Jurnal Pendidikan dan Teknologi Indonesia (JPTI)
Vol. 5, No. 12, Desember 2025, Hal. 3602-3609
DOI: https://doi.org/10.52436/1.jpti.1192
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Desain Pengamanan Jaringan Nirkabel Menggunakan Radius Server di Fakultas Teknologi Industri dan Informatika Uhamka

Abdurahman Luthfi[*1], Estu Sinduningrum[2]

[1,2]Teknik Informatika, Universitas Muhammadiyah Prof. Dr Hamka, Jakarta, Indonesia
Email: [1]abdluthfi05@gmail.com, [2]estu.ningrum@uhamka.ac.id.

Abstrak

Keamanan jaringan nirkabel menjadi isu strategis di lingkungan akademik, khususnya saat sistem autentikasi belum diterapkan secara terpusat. Penelitian ini mengambil lokasi di laboratorium teknologi informasi UHAMKA, yang sebelumnya tidak memiliki mekanisme autentikasi pengguna yang ketat, sehingga membuka potensi akses ilegal terhadap jaringan. Tujuan dari penelitian ini adalah merancang sistem keamanan jaringan nirkabel dengan menerapkan server radius sebagai pusat autentikasi, otorisasi, dan pemantauan akses pengguna. Penelitian menggunakan pendekatan *network development life cycle* (NDLC) yang terdiri dari lima tahap: analisis, desain, simulasi, implementasi, dan monitoring. Perancangan dilakukan dengan simulasi menggunakan cisco packet tracer untuk mengevaluasi struktur jaringan sebelum diterapkan secara nyata. Sistem diuji melalui metode *black box* guna menilai respon autentikasi terhadap berbagai jenis percobaan akses. Hasil menunjukkan bahwa sistem mampu membatasi akses hanya pada pengguna terdaftar, meningkatkan pengawasan lalu lintas jaringan, dan memperkuat proteksi terhadap ancaman dari luar. Penerapan sistem juga memberikan efisiensi dalam pengelolaam perangkat dan pengguna melalui pencatatan aktivitas yang sistematis. Penelitian ini menegaskan pentingnya autentikasi terpusat dalam mendukung keamanan jaringan dan kelancaran operasionnal digital di institusi Pendidikan yang memiliki aktivitas pengguna dalam jumlah besar.

Kata kunci: *Autentikasi, Cisco Packet Tracer, Infrastruktur Jaringan, Jaringan Nirkabel, Uji Black Box*

Wireless Network Security Design Using Radius Server at the Faculty of Industrial Technology and Informatics UHAMKA

Abstract

Wireless network security is a strategic issue in academic environments, especially when authentication systems have not been implemented centrally. This study was conducted at the UHAMKA information technology laboratory, which previously did hot have a strict user authentication mechanism, thus opening up the potential for illegal access to the network. The purpose of this study was to design a wireless network security system by implementing a radius server as a center for authentication, authorization, and user access monitoring. The research uses the network development life cycle (NDLC) approach, which consists of five stages: analysis, design, simulation, implementation, and monitoring. The design was carried out using simulation with cisco packet tracer to evaluate the network structure before actual implementation. The system was tested using the black box method to test the authentication response to various types of access attempts. The results show that the system is capable of restricting access to registered users only, enhancing network traffic monitoring, and strengthening protection against external threats. The implementation of the system also provides efficiciency in device and user management throught systematic activity logging. This research emphasizes the importance of centralized authentication in supporting network security and the smooth operation of digital systems in educational institutions with a small number of users.

Keywords: *Authentication, Black Box Testing, Cisco Packet Tracer, Network Infrastructure, Wireless Network*

1. PENDAHULUAN

Di Universitas Prof. Dr. Hamka (UHAMKA) sebagai salah satu institusi Pendidikan di Indonesia tidak terkecuali dari tantangan ini. Dengan ribuan pengguna aktif dan berbagai perangkat yang terhubung ke jaringan nirkabel, penting untuk merancang strategi keamanan yang efektif [1]. Salah satu solusi yang dapat digunakan adalah penggunaan *radius server* sebagai alat autentikasi dan otoritas [2]. Pesatnya perkembangan teknologi

p-ISSN: 2775-4227
e-ISSN: 2775-4219

informasi, jaringan nirkabel *wifi* telah menjadi tulang punggung komunikasi dan akses data di berbagai lingkungan, termasuk institusi pendidikan [3]. Namun penggunaan jaringan nirkabel juga membawa risiko keamanan yang signifikan. Serangan terhadap jaringan nirkabel dan pencurian data akses yang tidak sah dapat mengancam kerahasiaan dan integritas informasi yang berada dalam jaringan tersebut [4].

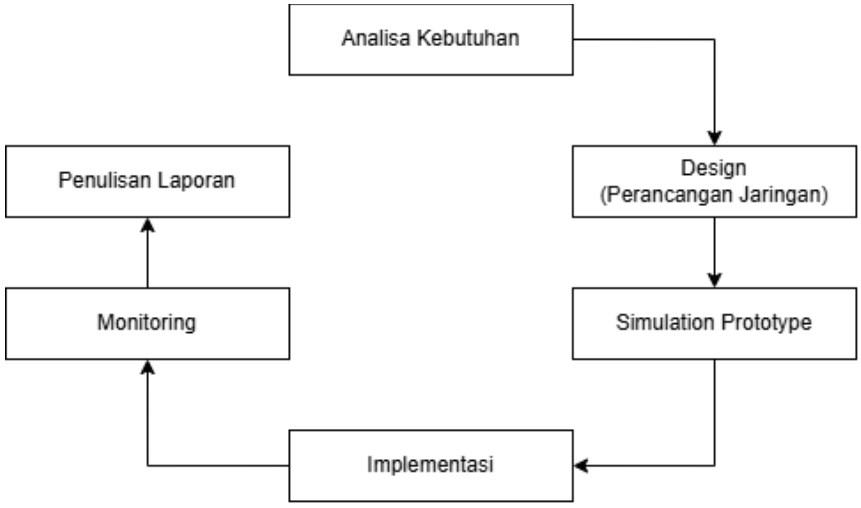
Teknologi (*WLAN)* adalah hasil Pengembangan jaringan area lokal yang awalnya menggunakan kabel kini membutuhkan koneksi nirkabel yang fleksibel, mudah, dan aman untuk menunjang kehidupan sehari-hari tanpa perlu banyak kabel [5]. Perangkat nirkabel yang menggunakan teknologi (*wifi)* tidak dapat dihindari dalam kehidupan karena permintaan informasi terbaru semakin meningkat, sebaliknya poliferasi media sosial membuat masyarakat kecanduan akses tanpa batas ke informasi melalui perangkat *mobile* [6]. Perangkat bergerak memiliki kemampuan untuk terhubung ke internet melalui *WLAN,* 802.11ac yang popular saat ini digunakan dalam jaringan nirkabel [7]. Kontrol pengguna di jaringan nirkabel, sistem otentikasi pengguna nirkabel menggunakan *radius server* dapat digunakan untuk memudahkan pengguna, meningkatkan keamanan, dan mengotentikasi mereka [8]. Akibatnya, banyak aktivitas jaringan yang sebenarnya tidak berbahaya salah di klasifikasikan sebagai ancaman [9].

Penelitian ini ditujukan untuk mengembangkan dan mengantisipasi resiko keamanan jaringan berupa serangan aktif dan pasif

2. METODE PENELITIAN

Penelitian ini memulai pendekatan yang diuji, sistematis, dan struktur untuk pengembangan jaringan komputer adalah kerangka kerja siklus pengembangan jaringan (NDLC). Metodologi ini memastikan untuk kemajuan yang luas mulai dari analisis awal hingga pemantauan berkelanjutan [10].

Dalam penelitian ini, (NDLC) digunakan dalam lima tahapan utama, yang masing-masing memiliki tujuan dan fungsi khusus. Tahapan-tahapan ini, tercantum dalam gambar 1 dan tabel 1 berikut:



Gambar 1. Diagram NDLC

Tabel 1. Tahapan-Tahapan NDLC

Tahapan NDLC	Deskripsi Umum	Aktivitas dalam penulisan
Analysis	Identifikasi kebutuhan sistem dan kelemahan infrastruktur	Mengidentifikasi kelemahan dan kebutuhan sistem pada infrastruktur jaringan nirkabel di UHAMKA, terutama kurangnya sistem autentikasi yang kuat melalui observasi dan kajian literatur.
Design	Perancangan topologi jaringan, skema akses data, dan tata letak	Menyesuaikan kebutuhan keamanan yang telah diidentifikasi dengan merancang topologi jaringan baru serta menyusun protokol autentikasi berbasis server RADIUS

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Simulation / Prototype	Simulasi desain menggunakan alat khusus untuk evaluasi kinerja awal	Melakukan simulasi rancangan menggunakan perangkat lunak jaringan seperti Cisco Packet Tracer untuk memastikan validitas dan efektivitas desain sebelum implementasi fisik.
Implementation	Penerapan rencana dan desain ke dalam sistem nyata	Mengonfigurasi server RADIUS, perangkat jaringan (seperti switch dan access point), serta melakukan pengujian konektivitas dan autentikasi di Laboratorium TI UHAMKA
Monitoring	Pemantauan berkelanjutan untuk memastikan kinerja dan mendeteksi masalah	Melakukan pemantauan terhadap jaringan untuk memastikan operasional berjalan sesuai tujuan serta mengidentifikasi potensi masalah keamanan secara proaktif.

2.1. Fase *Analysis*

Fase penting ini mencakup identifikasi komprehensif terhadap persyaratan sistem dan penilaian mendalam terhadap kelemahan infrastruktur yang ada, terutama melalui pengamatan langsung dan tinjauan literatur. Analisis tersebut secara khusus menunjukkan bahwa ketidakhadiran mekanisme otentikasi yang kuat menyebabkan masalah keamanan pada jaringan nirkabel Laboratorium IT UHAMKA.

2.2. Fase *Design*

Pada tahap ini, wawasan yang diperoleh dari fase analisis digunakan untuk merancang desain jaringan interkoneksi yang detail. Formulasi skema akses data dan perencanaan tata letak kabel fisik merupakan bagian dari tahap ini, dan hasilnya biasanya berupa diagram jaringan yang komprehensif. Proses desain spesifik dalam studi ini menghasilkan penciptaan topologi jaringan yang direkomendasikan dan rencana otentikasi berbasis server RADIUS yang efektif. Kedua skema tersebut dirancang secara cermat untuk memenuhi persyaratan keamanan yang berkembang.

2.3. Fase *Simulation Prototype*

Fase penting ini melibatkan memasukkan desain teoretis ke dalam simulasi nyata dengan menggunakan alat jaringan khusus seperti *Cisco Packet Tracer*. Tujuannya adalah untuk membantu peneliti berbicara satu sama lain dengan lebih baik dengan mengevaluasi fitur kinerja awal jaringan yang diusulkan. Sebelum implementasi fisik, simulasi terbukti sangat penting untuk memvalidasi kelayakan operasional desain. Ini memungkinkan identifikasi dini dan pengurangan potensi masalah. Pendekatan praktis dan langsung untuk memvalidasi desain jaringan jelas ditunjukkan oleh *Cisco Packet Tracer*, alat yang diakui secara luas untuk simulasi dan visualisasi jaringan standar industri. Ini menunjukkan bahwa peneliti mampu menguji konfigurasi yang berbeda secara menyeluruh, menganalisis pola aliran lalu lintas, dan dengan hati-hati memverifikasi proses autentikasi dalam lingkungan virtual yang terkontrol. Pengujian pra-implementasi adalah langkah penting dalam rekayasa jaringan profesional karena membantu menemukan dan memperbaiki kesalahan yang mungkin, mengoptimalkan kinerja, dan mengurangi risiko yang terkait dengan penerapan fisik yang mahal. Akibatnya, penggunaan alat yang sangat dihormati ini secara signifikan meningkatkan kredibilitas fase "Simulasi Prototipe" dan penerapan praktis dari temuan penelitian secara keseluruhan.

2.4. Fase *Implentation*

Fase penting ini melibatkan penerapan semua komponen yang telah direncanakan dan dirancang sebelumnya ke dalam lingkungan jaringan yang aktif. Ini menunjukkan kemampuan tim proyek untuk secara efektif menyelesaikan masalah teknis dan non-teknis yang dihadapi di lapangan. Fase implementasi termasuk konfigurasi server RADIUS dan berbagai perangkat jaringan, serta pelaksanaan pengujian dan autentikasi yang menyeluruh.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

2.5. Fase *Monitoring*

Pemantauan berkelanjutan adalah langkah penting setelah implementasi yang berhasil untuk memastikan bahwa jaringan komputer dan jalur komunikasinya beroperasi secara konsisten sesuai dengan tujuan awal pengguna dan untuk mendeteksi potensi masalah keamanan secara berkala. Fase ini memastikan pengawasan kinerja yang berkelanjutan dan memfasilitasi identifikasi proaktif kerentanan keamanan yang muncul untuk menjaga integritas dan fungsionalitas jaringan seiring waktu.

2.6. Metode Pengujian : *Black Box Testing*

black box adalah teknik pengujian perangkat lunak yang mengevaluasi fungsionalitas sistem dari perspektif eksternal, dengan fokus eksklusif pada input dan output tanpa pengetahuan tentang kode internal, struktur, atau detail implementasi sistem [11]. Metode ini sangat cocok untuk memverifikasi fungsionalitas operasional sistem autentikasi berbasis RADIUS [12]. Memungkinkan peneliti untuk memastikan bahwa pengguna dengan pernyataan yang sah dapat mengakses jaringan, sementara pengguna yang tidak sah ditolak secara efektif, memastikan sistem memenuhi tujuan keamanan inti.

Black box yang dipilih secara sengaja untuk penelitian ini memiliki konsekuensi khusus terhadap fokus dan arah praktis validasi sistem. perhatian utama adalah apakah mekanisme autentikasi dan otorisasi berfungsi dengan benar dan andal untuk pengguna aktual (yaitu, pengguna yang sah mendapatkan akses, dan pengguna yang tidak sah secara efektif diblokir) [13].

2.7. Skenario Pengujian : Black Box Testing

Pengujian dilakukan dengan beberapa skenario untuk menguji respons sistem terhadap input berbeda:

1. Pengguna valid: Login dengan kredensial sah
2. Pengguna tidak valid (salah password)
3. Pengguna tidak terdaftar dalam database RADIUS
4. Pengguna valid dengan perangkat tidak dikenali (MAC address baru)
5. Pengguna mencoba mengakses di luar jam akses yang ditentukan (jika ada pengaturan waktu).

2.8. Metode Pengambilan Sampel:

Pengujian dilakukan pada **10 perangkat** yang terdiri dari:

- 6 perangkat pengguna sah (mahasiswa & dosen)
- 4 perangkat tidak sah (perangkat dengan akun tidak valid, tidak terdaftar, atau tidak sesuai)

Setiap perangkat diuji dalam 5 percobaan login untuk setiap skenario yang ditentukan. Total percobaan: 10 perangkat x 5 skenario x 5 percobaan = 250 pengujian

2.9. Implementasi Pengujian:

1. Server Radius telah dikonfigurasi pada jaringan uji coba di Laboratorium TI UHAMKA.
2. Perangkat uji terhubung melalui Wi-Fi dengan captive portal.
3. Data hasil autentikasi dicatat melalui log server dan dianalisis untuk melihat respons sistem

3. HASIL DAN PEMBAHASAN

Jaringan di Laboratorium Teknologi Informasi UHAMKA, yang terletak di lantai 2, telah terhubung ke internet sebelum intervensi penelitian melalui penggunaan teknologi nirkabel sebagai infrastruktur utama. Namun, terdapat kekurangan keamanan jaringan yang signifikan: jaringan tidak memiliki sistem autentikasi yang kuat dan ketat. Hal ini menciptakan kerentanan yang signifikan karena memungkinkan siapa saja untuk mencoba terhubung ke Wi-Fi tanpa kontrol yang ketat. Akses tidak sah, kemungkinan pelanggaran data, dan berbagai bentuk penyalahgunaan jaringan adalah beberapa risiko besar yang mengancam jaringan sebagai akibat dari keadaan autentikasi yang kuat ini.

3.1. Analisis Dan Keadaan Jaringan

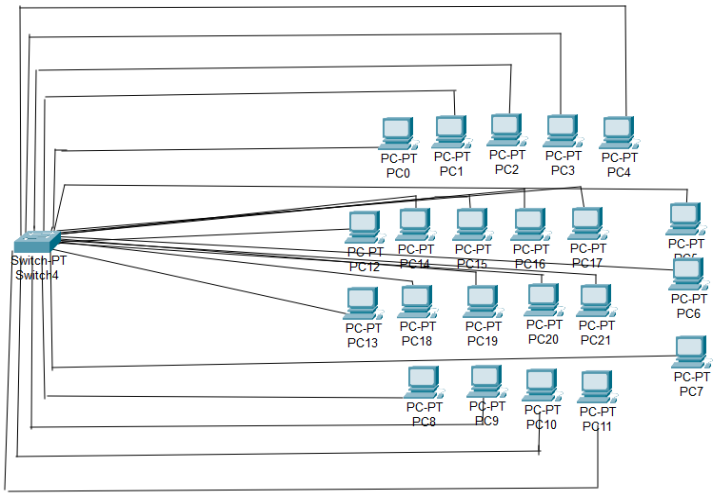
Jaringan yang ada pada Uhamka (lab Ti) lantai 2 sebelumnya telah memiliki jaringan komputer yang sudah terhubung ke jaringan internet dan menggunakan teknologi nirkabel sebagai infrastruktur jaringan. Namun, pemanfaatan teknologi nirkabel tersebut masih kurang dalam hal sistem keamanan. Oleh karena itu, sistem jaringan nirkabel yang telah ada sebelumnya didesain ulang dengan penambahan jaringan menggunakan RADIUS. Dengan adanya sistem radius tersebut, autentikasi pengguna yang akan mengakses internet dikelola oleh server

p-ISSN: 2775-4227
e-ISSN: 2775-4219

RADIUS sebagai pusat layanan yang mengatur seluruh elemen jaringan nirkabel [14]. Hanya pengguna yang telah diberikan hak akses oleh pengelola jaringan yang dapat mengakses hotspot, sehingga sistem keamanan menjadi lebih terjamin melalui penggunaan server RADIUS.

3.2. Topologi Jaringan Lama

Setelah melakukan pengamatan yang dilakukan penulis di Lab Ti UHAMKA, penulis memperoleh data terkait model topologi jaringan yang di terapkan. Untuk lebih jelasnya, penulis telah merancang topologi jaringan di Lab Ti UHAMKA seperti gambar 2 berikut:



Gambar 2. Topologi Jaringan di Lab Teknik Informatika Uhamka

Topologi jaringan pada Lab Ti UHAMKA seperti di gambar 2 di atas menggunakan topologi Star kelebihan dan kekurangan [15], sebagai infrastruktur jaringannnya.

Tabel 2. Kelebihan dan Kekurangan Topologi Star

Kelebihan	Kekurangan
Mudah menambah perangkat tanpa mengganggu jaringan aktif	Terbatas jumlah perangkat tergantung port pada switch

Penerapan tabel ini penting untuk memberikan konteks dasar dan menjaga integritas akademik. Selain sekadar mencantumkan fakta, tabel ini berfungsi sebagai dasar kritis untuk membandingkan desain baru yang diusulkan dengan integrasi RADIUS. Meskipun topologi Star secara inheren menawarkan keunggulan dalam hal kemudahan perluasan fisik dan isolasi kesalahan, keterbatasannya (jumlah terminal yang terbatas tergantung pada port switch) secara implisit menyoroti tantangan skalabilitas yang signifikan, tidak hanya untuk koneksi fisik tetapi lebih penting lagi untuk manajemen akses pengguna jika tidak dikendalikan secara terpusat. Perbandingan ini sangat penting untuk memahami mengapa desain baru diperlukan—tidak hanya untuk perbaikan keamanan segera tetapi juga untuk memfasilitasi pengelolaan yang lebih efisien dan skalabel dari basis pengguna yang terus berkembang dan dinamis. Hal ini secara efektif menggambarkan bahwa meskipun tata letak fisik berfungsi, ia kekurangan lapisan kontrol logis yang kemudian disediakan oleh implementasi RADIUS.

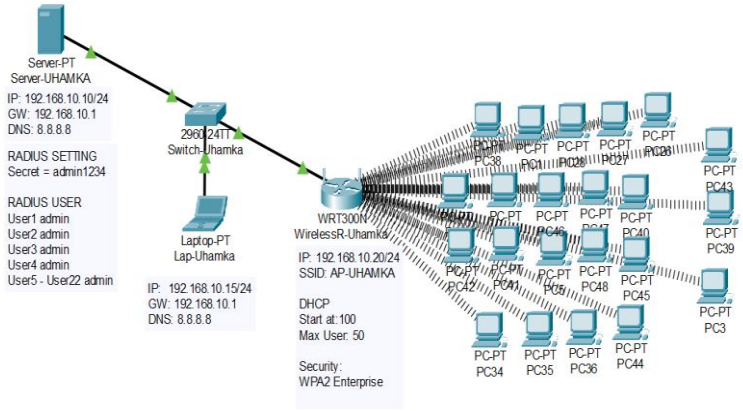
3.3. Topologi Jarigan Baru

Integrasi server RADIUS memerlukan perubahan yang menyebabkan perubahan sekitar 80% dalam desain jaringan umum. Perubahan arsitektur yang signifikan ini terutama disebabkan oleh kebutuhan untuk membangun jaringan Wi-Fi yang ditingkatkan. Namun, bagian infrastruktur fisik inti seperti Sebagian besar pengaturan tetap sama. Gambar 2 menunjukkan topologi jaringan yang didesain ulang dan diusulkan secara visual.

Pernyataan bahwa ada "perubahan 80%" dalam desain jaringan sebagai akibat dari implementasi RADIUS adalah detail kuantitatif yang sangat penting. Perubahan 80% menunjukkan perubahan arsitektur yang signifikan, bukan sekadar penyesuaian konfigurasi kecil. Alur logis autentikasi, otorisasi, pengalihan data, dan kontrol jaringan secara keseluruhan mengalami perubahan besar, meskipun infrastruktur fisik seperti switch mungkin tetap

p-ISSN: 2775-4227
e-ISSN: 2775-4219

ada. Ini menunjukkan pergeseran besar dari jaringan yang agak datar, tidak terorganisir, dan mungkin tidak aman menjadi lingkungan yang sangat terorganisir, didorong oleh kebijakan, dan sangat terstruktur. Ini menunjukkan upaya teknik yang besar dan integrasi mendalam server RADIUS ke dalam proses operasional inti jaringan. Ini berdampak pada cara perangkat terhubung, identifikasi pengguna, dan penerapan kebijakan keamanan di seluruh infrastruktur nirkabel. Ini bukan hanya penambahan server; itu adalah perombakan postur yang luas keamanan dan pendekatan jaringan.



Gambar 3. Topologi Jaringan yang disarankan

Pada gambar 3 topologi jaringan di atas, Setiap komponen sangat penting untuk menjamin bahwa sistem secara keseluruhan beroperasi dengan baik dan aman. Komponen-komponen penting yang diperlukan untuk desain yang diusulkan ditunjukkan sebagai tabel 3 berikut:

Tabel. 3. Peran dan Konfigurasi Komponen Jaringan

Komponen	Fungsi Utama
Server RADIUS	Mengelola autentikasi, otorisasi, dan akuntansi pengguna jaringan
Switch	Menghubungkan perangkat dan mengelola lalu lintas data antar perangkat
Wireless Router	Menyediakan SSID, DHCP, dan DNS untuk jaringan nirkabel
Access Point	Menyebarkan sinyal Wi-Fi dan terhubung ke server secara otomatis
Laptop/Komputer	Digunakan oleh mahasiswa untuk ujian dan aktivitas akademik lainnya

3.4. Perbandingan Jaringan Lama Dan Baru

Tabel. 4. Perbandingan Jaringan Lama Dan Baru

Aspek	Jaringan Lama (Tanpa RADIUS)	Jaringan Baru (Dengan RADIUS)
Autentikasi	Hanya SSID & password umum	Unsername & Password individual AAA
Kontrol Akses	Tidak ada	Hanya pengguna terdaftar
Monitoring	Terbatas	Log aktivitas Real-Time
Efisiensi Admin	Manual, sulit dikelola	Terpusat, mudah menambah/mencabut user
Keamanan	Rentan akses illegal	Proteksi lebih kuat & selektif

3.5. Implementasi

Server RADIUS dikonfigurasi untuk menyimpan database pengguna, terhubung ke *access point*, dan diintegrasikan dengan *captive portal*. *Switch* berperan menghubungkan perangkat utama, sementara *access point* mendistribusikan sinyal nirkabel. Setiap perangkat diuji koneksi menggunakan kredensial sah maupun tidak sah.

3.6. Pengujian

Pengujian menggunakan metode *black box testing* dengan lima skenario :

- **Pengguna sah**
- **Pengguna salah password**
- **Akun tidak terdaftar**
- **Perangkat baru**

p-ISSN: 2775-4227
e-ISSN: 2775-4219

- **Akses di luar jam operasi**

Dari total 250 percobaan, seluruh pengguna sah berhasil masuk, sedangkan pengguna ilegal ditolak sistem. *Log server* menunjukkan efektivitas autentikasi terpusat.

3.7. Diskusi

Hasil ini selaras dengan penelitian Pratama (2019) yang juga membuktikan efektivitas RADIUS dalam meningkatkan keamanan jaringan nirkabel. Perbedaannya, penelitian ini menambahkan mekanisme monitoring real-time, sehingga administrator dapat mendeteksi aktivitas mencurigakan lebih cepat. Dampak praktis yang dicapai meliputi:

- **Efisiensi administrator** → penambahan dan pencabutan akun lebih mudah.
- **Performa koneksi** → lebih stabil karena tidak ada pengguna ilegal yang membebani bandwidth.
- **Kendala** → konfigurasi awal membutuhkan waktu dan keterampilan teknis, serta server menjadi titik kritis yang harus dijaga keandalannya.

4. KESIMPULAN

Penelitian ini berhasil menunjukkan bahwa penerapan RADIUS server membawa beberapa manfaat penting:

- **Peningkatan Keamanan**: Sistem baru ini memastikan bahwa hanya pengguna dengan kredensial yang valid yang dapat terhubung ke jaringan. Hal ini mengurangi kerentanan yang sebelumnya ada, di mana siapa saja bisa mencoba terhubung tanpa kontrol yang ketat.
- **Efisiensi Pengelolaan**: Dengan sistem terpusat, administrator jaringan dapat lebih mudah menambah atau mencabut akun pengguna. Hal ini jauh lebih efisien dibandingkan dengan pengelolaan manual yang sulit.
- **Peningkatan Performa**: Karena akses ilegal dapat dicegah, tidak ada lagi pengguna yang tidak sah yang membebani *bandwidth*, sehingga koneksi menjadi lebih stabil. Jaringan yang lebih andal dan aman ini sangat mendukung kegiatan akademik, penelitian, dan operasional di lab.

Penelitian ini tidak hanya membuktikan keefektifan RADIUS server, sejalan dengan temuan dari penelitian sebelumnya, tetapi juga menambahkan **mekanisme pemantauan waktu nyata (real-time monitoring)** yang memungkinkan administrator untuk mendeteksi aktivitas mencurigakan dengan lebih cepat. Kontribusi ini memperkaya penerapan sistem keamanan jaringan di institusi pendidikan. Secara keseluruhan, penelitian ini menegaskan pentingnya otentikasi terpusat untuk menjaga kelancaran operasi digital di lingkungan dengan banyak pengguna.

DAFTAR PUSTAKA

[1] W. Najib and S. Sulistyo, "Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 9, no. 4, pp. 375–384, 2020.

[2] R. Rahman, "IMPLEMENTASI JARINGAN FIBER OPTIC DAN HOTSPOT SERVER RT RW NET BERBASIS MIKROTIK DENGAN FITUR MIKHMON DI FAST. NET," 2024, *UNUSIA*.

[3] M. S. Rahayu, "Kemampuan Komunikasi Persuasif Sales Balifiber untuk Menarik Konsumen di Wilayah Jakarta Timur 1," 2024, *Universitas Nasional*.

[4] A. Saraun, A. S. M. Lumenta, and D. F. Sengkey, "An Analysis of WLAN Security at the Minahasa Regency Office of Educational Affairs," *J. Tek. Inform. vol*, vol. 17, no. 1, pp. 565–572, 2021.

[5] B. V. Indriyono, E. H. Rachmawanto, C. Umam, N. Pamungkas, and F. Y. Saidalvi, "Sistem Kendali Kunci Otomatis Pada Motor Matic Menggunakan Mikrokontroler Berbasis Android," in *Seminar Nasional Inovasi dan Pembangunan Teknologi Terapan (SENOVTEK)*, 2022, pp. 79–92.

[6] L. E. Yulianti, "Netiquette: penguatan soft skill netizen untuk generasi berkarakter," *JIRA J. Inov. dan Ris. Akad.*, vol. 2, no. 11, pp. 1532–1554, 2021.

[7] H. HABIBI, S. H. Anwariningsih, and A. Charolina, "Desain dan Konfigurasi Jaringan Komputer di Kantor Sekretariat Daerah Kota Salatiga," 2020, *Universitas Sahid Surakarta*.

[8] R. W. Pratama, "Implementasi Sistem Autentikasi User Menggunakan Radius Server Dan Active Directory Pada Jaringan Wireless Di PT. Kudo Teknologi Indonesia," *Res. no. April*, vol. 2019, 2019.

[9] K. A. Nugroho, T. Hariguna, A. S. Barkah, M. I. Komputer, U. A. Purwokerto, and U. A. Purwokerto, "Deteksi Anomali Trafik Jaringan dan Aktivitas Pengguna Menggunakan Isolation Forest untuk

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Meningkatkan Keamanan Jaringan Network Traffic and User Activity Anomaly Detection Using Isolation Forest to Improve Network Security," vol. 5, no. 5, pp. 1365–1376, 2025.

[10] N. Nurdadyansyah and M. Hasibuan, "Perancangan Local Area Network Menggunakan NDLC Untuk Meningkatkan Layanan Sekolah," *J. KONIK*, vol. 5, pp. 342–346, 2021.

[11] N. H. Nawawi, "RANCANG BANGUN APLIKASI SOSIAL MEDIA BERBASIS MOBILE MENGGUNAKAN FLUTTER STUDI KASUS PT CRANIUM ROYAL ADITAMA," 2024, *Sekolah Tinggi Teknologi Terpadu Nurul Fikri*.

[12] E. A. Apriadi, "BAB 4 AUTENTIKASI DAN OTORISASI," *Keamanan Jar. Komput.*, p. 44, 2025.

[13] R. SAPUTRA, "ANALISIS PENERAPAN SISTEM INFORMASI AKUNTANSI DALAM PROSES TRANSAKSI AUTOMATED TELLER MACHINE (ATM) UNTUK PROSES YANG LEBIH EFEKTIF PADA PT BANK SUMUT KCP SEI SIKAMBING MEDAN," 2024, *Fakultas Sosial Sains*.

[14] I. Baihaqi, "PERANCANGAN SISTEM MANAJEMEN RADIUS SERVER UNTUK KEAMANAN AKSES PERANGKAT JARINGAN BERBASIS WEB".

[15] A. M. Saprizal and G. Amori, "ANALISIS IMPLEMENTASI TOPOLOGI STAR DAN HYBRID STUDI KASUS JARINGAN MULTIMEDIA SARI MULIA," *KOMNET J. Komputer, Jar. dan Internet*, vol. 3, no. 1, pp. 116–120, 2024.