ISSN: 2503-054X
Vol. 10 No: 1, April 2025

# Implementasi Firewall MAC Address Filtering Pada Keamanan Jaringan WLAN

1st Taufiq Timur Warisaji
Universitas Muhammadiyah Jember
Jember, Indonesia
taufiqtimur@unmuhjember.ac.id

2nd Ulya Anisatur Rosyidah
Universitas Muhammadiyah Jember
Jember, Indonesia
ulyaanisatur@unmuhjember.ac.id

3th Lintang Setyo Kurniawati
Universitas Muhammadiyah Jember
Jember, Indonesia
lintang@unmuhjember.ac.id

***Abstract*— Penggunaan jaringan nirkabel berbasis 802.11 telah menjadi salah satu layanan jaringan yang paling banyak digunakan, tetapi hal ini juga meningkatkan kerentanan keamanan. Meningkatnya akses tidak sah ke jaringan nirkabel sering kali dikaitkan dengan ketersediaan perangkat lunak dan alat yang dapat diunduh secara daring untuk mendekripsi enkripsi keamanan nirkabel. Untuk mengurangi akses tidak sah, sistem keamanan berlapis dapat diterapkan dengan menggabungkan fitur-fitur seperti Hotspot Login dan MAC address filtering. Sistem berlapis ini dapat memblokir pengguna yang mencoba mengakses jaringan tanpa otorisasi dengan memverifikasi hak akses dua kali: dengan mencocokkan nama pengguna dan kata sandi yang dimasukkan selama Hotspot Login dengan alamat MAC perangkat klien. Temuan penelitian menunjukkan bahwa klien yang menggunakan perangkat yang berbeda, bahkan dengan nama pengguna dan kata sandi yang sama, tidak dapat mengakses jaringan. Oleh karena itu, setiap klien yang ingin terhubung ke internet harus menggunakan perangkat dengan alamat MAC terdaftar dan hak akses pengguna dan kata sandi yang sesuai seperti yang ditentukan dalam Hotspot Login.**

***Kata kunci — hotspot login, MAC address filtering, wireless security***

## I. PENDAHULUAN

Perkembangan pesat perangkat WiFi telah mengubah konektivitas dalam kehidupan modern, dengan perkiraan menunjukkan lebih dari 10 miliar unit terjual secara global, dan lebih dari 4,5 miliar masih digunakan secara aktif. Pertumbuhan ini didorong oleh meningkatnya permintaan teknologi nirkabel di berbagai sektor. Pergeseran ke arah konektivitas nirkabel telah menyebabkan penjualan perangkat dengan WiFi tertanam yang signifikan, melampaui 1 miliar unit pada tahun 2011 dan diproyeksikan akan melampaui 2 miliar pada tahun 2015 [1] . Perluasan jaringan area lokal nirkabel (WLAN) telah difasilitasi oleh perubahan peraturan, yang memungkinkan adopsi yang luas di rumah dan lembaga [2] . Sebagian besar lalu lintas data seluler dialihkan ke jaringan WiFi, dengan perkiraan yang menunjukkan bahwa pada tahun 2015, hampir 9.000 petabyte data seluler akan ditransfer melalui WiFi. Tren ini menggarisbawahi peran penting WiFi dalam mengelola meningkatnya permintaan layanan data, terutama karena lalu lintas seluler diperkirakan akan tumbuh secara signifikan[1]. Meskipun manfaat teknologi WiFi sudah jelas, kekhawatiran mengenai dampaknya terhadap keamanan dan kesehatan masih ada, sehingga mendorong penelitian dan wacana publik yang terus berlanjut mengenai implikasi penggunaan perangkat nirkabel secara luas [3]

Ada beberapa penelitian tentang kerentanan inheren karena sifat siaran gelombang radio yang memerlukan kebijakan autentikasi yang kuat untuk melindungi dari berbagai ancaman keamanan. Kebijakan ini penting untuk mencegah akses tidak sah, modifikasi data, dan serangan penolakan layanan. Certificateless Aggregate Signcryption: Skema baru yang diusulkan untuk jaringan sensor medis nirkabel meningkatkan autentikasi dan integritas data sekaligus menjaga privasi. Skema ini menggunakan jaringan saraf tiruan untuk mencapai kompleksitas rendah dan efisiensi tinggi dalam mengamankan data medis [4] . Jamming and Spoofing Detection: Arsitektur deteksi inovatif telah dikembangkan untuk melawan serangan jamming dan spoofing, yang dapat mengganggu komunikasi secara serius. Arsitektur ini memanfaatkan teori pengujian hipotesis untuk meningkatkan integritas sinyal dan keamanan lokasi di jaringan 4G/5G [5]. Jamming Attack Detection: Dua skema deteksi untuk serangan jamming selama autentikasi lapisan fisik telah diusulkan, dengan fokus pada perbedaan varians noise untuk meningkatkan keamanan terhadap peniruan identitas dan penolakan sinyal [6]. User Grouping and Power Optimization: Kerangka kerja untuk sistem mmWave-NOMA menangani keamanan dengan mengklasifikasikan pengguna berdasarkan kondisi saluran, mengoptimalkan alokasi daya untuk meningkatkan kerahasiaan terhadap penyadap [7]. Meskipun perkembangan di bidang ini secara signifikan memperkuat keamanan jaringan nirkabel, ancaman siber yang terus berkembang memerlukan inovasi berkelanjutan dalam mekanisme autentikasi dan deteksi untuk tetap unggul terhadap potensi kerentanan.

Banyak pengguna jaringan nirkabel tidak menyadari risiko yang ada saat mereka terhubung ke Wireless Access Point (WAP), seperti kemungkinan sinyal WLAN dikompromikan oleh peretas. Menghubungkan ke Wireless Access Point (WAP) melibatkan beberapa risiko, terutama terkait dengan kerentanan keamanan dan masalah kinerja jaringan. Risiko ini dapat muncul dari berbagai faktor, termasuk akses tidak sah, intersepsi data, dan gangguan jaringan. Memahami risiko ini sangat penting untuk mengembangkan strategi yang efektif untuk menguranginya. Location Forgery and Privacy Concerns: Pengguna yang terhubung ke WAP mungkin menghadapi risiko terkait pemalsuan lokasi dan pelanggaran privasi. Sistem seperti PriLA bertujuan untuk mengatasi masalah ini dengan menggunakan tanda tangan lapisan fisik untuk mengautentikasi lokasi pengguna tanpa membocorkan informasi yang signifikan. Namun, risiko data lokasi dipalsukan atau disalahgunakan tetap menjadi perhatian [8]. Denial of Service (DoS) dan Replay Attacks: Dalam jaringan seluler, khususnya yang menggunakan WiMAX, pengguna rentan terhadap serangan DoS dan replay selama serah terima antara titik akses. Skema pra-autentikasi berbasis EAP yang disempurnakan telah diusulkan untuk mengurangi kerentanan ini, tetapi skema tersebut masih memerlukan implementasi yang cermat untuk memastikan keamanan [9]. Channel



No. 1-005/Vol. 9/2025/TechnoXplore
DOI 10.36805/technoxplore.v10i1. 8331

ISSN: 2503-054X
Vol. 10 No: 1, April 2025

Interference: Dalam jaringan nirkabel yang digunakan secara padat, interferensi saluran merupakan risiko yang signifikan. Interferensi ini dapat menyebabkan masalah terminal yang tersembunyi dan terbuka, yang menurunkan kinerja jaringan. Solusinya melibatkan sistem kerja sama AP yang mendeteksi dan mengelola masalah ini, tetapi memerlukan sinkronisasi dan koordinasi yang tepat [10]. Blockage and Connectivity Challenges: Dalam jaringan mmWave, penyumbatan dapat menyebabkan konektivitas yang tidak stabil, yang memengaruhi keandalan. Konektivitas multititik yang terkoordinasi dan desain beamformer yang kuat diusulkan untuk mengatasi tantangan ini, tetapi melibatkan proses komputasi yang kompleks [11]. Energy Constraints: Dalam jaringan komunikasi bertenaga nirkabel, mobilitas titik akses dapat menyebabkan kendala energi, yang memengaruhi transmisi data. Mengoptimalkan konsumsi dan pemanenan energi sangat penting untuk memaksimalkan throughput, tetapi melibatkan masalah pengoptimalan yang kompleks [12]. Sementara makalah ini menyoroti risiko signifikan yang terkait dengan koneksi ke WAP, mereka juga mengusulkan solusi inovatif untuk mengurangi risiko ini. Namun, penerapan solusi ini memerlukan pertimbangan cermat terhadap sumber daya komputasi, arsitektur jaringan, dan masalah privasi pengguna. Menyeimbangkan keamanan, kinerja, dan efisiensi energi tetap menjadi tantangan kompleks dalam manajemen jaringan nirkabel.

IEEE 802.11 telah menjadi salah satu jaringan nirkabel yang paling umum digunakan. Peretas dan penyusup dapat mengeksploitasi internet untuk menemukan kelemahan keamanan karena sifat media nirkabel yang terbuka. Sistem keamanan MAC Address Filtering adalah metode yang digunakan untuk meningkatkan keamanan jaringan dengan mengendalikan akses berdasarkan alamat MAC perangkat. Sistem ini khususnya relevan dalam jaringan nirkabel dan Jaringan Area Lokal (LAN), yang membantu mencegah akses tidak sah dan mengurangi berbagai jenis serangan. Jaringan sensor nirkabel rentan terhadap injeksi data palsu oleh node yang disusupi. Skema Location and Optimal Coverage based Filtering (LOCF) meningkatkan keamanan dengan mengharuskan laporan untuk menyertakan dukungan dari beberapa sensor, yang diverifikasi melalui MAC dan lokasi sensor. Pendekatan ini meningkatkan efisiensi penyaringan dan ketahanan terhadap node yang disusupi [13]. Skema sink filtering dalam jaringan sensor heterogen menggunakan kepala kluster untuk menggabungkan data, yang harus menyertakan beberapa MAC dari sensor dasar. Metode ini tangguh terhadap kompromi node dan secara efisien menyaring laporan palsu.

Penggunaan MAC addresses sebagai pengenal unik dalam perangkat jaringan memainkan peran penting dalam mengendalikan akses dan meningkatkan keamanan. Firewall sering menggunakan alamat ini untuk menyaring koneksi, sehingga mencegah akses yang tidak sah. Namun, efektivitas dan keamanan sistem berbasis MAC addresses dipengaruhi oleh berbagai faktor, termasuk potensi spoofing alamat dan kebutuhan akan enkripsi yang kuat serta mekanisme deteksi intrusi. MAC addresses berfungsi sebagai pengenal unik untuk perangkat jaringan, yang memungkinkan firewall untuk menyaring koneksi dan mencegah akses yang tidak sah. Ini penting untuk menjaga keamanan jaringan, terutama di lingkungan dengan banyak perangkat yang terhubung, seperti jaringan IoT . Standar MAC IEEE 802.15.4 menggabungkan bidang keamanan di header MAC, yang penting untuk mengautentikasi data sensitif. Ini dicapai melalui metode pembuatan kunci yang dioptimalkan, seperti kriptosistem kunci publik ElGamal, yang meningkatkan keamanan data dalam aplikasi IoT [14].

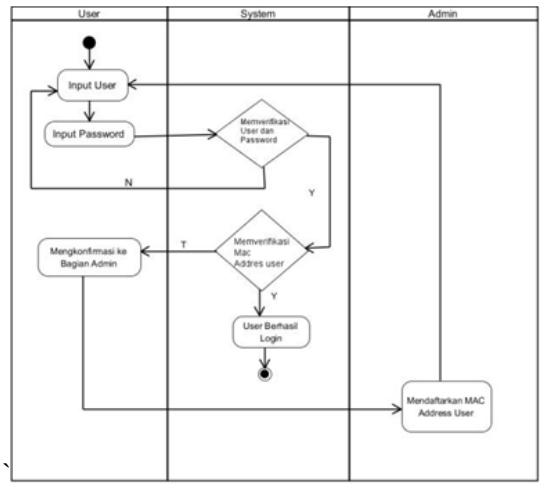
Keamanan berlapis dalam jaringan nirkabel adalah pendekatan komprehensif yang melibatkan beberapa langkah keamanan di berbagai lapisan tumpukan protokol jaringan untuk melindungi dari berbagai ancaman. Keamanan berlapis melibatkan penerapan langkah keamanan di beberapa lapisan tumpukan protokol jaringan, yang menyediakan pertahanan bertingkat terhadap potensi ancaman. Pendekatan ini bermanfaat dalam jaringan ad hoc seluler, tempat node berkomunikasi secara peer-to-peer tanpa bergantung pada infrastruktur yang telah ditentukan sebelumnya [14], [15] . Sistem hotspot login adalah komponen penting dari keamanan berlapis, yang menyediakan lapisan autentikasi awal bagi pengguna yang mengakses jaringan nirkabel. Sistem ini sering menggunakan beberapa protokol autentikasi, seperti teknik tantangan-respons, untuk memverifikasi identitas pengguna dan mencegah akses yang tidak sah . MAC address filtering adalah lapisan keamanan lain yang membatasi akses jaringan ke perangkat dengan alamat MAC tertentu. Metode ini menyediakan tingkat kontrol akses dasar, yang mencegah perangkat yang tidak sah terhubung ke jaringan . Penerapan filtering berdasarkan MAC Address memungkinkan pembatasan akses hanya untuk perangkat tertentu yang dapat tersambung ke jaringan wireless hotspot, dengan mempertimbangkan kombinasi IP Address dan MAC Address yang telah didaftarkan . Diharapkan bahwa keamanan berlapis ini mampu meningkatkan perlindungan terhadap jaringan komputer. Karena frekuensi jaringan wireless lebih mudah diakses dibandingkan jaringan kabel, maka sistem komunikasi wireless menjadi lebih rentan terhadap potensi ancaman keamanan. Oleh sebab itu, diperlukan penerapan tindakan keamanan yang lebih ketat pada jaringan wireless. Beberapa penelitian sebelumnya menunjukkan bahwa celah pada sistem login hotspot dapat dieksploitasi oleh pihak yang tidak berwenang, yang berpotensi mengganggu stabilitas jaringan serta membahayakan privasi pengguna sah [16],[17]. Kondisi ini menjadi alasan penting bagi penerapan sistem keamanan berlapis pada jaringan wireless, seperti penggunaan sistem login hotspot dan filtering MAC Address. Dengan sistem ini, setiap perangkat yang ingin mengakses jaringan internet harus terlebih dahulu mendaftarkan MAC Address-nya. Hanya perangkat yang telah terdaftar yang diperbolehkan terhubung ke jaringan, sementara perangkat yang belum terdaftar akan otomatis diblokir dari akses.

## II. METODE PENELITIAN

Dalam penelitian mengenai Optimasi Keamanan Jaringan Wireless melalui MAC Address Filtering, penulis memanfaatkan perangkat Mikrotik RouterBoard 951Ui-2HND. Perangkat tersebut dikonfigurasi dalam dua mode access point, yaitu mode station untuk mengakses jaringan internet, serta mode ap bridge untuk terhubung ke jaringan lokal. Konfigurasi ini bertujuan untuk melakukan pengujian terhadap konektivitas dan keamanan jaringan. Penerapan keamanan berlapis, berupa login hotspot dan MAC Address filtering, diharapkan mampu mencegah akses tidak sah dari pengguna asing ke jaringan wireless.


No. 1-005/Vol. 9/2025/TechnoXplore
DOI 10.36805/technoxplore.v10i1. 8331

ISSN: 2503-054X
Vol. 10 No: 1, April 2025




**Gambar 1** Activity Diagram

Penelitian ini menggunakan metode Security Policy Development Life Cycle (SPDLC), yang mencakup enam tahapan yang dapat dilihat pada gambar 2 dan dijelaskan dibawah ini :


**Gambar 2** Model SPDLC

a. Identifikasi: Tahapan ini bertujuan untuk mengenali permasalahan yang berkaitan dengan keamanan jaringan wireless. Ini termasuk identifikasi perangkat yang terhubung ke jaringan, area yang berpotensi rawan, dan kerentangannya. Proses ini penting untuk memahami resiko yang akan di hadapi jaringan tersebut.

b. Analisis: Pada tahap ini, dilakukan uji coba guna mengidentifikasi potensi risiko dan ancaman terhadap keamanan jaringan wireless. Hal ini meliputi identifikasi perangkat yang terhubung ke jaringan, potensi area rawan, serta ancaman, dan kerentanannya.proses ini penting untuk memahami resiko yang di hadapi oleh jaringan tersebut.

c. Perancangan (Design): Peneliti menyusun rancangan sistem keamanan jaringan dengan menerapkan MAC Address filtering. Metode ini digunakan untuk membatasi akses ke jaringan hanya pada perangkat yang memiliki alamat MAC yang terdaftar.

d. Implementasi: Pada tahap ini, dilakukan konfigurasi sistem keamanan jaringan wireless, disertai dengan pengujian konektivitas untuk menilai efektivitas sistem yang telah diterapkan. Konfigurasi mencakup penerapan MAC Address filtering untuk membatasi akses hanya pada perangkat yang telah terdaftar, serta penguatan keamanan, mengatur firewall untuk menyaring lalu lintas mencurigakan.

e. Audit: Tahapan ini digunakan untuk mengevaluasi dan memverifikasi efektivitas sistem keamanan yang telah diimplementasikan. audit ini dapat berupa pengujian mengidentifikasi masalah atau celah yang mungkin muncul setelah sistem dimulai. Tujuan utamanya adalah untuk memastikan bahwa kontrol yang di terapkan dapat menangkal ancaman.

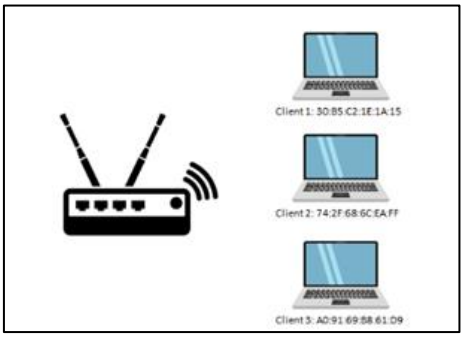
f. Evaluasi: Dilakukan peninjauan menyeluruh terhadap sistem keamanan guna menilai kinerja dan efektivitas dari keseluruhan proses yang telah dijalankan. Melibatkan pengumpulan tentang efektivitas kebijakan keamanan, termasuk analisis kinerja, keandalan, dan efek sistem keamanan terhadap operasional jaringan. Hasil evaluasi akan digunakan untuk memperbaiki dan pengembangan kebijakan keamanan di masa mendatang.

## III. HASIL DAN PEMBAHASAN

Untuk menerapkan Wireless Security Optimization dengan metode MAC Address Filtering, penulis menggunakan skema jaringan seperti yang ditunjukkan pada Gambar 2, dengan rincian IP Address yang tercantum pada Tabel 1.


No. 1-005/Vol. 9/2025/TechnoXplore
DOI 10.36805/technoxplore.v10i1. 8331

ISSN: 2503-054X
Vol. 10 No: 1, April 2025




**Gambar 3** Skema Jaringan

Gambar 3 menyajikan skema jaringan yang diterapkan dalam penelitian ini, di mana client 1 memiliki MAC Address 30:B5:C2:1E:1A:15, client 2 memiliki MAC Address 74:2F:68:6C:EA:FF, dan client 3 menggunakan MAC Address A0:91:69:B8:61:D9. Setiap client memperoleh akses jaringan setelah melalui proses autentikasi melalui sistem login Hotspot, dengan kredensial username dan password yang bersifat individual. Adapun spesifikasi IP Address masing-masing perangkat tercantum pada Tabel 1.

**Tabel 1.** IP Address

| Interface | IP Address | Network |
|---|---|---|
| Wlan1 (to Public) | 192.168.43.1 | 192.168.43.0 |
| Ether2 (to Local) | 192.168.2.1 | 192.168.2.0 |
| Wlan2 (to Local) | 192.168.10.1 | 192.168.10.0 |
| Client 1 | DHCP Client | 192.168.10.0 |
| Client 2 | DHCP Client | 192.168.10.0 |
| Client 3 | DHCP Client | 192.168.10.0 |

Sebagaimana ditunjukkan pada Tabel 1, antarmuka WLAN 1 dengan alokasi IP Address 192.168.43.1 berperan sebagai penghubung menuju jaringan IP publik. Sementara itu, antarmuka ether2 yang menggunakan IP Address 192.168.2.1 difungsikan sebagai gateway bagi jaringan lokal berbasis kabel. Adapun antarmuka WLAN 2 dengan IP Address 192.168.10.1 berfungsi sebagai gateway untuk jaringan lokal berbasis nirkabel.

**Tabel 2.** User dan Password

| MAC Address | User | Password |
|---|---|---|
| 30:B5:C2:1E:1A:15 | FMY | FMY2020 |
| 74:2F:68:6C:EA:FF | RAP | RAP2020 |
| A0:91:69:B8:61:D9 | RCD | RCD2020 |

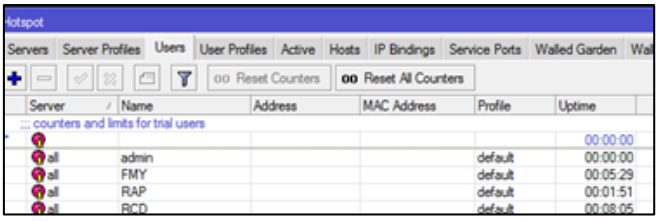
Tabel 2 memaparkan rincian hak akses klien untuk terhubung ke jaringan nirkabel. Akun pengguna FMY dengan kata sandi FMY2020 hanya dapat diakses oleh klien dengan MAC Address 30:B5:C2:1E:1A:15, sedangkan akun RAP dengan kata sandi RAP2020 terbatas pada klien dengan MAC Address 74:2F:68:6C:EA:FF. Sementara itu, akun RCD hanya dapat digunakan oleh klien yang memiliki MAC Address A0:91:69:B8:61:D9. Dalam upaya mengoptimalkan keamanan jaringan nirkabel melalui metode penyaringan MAC Address, dilakukan dua skenario pengujian. Pada skenario pertama, seluruh klien diizinkan mengakses jaringan menggunakan kombinasi username dan password tanpa pembatasan alamat MAC. Sebaliknya, pada skenario kedua, akses jaringan dibatasi secara spesifik berdasarkan kombinasi antara username, password, dan MAC Address yang telah ditentukan..

A. *Simulasi pengujian konektivitas 1*

Pada tahap pengujian konektivitas dalam skenario 1, peneliti melakukan evaluasi terhadap keamanan jaringan nirkabel dengan memanfaatkan mekanisme login Hotspot. Gambar 3 menunjukkan bahwa pengguna Hotspot berhasil terhubung ke jaringan nirkabel. Terdapat tiga pengguna yang telah diberikan otorisasi akses untuk terhubung ke jaringan melalui sistem keamanan login Hotspot.

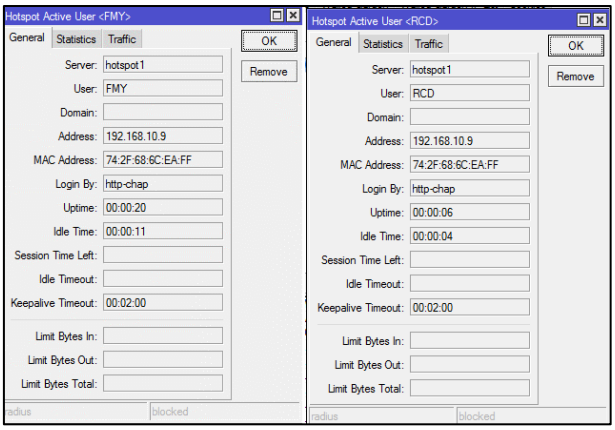

No. 1-005/Vol. 9/2025/TechnoXplore
DOI 10.36805/technoxplore.v10i1. 8331

ISSN: 2503-054X
Vol. 10 No: 1, April 2025




**Gambar 4** User

Penerapan sistem keamanan jaringan nirkabel melalui mekanisme login Hotspot memungkinkan pembatasan akses pengguna berdasarkan kombinasi username dan password yang telah ditentukan oleh administrator jaringan. Namun demikian, pendekatan ini masih memiliki kelemahan. Sebagaimana ditunjukkan pada Gambar 4, terdapat klien dengan MAC Address 74:2F:68:6C:EA:FF yang berhasil melakukan login menggunakan akun pengguna FMY dan RCD, meskipun MAC Address tersebut seharusnya hanya digunakan oleh pengguna RAP.




**Gambar 5** Pengguna Aktif Hotspot

Tabel 3 mengilustrasikan adanya kerentanan dalam sistem keamanan jaringan nirkabel yang hanya mengandalkan login Hotspot. Apabila seorang klien mengetahui kombinasi username dan password milik klien lain, maka ia dapat memanfaatkan informasi tersebut untuk mengakses jaringan Wi-Fi. Pada tabel tersebut, klien 1 dengan MAC Address 30:B5:C2:1E:1A:15 mampu melakukan login menggunakan akun FMY, RAP, dan RCD. Hal serupa terjadi pada klien 2 dengan MAC Address 74:2F:68:6C:EA:FF, yang juga berhasil masuk menggunakan ketiga akun tersebut. Bahkan, klien 3 dengan MAC Address A0:91:69:B8:61:D9—yang seharusnya hanya memiliki akses melalui akun RCD—dapat terhubung ke jaringan nirkabel menggunakan akun FMY dan RAP. Kelemahan pada sistem login Hotspot ini berpotensi dimanfaatkan oleh pihak yang tidak berwenang untuk mengganggu kestabilan jaringan serta membahayakan privasi pengguna yang akunnya disalahgunakan.

Tabel 3. Spesifikasi Keamanan Hotspot Login

| MAC Address | USER | PASSWORD | KONEKTIVITAS |
|---|---|---|---|
| 30:B5:C2:1E:1A:15 | FMY | FMY2020 | OK |
| | RAP | RAP2020 | OK |
| | RCD | RCD2020 | OK |
| 74:2F:68:6C:EA:FF | FMY | FMY2020 | OK |
| | RAP | RAP2020 | OK |
| | RCD | RCD2020 | OK |
| A0:91:69:B8:61:D9 | FMY | FMY2020 | OK |
| | RAP | RAP2020 | OK |
| | RCD | RCD2020 | OK |

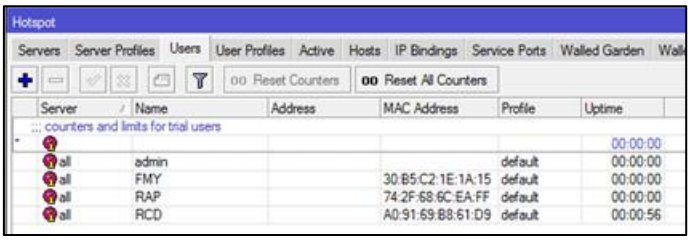
B. *Simulasi uji konektivitas 2*

Skenario pengujian jaringan nirkabel kedua adalah membandingkan keamanan jaringan nirkabel menggunakan login hotspot dengan penyaringan alamat MAC. Pendekatan ini bertujuan untuk mengurangi risiko seperti yang dijelaskan dalam tabel 3, di mana semua nama pengguna dan kata sandi dapat digunakan oleh siapa saja selama mereka mengetahui informasi login. Gambar 5 menjelaskan bahwa setiap pengguna yang akan terhubung ke jaringan nirkabel harus mendaftarkan alamat MAC mereka di daftar Pengguna Hotspot. Tujuannya adalah agar nama pengguna FMY hanya dapat digunakan oleh perangkat dengan Alamat MAC

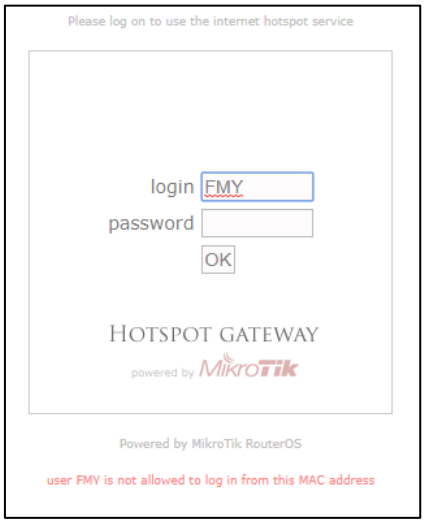

No. 1-005/Vol. 9/2025/TechnoXplore
DOI 10.36805/technoxplore.v10i1. 8331

ISSN: 2503-054X
Vol. 10 No: 1, April 2025

30:B5:C2:1E:1A:15, nama pengguna RAP hanya oleh perangkat dengan Alamat MAC 74:2F:68:6C:EA:FF, dan nama pengguna RCD hanya oleh perangkat dengan Alamat MAC A0:91:69:B8:61:D9. Ketika ada klien yang mencoba mengakses jaringan menggunakan nama pengguna dan kata sandi yang berbeda, MikroTik RouterBoard akan secara otomatis menolaknya, seperti yang ditunjukkan pada Gambar 6. Gambar 6 dan 7 menjelaskan bahwa klien dengan alamat MAC yang berbeda mencoba mengakses jaringan nirkabel menggunakan akun FMY, tetapi perangkat tidak dapat terhubung ke jaringan komputer.

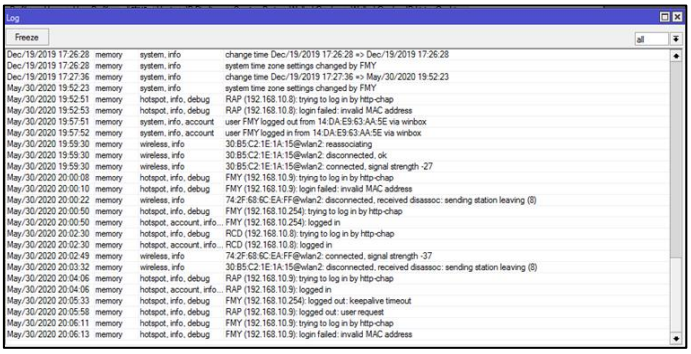



**Gambar 6** MAC Address Pengguna Hotspot




**Gambar 7 Login MAC Address**

Tabel IV menunjukkan hasil pengujian konektivitas jaringan nirkabel menggunakan login hotspot dengan filter alamat MAC. Sebelum filter ini, semua klien dapat menggunakan nama pengguna dan kata sandi siapa pun. Namun, setelah filter alamat MAC diterapkan, pengguna FMY hanya dapat diakses oleh perangkat dengan alamat MAC 30: B5: C2: 1E: 1A: 15, sedangkan pengguna RAP hanya dapat digunakan oleh perangkat dengan alamat MAC 74: 2F: 68: 6C: EA: FF.




**Gambar 8 Percobaan Login Menggunakan MAC Address Berbeda**

Tabel 4. Uji Konektivitas


No. 1-005/Vol. 9/2025/TechnoXplore
DOI 10.36805/technoxplore.v10i1. 8331

ISSN: 2503-054X
Vol. 10 No: 1, April 2025

| MAC Address | USER | PASWD | KONEKTIVITAS | |
|---|---|---|---|---|
| | | | AFTER | BEFORE |
| 30:B5:C2:1E:1A:15 | FMY | FMY2020 | OK | OK |
| | RAP | RAP2020 | OK | BLOCK |
| | RCD | RCD2020 | OK | BLOCK |
| 74:2F:68:6C:EA:FF | FMY | FMY2020 | OK | BLOCK |
| | RAP | RAP2020 | OK | OK |
| | RCD | RCD2020 | OK | BLOCK |
| A0:91:69:B8:61:D9 | FMY | FMY2020 | OK | BLOCK |
| | RAP | RAP2020 | OK | BLOCK |
| | RCD | RCD2020 | OK | OK |

## IV. KESIMPULAN

Penerapan keamanan jaringan nirkabel dengan MAC address filtering efektif untuk memblokir pengguna yang mencoba mengakses jaringan tanpa izin. Model keamanan berlapis yang menggabungkan hotspot login dan MAC address filtering ini mampu meningkatkan perlindungan bagi infrastruktur jaringan dan pengguna layanan. Sistem keamanan ini melakukan verifikasi hak akses sebanyak dua kali, yaitu dengan cara mencocokkan username dan password pada hotspot login dengan MAC address perangkat klien. Dengan demikian, setiap klien yang ingin terhubung ke internet harus menggunakan perangkat dengan MAC address yang terdaftar dan sesuai dengan hak akses username dan password pada hotspot login.

## DAFTAR PUSTAKA

[1] E. Au, L. Wilhelmsson, T. Baykas, and J. Kim, "Guest Editorial: Recent and Future Evolution of Wi-Fi," *IEEE Commun. Stand. Mag.*, vol. 6, no. 2, pp. 8–11, 2022, doi: 10.1109/MCOMSTD.2022.9855241.

[2] K. Pahlavan and P. Krishnamurthy, "Evolution and Impact of Wi-Fi Technology and Applications: A Historical Perspective," *Int. J. Wirel. Inf. Networks*, vol. 28, no. 1, pp. 3–19, 2021, doi: 10.1007/s10776-020-00501-8.

[3] I. Prlić *et al.*, "Wi-Fi technology and human health impact: A brief review of current knowledge," *Arh. Hig. Rada Toksikol.*, vol. 73, no. 2, pp. 94–106, 2022, doi: 10.2478/aiht-2022-73-3402.

[4] J. S. Runtao Ren, "A Security-Enhanced and Privacy-Preserving Certificateless Aggregate Signcryption Scheme-Based Artificial Neural Network in Wireless Medical Sensor Network". in in *IEEE Sensors Journal*, vol. 23, no. 7, pp. 7440-7450, 1 April1, 2023, doi: 10.1109/JSEN.2023.3247581

[5] I. P. Danilo Orlando, Stefania Bartoletti, "Innovative Attack Detection Solutions for Wireless Networks With Application to Location Security". in *IEEE Transactions on Wireless Communications*, vol. 22, no. 1, pp. 205-219, Jan. 2023, doi: 10.1109/TWC.2022.3192225

[6] Z. L. Haijun Tan, "Detection of Jamming Attacks for the Physical-Layer Authentication". in *IEEE Transactions on Wireless Communications*, vol. 22, no. 12, pp. 9579-9594, Dec. 2023, doi: 10.1109/TWC.2023.3272337

[7] S. W. Yang Cao, "Joint User Grouping and Power Optimization for Secure mmWave-NOMA Systems". in *IEEE Transactions on Wireless Communications*, vol. 21, no. 5, pp. 3307-3320, May 2022, doi: 10.1109/TWC.2021.3120268

[8] V. Shukla, A. Chaturvedi, and N. Srivastava, "Nanotechnology and cryptographic protocols: Issues and possible solutions," *Nanomater. Energy*, vol. 8, no. 1, pp. 24–26, 2019, doi: 10.1680/jnaen.18.00006.

[9] A. K. Yadav, M. Misra, P. K. Pandey, K. Kaur, S. Garg, and M. Liyanage, "LEMAP: A Lightweight EAP based Mutual Authentication Protocol for IEEE 802.11 WLAN," *IEEE Int. Conf. Commun.*, vol. 2022-May, pp. 692–697, 2022, doi: 10.1109/ICC45855.2022.9839094.

[10] Y. Kihira, K. Yamamoto, A. Taya, T. Nishio, Y. Koda, and K. Yano, "Interference-free AP identification and shared information reduction for tabular Q-learning-based WLAN coordinated spatial reuse," *IEICE Commun. Express*, vol. 11, no. 7, pp. 392–397, 2022, doi: 10.1587/comex.2022xbl0051.

[11] J. K. Dileep Kumar, "Blockage-Aware Reliable mmWave Access via Coordinated Multi-Point Connectivity".

[12] B. X. Xiaoying Liu, "Throughput Maximization of Wireless-Powered Communication Network With Mobile Access Points".

[13] st Isaac Chin Eian, nd Lim Ka Yong, rd Majesty Yeap Xiao Li, and th Yeo Hui Qi, "Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges," *Preprints*, no. October, 2020, doi: 10.20944/preprints202010.0018.v1.

[14] B. Rong, "BOOK REVIEWS Security in Wireless Communication," *IEEE Wirel. Commun.*, vol. 30, no. February, pp. 10–11, 2023.

[15] T. Asamov, E. Yamangil, E. Boros, P. B. Kantor, and F. Roberts, "Optimal Layered Defense For Site Protection," *Springer Optim. Its Appl.*, vol. 202, pp. 1–21, 2023, doi: 10.1007/978-3-031-31654-8_1.

[16] S. Suhadin, "Evaluation Of Network Access Restrictions Using Mac Address Filtering On Microtik To Improve Network



No. 1-005/Vol. 9/2025/TechnoXplore
DOI 10.36805/technoxplore.v10i1. 8331

ISSN: 2503-054X
Vol. 10 No: 1, April 2025

Security," *J. World Sci.*, vol. 1, no. 3, pp. 112–120, 2022, doi: 10.58344/jws.v1i3.12.
[17] I. Didmanidze, Z. Beridze, and V. Zaslavski, "Analysis of wireless network security systems problems and those solutions," *Model. Control Inf. Technol.*, no. 4, pp. 139–140, 2020, doi: 10.31713/mcit.2020.31.


No. 1-005/Vol. 9/2025/TechnoXplore
DOI 10.36805/technoxplore.v10i1. 8331