius pada Pengguna jaringan wireless untuk meningkatkan keamanan jaringan komputer” yaitu merancang dan mengimplementasikan jaringan wireless LAN dengan melakukan sistem kontrol validasi pengguna jaringan wireless LAN. Teknologi yang digunakan yaitu RADIUS (*Remote Authentication Dial-In User Service*) yang bertujuan melakukan autentikasi, otorisasi, dan akunting [8].

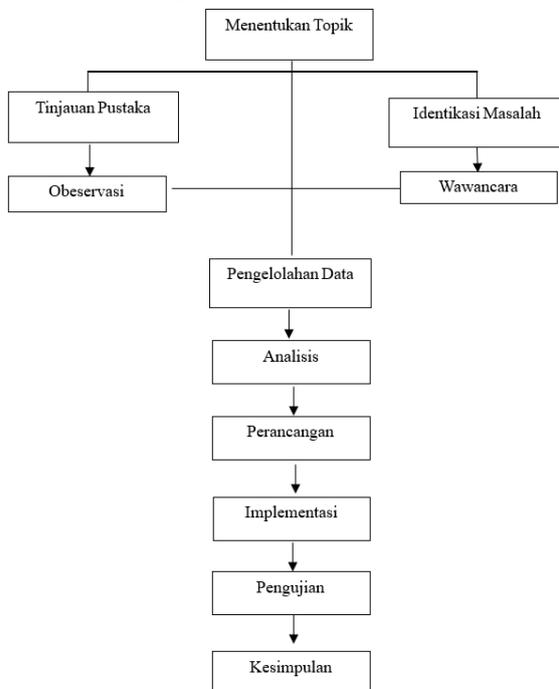
Penelitian yang dilakukan Syahputra, H. ., & Wijaya, R. . (2022) yang berjudul “Pembangunan Jaringan Hotspot Berbasis Mikrotik pada Kampung Tematik di Kecamatan Padang Utara”. Meneliti tentang peranan jaringan WLAN layanan hotspot untuk meningkatkan kesejahteraan masyarakat kampung tematik dengan melakukan peningkatan potensi lokal. Akses internet dimanfaatkan untuk menggali informasi produk-produk dan memasarkan produk dengan cara online [9].

Penelitian yang dilakukan oleh Rifky Wahyu Pratama (2019) menerapkan autentikasi pada jaringan wireless LAN di PT. Kudo Teknologi Indonesia. Metode yang digunakan yaitu autentikasi dengan mengintegrasikan layanan windows active directory dengan radius server. Hasilnya yaitu pengguna yaitu karyawan atau pengunjung yang sedang menggunakan layanan hotspot pada jaringan wireless dapat terkontrol akun penggunanya, dengan memanfaatkan manajemen user dari active directory. Akun tersebut dapat digunakan di layanan-layanan

lain dalam kasus ini di layanan hotspot (*single user*). Pembatasan akses pada akun hotspot dilakukan di Mikrotik tetapi untuk akunya diambilkan dari layanan windows *active diretory* [10].

## Metode Penelitian

Tahapan penelitian dijabarkan secara bertahap berdasarkan diagram alur pada Gambar 1.



Gambar 1. Diagram alur penelitian

### 1. Menentukan Topik

Menentukan topik penelitian dengan disesuaikan objek penelitian.

### 2. Tinjauan Pustaka

Mengumpulkan studi pustaka dari jurnal-jurnal yang sejenis penelitian yang akan dilakukan dengan mencari tahu tentang alur penelitian, permasalahan, solusi dan metode yang diusulkan untuk proses penelitian.

### 3. Identifikasi Masalah

Menemukan kendala atau permasalahan pada objek penelitian apa yang terjadi di lapangan khususnya pada jaringan WLAN pada layanan hotspot.

### 4. Observasi

Metode penelitian dengan cara mengamati secara langsung tentang kondisi sesungguhnya yang terjadi di lokasi penelitian

### 5. Wawancara kepada pengelola dan pemilik

Menanyakan kepada pegelola jaringan atau pemilik jaringan tentang kondisi terjadi dilapangan.

### 6. Pengolahan Data

Beberapa fakta yang didapatkan dari observasi dan wawancara di lapangan dilanjutkan dengan pengolahan data. Data yang dimaksud adalah data

kendala pada objek penelitian dan memberikan masukan perbaikan.

### 7. Analisis

Menganalisa permasalahan yang ada pada objek penelitian menggunakan data-data yang telah didapatkan. Data tersebut menjadi dasar perancangan sistem autentikasi pada jaringan WLAN.

### 8. Perancangan

Tahap perancangan dengan membuat diagram topologi jaringan WLAN pada layanan hotspot dan menjabarkan kebutuhan jaringan WLAN yang diperlukan untuk memperbaiki keamanan pada layanan hotspot.

### 9. Implementasi sistem jaringan

Pada tahapan ini dilakukan penerapan perancangan yaitu dengan instalasi layer fisik, instalasi perangkat jaringan dan konfigurasi dasar jaringan. Setelah dipastikan telah terhubung dengan satu sama lain perangkat jaringan jaringan dan perangkat yang terhubung di jaringan, langkah selanjutnya yaitu dengan instalasi radius server pada router Mikrotik. Mikrotik difungsikan routing dan melayani autentikasi. Routing untuk memastikan jaringan lokal dapat terhubung ke internet dan megaktifkan raius sebagai layanan autentikasi.

### 10. Pengujian

Pada tahap pengujian yaitu pengujian proses bisnis user dalam mendapatkan akun dan login ke layanan hotspot, setelah akun dinyatakan tervalidasi di sistem maka dilakukan kontrol akses user.

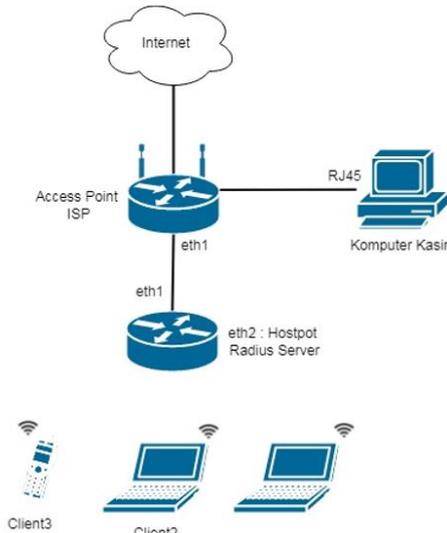
### 11. Kesimpulan

Menyampaikan kesimpulan hasil dari penelitian. Dengan menyampaikan proses dan hasil yang dicapai pada penelitian.

## Hasil dan Pembahasan

### 1. Perancangan

Perancangan diagram topologi jaringan pada pengujian metode ini dibangun berdasarkan konsep dan gambaran dari perangkat sebenarnya. Menggunakan 2 router Mikrotik. Router 1 difungsikan sebagai *edge device* yaitu berperan meroutingkan jaringan lokal ke internet dengan memanfaatkan *default route*. Protokol NAT (*network address translation*) untuk menerjemahkan *ip private* jaringan WLAN ke internet. Router 2 difungsikan sebagai server radius yaitu menangani autentikasi akun pengguna layanan hotspot pada jaringan WLAN. Beberapa unit laptop dan *mobile phone* berfungsi sebagai *radius Client*.



Gambar 2. Topologi jaringan

Adapun perancangan IP Address yang digunakan pada topologi pada Gambar 1 sebagai berikut.

Tabel 1. Desain Alamat IP (Internet Protocol)

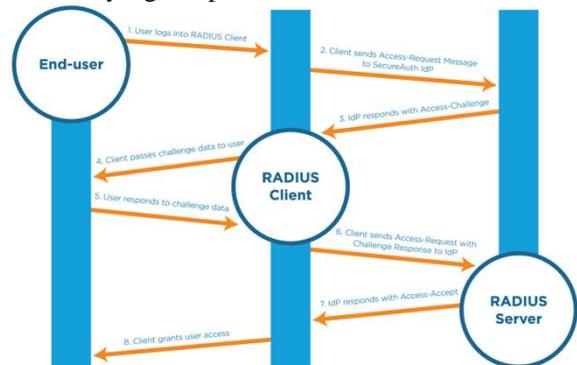
No	Nama	Port	Alamat IP
1	Mikrotik RB951Ui 2HND Router Wireles	Eth1 ( Bridge ISP)	192.168.1.19/24
		Eth1 (Hostpot)	10.5.50.1/24
		Radius Server	127.0.0.1/24
		Hostpot Radius	10.5.50.2/24
2	Komputer kasir	RJ45 NC	192.168.1.8
3	Leptop Acer client	RJ45 NC	10.5.50.254

Terdapat tiga pilar yang akan membentuk proses ini yaitu pengguna, *Network Access Server* dan radius server yang melakukan AAA (Authetication, Authorization, Acounting). Tahapannya yaitu pelanggan yang datang ke café dengan memesan produk café, kemudian petugas café memberikan akun layanan hotspot kepada pelanggan. Pengguna menghubungkan *mobile phone* atau laptop ke SSID (*service set identifier*) yang disediakan, kemudian diarahkan ke halaman *login*. Disilanjikan fase validasi dan kontrol keamanan bagi pengguna. *Radius server* sebagai *Network Access Server* melakukan validasi akun pengguna melalui AAA server. Jika radius server mengenali akun tersebut, maka server AAA akan meneruskan informasi kepada NAS bahwa akun tersebut memiliki hak menggunakan jaringan dan

mendapatkan *bandwidth* yang disediakan, serta layanan yang telah diatur oleh pengelola. Selanjutnya, dilakukan pencatatan atas aktivitas yang telah dilakukan yaitu seperti aktivitas pengguna dalam mengakses layanan, besaran data dan bandwidth yang telah digunakan, rentang waktu pengguna menggunakan layanan hotspot pada jaringan WLAN, dan lain sebagainya.

## 2. Proses Autentikasi Layanan Hotspot

Pada proses autentikasi pada layanan hotspot di jaringan WLAN, radius server berperan menangani AAA (*Authentication, Authorization, Accounting*) yaitu dengan meng-autentikasi akun pengguna, otorisasi terhadap pengguna untuk mendapatkan layanan hotspot, dan juga *accounting*, menghitung nilai layanan yang digunakan oleh pengguna. Pengguna akan memasukan akun yaitu *username* dan *password* yang diarahkan ke server radius dan server radius melakukan validasi. Server radius menerima kode akun tersebut dan memvalidasinya dengan identitas yang telah ada di database server radius, Jika akun yang dimasukan benar atau tepat dengan identitas yang ada pada database maka server akan memberikan hak akses ke jaringan WLAN, tetapi jika akun yang dimasukan adalah tidak tepat atau salah, maka server akan meminta agar akun tersebut dapat memasukan identitas dengan benar, sesuai identitas yang ada pada database.



Gambar 3. Proses Autentikasi

## 3. Konfigurasi Sistem Jaringan

- Konfigurasi Bridge\_ISP**  
Ethernet 1 dikonfigurasi sebagai *bridge\_ISP*. Merupakan metode pengelompokan *interface* yang berguna sebagai penghubung ISP dengan Mikrotik supaya menjadi satu segmen jaringan yang sama dan melakukan *bridging* antar *interface* ethernet dengan memakai jaringan wifi.
- DHCP Client pada port Bridge\_ISP**  
Setiap client akan mendapatkan ip address secara otomatis berdasarkan DHCP *bridge1\_ISP* yang digunakan sebagai alamat user agar dapat terhubung ke jaringan Hspotpot.
- DNS**  
Mengisi DNS untuk meminta informasi ip Address Google agar dapat terhubung ke

- internet menggunakan ip address 8.8.8.8 dan 8.8.4.4 yang merupakan domain name sistem dari google yang disediakan secara umum.
- d. Routing Jaringan  
Rounting di setting *default static* artinya routing yang mengarah ke *outside network*, agar semua lalu lintas keluar dapat terarah melalui Bridge1\_ISP yang sudah diseting sebagai DHCP dengan gateway 192.168.1.1.
  - e. Setting Hostpot Radius
    - 1) menyediakan adanya IP address secara dinamis yang diberikan server DHCP kepada client yang meminta IP address.
    - 2) Menyediakan sertifikat SSL untuk mengamankan proses autentikasi pengguna di jaringan *hotspot*.
    - 3) Membuat user admin yang bertugas untuk mengatur user dan kapasitas bandwidth.
    - 4) Setting alamat radius, protocol, port autentikasi, port aaccounting, dan batawan waktu.
    - 5) Membuat user profile untuk pengguna pengunjung café dan mengatur kapasitas bandwidth.
  - f. Pengujian Sistem Autentikasi User  
User di uji menggunakan account yang telah terdaftar melalui user manager Mikrotik menggunakan akses Hostpot sebagai autentikasi user. User login menggunakan browser, kemudian akan di arahkan secara otomatis ke halamn log in Mikrotik Hostpot Radius, dilakukan validasi akun, jika akun tersebut tersedia di dalam server radus dan password benar, maka sukses masuk dan mendapatkan akses internet, jika tidak valid, maka pengguna tidak mendapatkan layanan internet.

Secara keseluruhan dari hasil yang sudah dipaparkan adalah Autentikasi jaringan Hostpot Radius menggunakan munggunakan Mikrotik berkerja dengan 3 mekanisme:

1. Memverifikasi atau memvalidasi identitas user yang akan masuk kedalam sistem
2. akun yang telah terverifikasi dan tervalidasi dicatat setiap aktivitas terhubung ke jaringan WLAN yaitu dengan menghitung durasi waktu yang digunakan serta jumlah transfer datanya di jaringan.
3. Data Autentikasi user akan tercatat di server database yang kemudian dicocokkan setiap user yang mencoba login akses ke Hostpot.

## Kesimpulan

Adanya autentikasi dan pengaturan password yang komplek dapat mengurangi risiko penggunaan layanan *hotspot* di café secara ilegal dan keamanan layanan *hotspot*. Karena autentikasi telah memenuhi protokol keamanan dengan menerapkan akun temporal dan password sesuai ketentuan kaidah keamanan jaringan. Tingkat keamanan Hostpot

meningkat dengan adanya *Remote Authentication Dial-in User Service secara terpusat*. Metode Radius server pada mikrotik, sistem autentikasi User yang dibangun cukup efektif dikarenakan adanya pemantauan aktivitas user yang terhubung ke jaringan wireless LAN pada layanan *hotspot*. Pengguna yang sudah terhubung ke layanan *hotspot* dapat terkontrol penggunaan bandwidth yaitu memiliki Limitasi Profile untuk kuota 200Mb selama 2 jam dengan bandwith sebesar 2 Mbps, pada parameter upload dan download diberikan limit sebesar 200M.

## Daftar Pustaka

- [1] F. Teknik and D. Komputer, "Implementasi Hotspot Server Dan Manajemen Bandwidth Menggunakan PCQ Pada Mikrotik," 2021, Accessed: Jan. 08, 2023. [Online]. Available: <http://repository.upbatam.ac.id/id/eprint/1033>.
- [2] P. HARIANTO, "QUALITY OF SERVICE PENGGUNAAN MIKROTIK RB750GR3 MENGGUNAKAN METODE SIMPLE QUEUE UNTUK JARINGAN HOTSPOT SEBAGAI USAHA RT ...," 2022, Accessed: Jan. 08, 2023. [Online]. Available: <https://repository.mercubuana.ac.id/73022/>.
- [3] R. RIZKYANI, "ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) TERHADAP SERANGAN PACKET SNIFFING DI KANTOR KORAN SERUYA," 2019, Accessed: Jan. 08, 2023. [Online]. Available: <http://repository.uncp.ac.id/id/eprint/331>.
- [4] A. A. Gumelar, "PERANCANGAN JARINGAN HOTSPOT BERBASIS RADIUS SERVER UNTUK MANAJEMEN PENGGUNAAN INTERNET DI SMK NEGERI 3 PEKALONGAN," *SEMNAS TEKNO MEDIA ONLINE*, vol. 5, no. 1, pp. 3-8-43, Feb. 2017, Accessed: Dec. 26, 2022. [Online]. Available: <https://ojs.amikom.ac.id/index.php/semnasteknomedia/article/view/1763>.
- [5] P. Manajemen *et al.*, "Perancangan manajemen hotspot menggunakan autentikasi radius server mikrotik pada kantor walikota administrasi jakarta barat," *Repository.Nusamandiri.Ac.Id*, 2019. [https://repository.nusamandiri.ac.id/index.php/rep\\_o/viewitem/13741](https://repository.nusamandiri.ac.id/index.php/rep_o/viewitem/13741) (accessed Dec. 26, 2022).
- [6] i W. Sukartayasa and I. P. Hariyadi, "PERANCANGAN KEAMANAN JARINGAN AUTHENTICATION LOGIN HOTSPOT MENGGUNAKAN RADIUS SERVER DAN PROTOKOL EAP-TTLS PADA MIKROTIK DI IDOOP HOTEL," *J. Bumigora Inf. Technol.*, vol. 1, no. 1, pp. 51-59, Jul. 2019, doi: 10.30812/BITE.V1I1.421.
- [7] S. Qidri, M. Asfi, T. S. Ridho, and M. Hatta, "Pengelolaan Hak Akses User Jaringan Menggunakan Freeradius Untuk Login Jaringan," *J. Sains dan Inform.*, vol. 6, no. 2, pp. 183-192, Dec. 2020, doi: 10.34128/JSI.V6I2.243.
- [8] E. Agus Darmadi Politeknik Tri Mitra Karya Mandiri, B. Semper Jomin Baru, and C. - Karawang, "PERANCANGAN SISTEM

- OTENTIKASI RADIUS PADA PENGGUNA JARINGAN WIRELESS UNTUK MENINGKATKAN KEAMANAN JARINGAN KOMPUTER,” *ikraith-informatika*, vol. 2, no. 3, pp. 9–16, Nov. 2018, Accessed: Dec. 26, 2022. [Online]. Available: <https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/249>.
- [9] H. Syahputra, R. W.-M. I. U. YPTK, and undefined 2022, “Pembangunan Jaringan Hotspot Berbasis Mikrotik pada Kampung Tematik di Kecamatan Padang Utara,” *jmi-upiyptk.org*, vol. 29, pp. 60–66, 2022, doi: 10.35134/jmi.v29i1.108.
- [10] R. W. Pratama, “Implementasi Sistem Autentikasi User Menggunakan Radius Server Dan Active Directory Pada Jaringan Wireless Di PT . Kudo Teknologi Indonesia,” *ResearchGate*, no. April 2019, 2019.