IMPLEMENTASI AUTENTIKASI DUA FAKTOR GUEST WI-FI BERBASIS WHATSAPP GATEWAY UNTUK KEAMANAN JARINGAN

IMPLEMENTING TWO-FACTOR GUEST WI-FI AUTHENTICATION VIA WHATSAPP GATEWAY FOR ENHANCED SECURITY

Mustika Kurnia Mayangsari[1], Adianto[2*], Mirza Ardiana[3], Sholahuddin Muhammad Irsyad[4]

*E-mail: adianto@ppns.ac.id

[1, 2]Prodi Teknik Otomasi, Teknik Kelistrikan Kapal, Politeknik Perkapalan Negeri Surabaya
[4]Prodi Teknik Kelistrikan Kapal, Teknik Kelistrikan Kapal, Politeknik Perkapalan Negeri Surabaya
[3]Prodi Manajemen Bisnis, Teknik Bangunan Kapal, Politeknik Perkapalan Negeri Surabaya

Abstrak

Ketersediaan Wi-Fi publik dengan *Single-Factor Authentication* (SFA) sering menjadi celah keamanan siber. Penelitian ini mengusulkan sistem *Two-Factor Authentication* (2FA) menggunakan *WhatsApp Gateway* sebagai penyedia kode OTP. Dengan metode rekayasa sistem, pengguna wajib memverifikasi identitas melalui perangkat seluler setelah memasukkan kredensial utama. Hasil pengujian menunjukkan sistem berjalan stabil hingga 50 virtual users. Namun, performa menurun pada 75 virtual users dan mencapai *error rate* 2,30% pada beban 100 virtual users. Integrasi ini efektif memperkuat keamanan jaringan publik secara akuntabel tanpa mengorbankan kenyamanan pengguna secara drastis.

Kata kunci*: *Wi-Fi, Two-Factor Authentication, WhatsApp, Raspberry Pi, MikroTik

Abstract

Public Wi-Fi services with single-factor authentication often pose significant cybersecurity risks. This study proposes a Two-Factor Authentication (2FA) system for guest networks that uses a WhatsApp Gateway to deliver One-Time Passwords (OTPs). Using a systems engineering approach, the model requires users to verify their identities via mobile devices after initial credential entry. Testing confirms the system remains stable for up to 50 concurrent virtual users. However, performance declines at 75 concurrent virtual users, reaching a 2,30% error rate at 100 concurrent virtual users. This integration successfully strengthens network integrity and accountability without significantly compromising convenience.

***Keywords**: Wi-Fi, Two-Factor Authentication, WhatsApp, Raspberry Pi, MikroTik*

1. PENDAHULUAN

Eskalasi penetrasi internet di ruang publik telah menggeser paradigma konektivitas menjadi kebutuhan fundamental bagi mobilitas pengguna. Namun, penyediaan layanan *Guest Wi-Fi* sering kali mengabaikan aspek keamanan jaringan yang mumpuni, di mana infrastruktur publik umumnya bersifat *open access* atau hanya dilindungi oleh mekanisme *Single-Factor Authentication* (SFA) yang rentan terhadap eksploitasi [1], [2]. Kondisi ini diperparah oleh aspek psikologi pengguna, yaitu terdapat studi empiris terhadap pola perilaku mahasiswa di Jepang yang menunjukkan bahwa meskipun terdapat kesadaran yang jelas mengenai risiko penggunaan Wi-Fi

publik yang tidak aman, sebagian besar pengguna tetap memilih untuk terhubung demi alasan praktis dan kenyamanan [3]. Fenomena perilaku ini menciptakan kerentanan kritis yang memungkinkan terjadinya serangan siber seperti *man-in-the-middle* [4], [5] atau *credential harvesting* [6], yang secara langsung mengancam integritas data pribadi pengguna. Kerentanan inheren ini tidak hanya mengancam privasi data pengguna, tetapi juga membuka celah bagi aktor ancaman untuk melakukan infiltrasi ke dalam segmen jaringan yang lebih krusial[7].

Secara teknis, ketergantungan pada satu lapis autentikasi gagal dalam memenuhi prinsip akuntabilitas dan non-repudiasi dalam manajemen jaringan. Penggunaan *Pre-Shared Key* yang bersifat komunal mengakibatkan identifikasi pengguna menjadi anonim [8], sehingga sulit bagi administrator jaringan untuk melakukan audit jejak digital jika terjadi aktivitas anomali [9]. Oleh karena itu, diperlukan sebuah transformasi mekanisme kendali akses yang mampu memverifikasi identitas pengguna secara *real-time* melalui entitas unik yang dimiliki secara personal [10].

Penerapan *Two-Factor Authentication* (2FA) merupakan strategi mitigasi risiko yang krusial untuk memperkuat integritas sistem autentikasi [11]. Dengan mengintegrasikan faktor kepemilikan (*possession factor*) [12] ke dalam proses login, keamanan jaringan tidak lagi hanya bergantung pada apa yang diketahui pengguna, tetapi juga pada perangkat fisik yang mereka kuasai. Konsep ini secara signifikan mereduksi kemungkinan akses tidak sah meskipun kredensial utama telah terekspos, karena penyerang tetap memerlukan akses ke lapisan verifikasi kedua untuk mendapatkan otorisasi penuh.

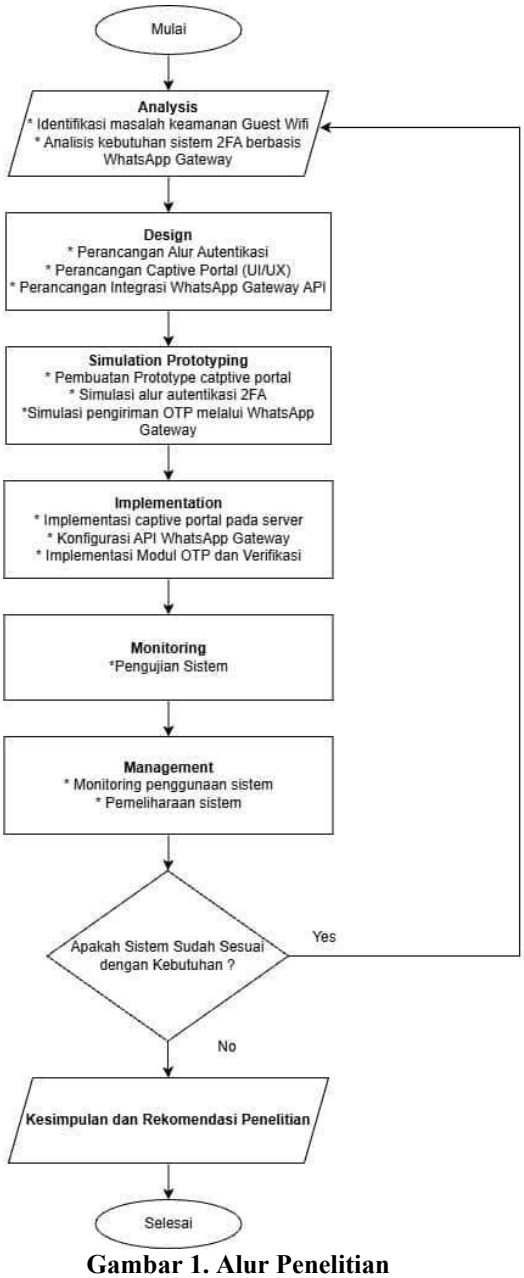
Meskipun pengiriman *One-Time Password* (OTP) melalui SMS telah lama diadopsi, efektivitasnya kini terkendala oleh biaya operasional yang fluktuatif serta latensi pengiriman yang dipengaruhi oleh kualitas sinyal seluler [13]. Sebagai alternatif yang lebih disruptif, penggunaan *WhatsApp Gateway* berbasis API (*Application Programming Interface*). Menawarkan efisiensi transmisi data yang lebih tinggi dan tingkat ubiquitas platform yang masif di kalangan pengguna. Integrasi ini memungkinkan distribusi kode autentikasi secara *Out-of-Band* (OOB) dengan reliabilitas yang lebih stabil, menjamin fungsionalitas sistem tetap terjaga tanpa membebani infrastruktur dengan biaya pesan konvensional yang tinggi.

Berdasarkan problematika tersebut, penelitian ini mengusulkan sebuah model autentikasi Wi-Fi tamu yang komprehensif dengan mengintegrasikan sistem *captive portal* dan *WhatsApp Gateway*. Fokus utama adalah pada kekokohan jaringan (*robustness*) serta mengukur pengaruhnya terhadap pengalaman pengguna (*quality of experience*). Melalui pendekatan ini, diharapkan tercipta sebuah framework akses jaringan publik yang tidak hanya aman dari ancaman siber, tetapi juga efisien dan akuntabel dari sisi manajerial.

2. METODOLOGI

Penelitian ini menggunakan pendekatan rekayasa sistem dengan model pengembangan *Network Development Life Cycle* (NDLC). Model ini dipilih karena mampu memberikan kerangka kerja yang sistematis dalam perancangan, implementasi, dan evaluasi sistem jaringan, khususnya pada pengembangan mekanisme autentikasi berbasis 2FA pada jaringan *Guest Wi-Fi*.

Tahapan dalam metode NDLC yang digunakan dalam penelitian ini meliputi *analysis, design, simulation prototyping, implementation, monitoring,* dan *management*, yang dijelaskan sebagai berikut[14], [15]:



Gambar 1. Alur Penelitian

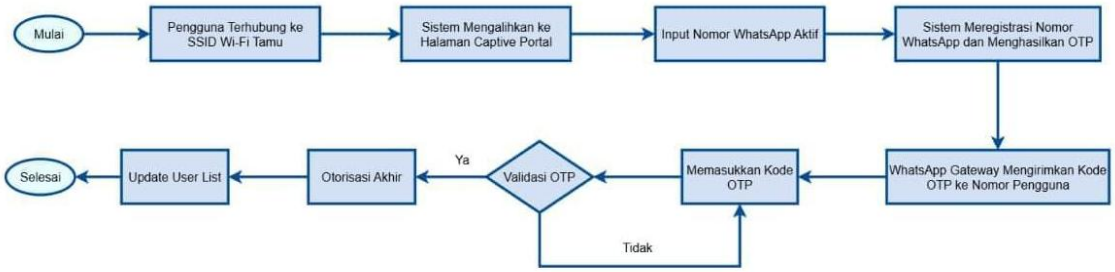
2.1 Analysis

Tahap analisis dilakukan untuk mengidentifikasi permasalahan serta kebutuhan sistem yang akan dikembangkan, dengan fokus utama pada evaluasi kelemahan mekanisme autentikasi satu faktor pada jaringan *Guest Wi-Fi* yang rentan terhadap penyalahgunaan. Pada tahap ini dilakukan identifikasi potensi ancaman dan celah keamanan pada sistem autentikasi konvensional, diikuti dengan analisis kebutuhan penerapan autentikasi 2FA sebagai solusi peningkatan keamanan. Selain itu, dilakukan studi literatur yang mencakup teknologi captive portal, mekanisme *One-Time Password* (OTP), serta integrasi *WhatsApp Gateway* sebagai media distribusi kredensial. Analisis juga mencakup identifikasi kebutuhan fungsional, seperti proses autentikasi dan pengiriman OTP, serta kebutuhan non-fungsional yang meliputi aspek keamanan, performa, dan

kemudahan penggunaan (*usability*). Hasil dari tahap ini berupa spesifikasi kebutuhan sistem yang menjadi dasar dalam proses perancangan sistem selanjutnya.

2.2 *Design*

Tahap perancangan dilakukan untuk mendefinisikan arsitektur sistem dan alur autentikasi yang akan dikembangkan. Berikut alur rancangan arsitektur autentikasi dalam penelitian ini:



Gambar 2. Proses Autentikasi 2FA

Proses autentikasi pada gambar tersebut dirancang agar sistem dapat meregistrasi dan mengelola identitas tamu secra otomatis berdasarkan nomor WhatsApp pengguna, yang kemudian diikuti dengan pengiriman kode akses atau kredensial hotspot secara langsung ke perangkat seluler pengguna.

2.3 Simulasi *Prototyping*

Tahap simulasi *prototyping* bertujuan untuk memvalidasi rancangan sistem melalui pengembangan prototipe dalam lingkungan simulasi sebelum diimplementasikan pada kondisi nyata. Pada tahap ini dilakukan pengembangan awal captive portal sebagai antarmuka autentikasi pengguna, yang kemudian digunakan untuk mensimulasikan alur autentikasi dua faktor (2FA) secara menyeluruh. Proses simulasi mencakup pengujian pengiriman kode OTP melalui *WhatsApp Gateway* dalam mode uji coba untuk memastikan integrasi antarkomponen sistem berjalan dengan baik. Selain itu, dilakukan validasi fungsional awal terhadap seluruh proses utama, meliputi login pengguna, pengiriman OTP, serta mekanisme verifikasi. Tahap ini memastikan bahwa desain sistem telah berjalan secara logis, terintegrasi, dan memenuhi kebutuhan fungsional sebelum dilanjutkan ke tahap implementasi pada lingkungan jaringan yang sebenarnya.

2.4 Implementasi

Tahap implementasi dilakukan dengan menerapkan sistem yang telah dirancang ke dalam lingkungan jaringan yang sebenarnya sehingga dapat beroperasi secara nyata. Pada tahap ini dilakukan proses deployment *captive portal* pada server atau perangkat jaringan hotspot sebagai antarmuka autentikasi pengguna. Selanjutnya, dilakukan integrasi API *WhatsApp Gateway* ke dalam sistem untuk mendukung pengiriman kredensial atau OTP sebagai faktor autentikasi kedua. Modul OTP diimplementasikan untuk menghasilkan, mengirim, dan memverifikasi kode autentikasi yang digunakan oleh pengguna. Selain itu, sistem autentikasi 2FA diaktifkan pada jaringan *Guest Wi-Fi* sehingga setiap pengguna diwajibkan melalui proses verifikasi sebelum memperoleh akses jaringan. Tahap ini menghasilkan sistem yang telah terintegrasi secara menyeluruh dan siap untuk dilakukan pengujian pada kondisi operasional.

2.5 Monitoring Sistem

Tahap monitoring berfokus pada proses pengujian sistem untuk mengevaluasi kinerja dan keamanannya. Parameter dan skenario pengujian ini digunakan sebagai dasar evaluasi performa sistem pada bagian hasil dan pembahasan. Dilakukan secara komprehensif melalui tiga tahap utama, yaitu pengujian fungsional, pengujian performa, dan pengujian keamanan. Pengujian fungsional dilakukan untuk memvalidasi seluruh alur operasional, mulai dari proses pengalihan (redirection) otomatis saat perangkat terhubung ke Wi-Fi hingga pemberian otorisasi akses akhir bagi pengguna. Pengujian performa difokuskan pada efisiensi waktu respons pengiriman kredensial melalui WhatsApp Gateway serta stabilitas aktivasi akun pada daftar pengguna hotspot. Terakhir, pengujian keamanan dilakukan untuk memastikan bahwa mekanisme autentikasi dua faktor tersebut efektif dalam memitigasi risiko akses tidak sah dan menjaga integritas data identitas tamu yang telah teregistrasi di dalam sistem.

2.6 Manajemen Sistem

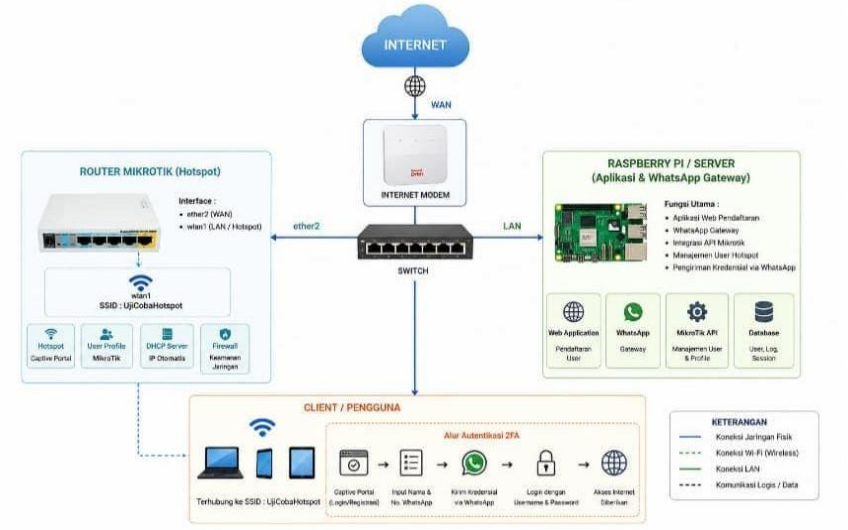
Tahap manajemen sistem bertujuan untuk memastikan sistem berjalan secara berkelanjutan dan stabil. Kegiatan yang dilakukan meliputi monitoring aktivitas pengguna dan kinerja sistem, pemeliharaan sistem, serta evaluasi operasional sebagai dasar untuk pengembangan dan peningkatan sistem selanjutnya.

3. HASIL DAN PEMBAHASAN

Berdasarkan tahapan metode NDLC yang telah dijelaskan pada bagian sebelumnya, sistem autentikasi berbasis *Two-Factor Authentication* menggunakan *WhatsApp Gateway* berhasil diimplementasikan pada jaringan *Guest Wi-Fi*. Maka berikut hasil dari penelitian berikut ini:

3.1 Implementasi Arsitektur Sistem

Arsitektur jaringan yang diusulkan dalam penelitian ini untuk mengimplementasikan mekanisme autentikasi 2FA pada jaringan *Guest Wi-Fi* dengan memanfaatkan *WhatsApp Gateway* sebagai media distribusi kredensial yaitu sebagai berikut :



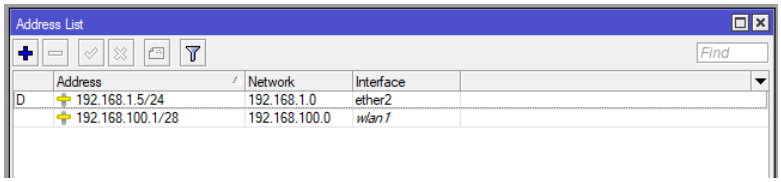
Gambar 3. Arsitektur 2FA

Internet cloud merepresentasikan sumber konektivitas eksternal yang menyediakan akses jaringan global. Koneksi internet ini diteruskan melalui perangkat modem yang berfungsi sebagai penghubung antara jaringan publik dan jaringan lokal. Modem kemudian menyalurkan koneksi ke jaringan internal melalui perangkat *switch*.

Switch berperan sebagai pusat distribusi jaringan yang menghubungkan beberapa perangkat dalam satu segmen jaringan lokal (LAN). Dalam arsitektur ini, switch menghubungkan router Mikrotik sebagai penyedia layanan hotspot dan server Raspberry Pi sebagai pusat pengolahan sistem autentikasi.

Router Mikrotik berfungsi sebagai gateway utama jaringan hotspot yang menyediakan akses Wi-Fi kepada pengguna. Router ini dikonfigurasi dengan dua interface utama:

- ether2: digunakan sebagai jalur komunikasi ke jaringan eksternal dan server
- wlan1: digunakan sebagai interface hotspot untuk pengguna (SSID: UjiCobaHotspot)



Gambar 4. Konfigurasi ether2 dan wlan1 pada Mikrotik

Raspberry Pi berperan sebagai pusat kontrol sistem autentikasi, yang menjalankan beberapa fungsi utama yaitu aplikasi web untuk registrasi pengguna (*captive portal backend*), integrasi dengan *WhatsApp Gateway*, pengelolaan data pengguna dan kredensial, dan komunikasi dengan MikroTik melalui API. Ketika pengguna melakukan registrasi, server akan menerima data pengguna (nama dan nomor WhatsApp), mengirim data tersebut ke Mikrotik untuk pembuatan akun hotspot, dan mengirimkan username dan password ke pengguna melalui WhatsApp.

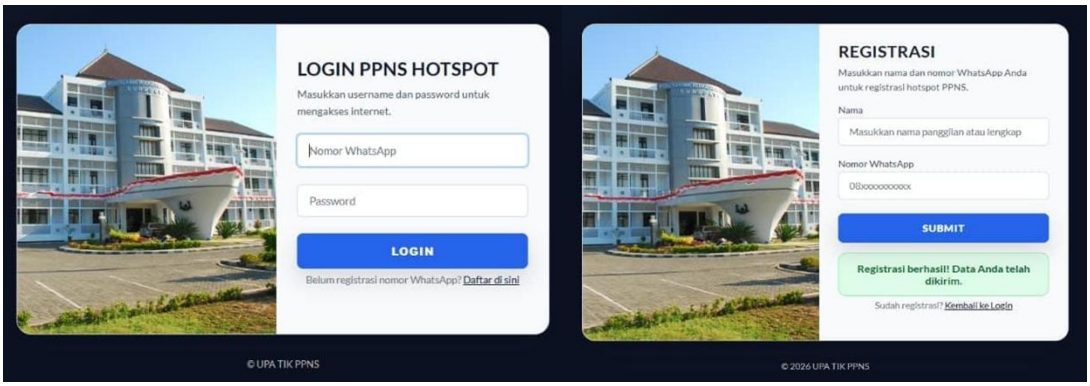
Client atau pengguna merupakan perangkat pengguna seperti laptop atau smartphone yang terhubung ke jaringan Wi-Fi. Pengguna mengakses jaringan melalui SSID yang disediakan oleh MikroTik. Alur koneksi pengguna meliputi terhubung ke jaringan Wi-Fi (UjiCobaHotspot), dialihkan secara otomatis ke captive portal, melakukan registrasi dengan memasukkan nomor WhatsApp, menerima kredensial melalui WhatsApp, dan melakukan login untuk mendapatkan akses internet.

Gambar 5. SSID UjiCobaHotspot

3.2 Implementasi *Captive Portal* dan *WhatsApp Gateway*

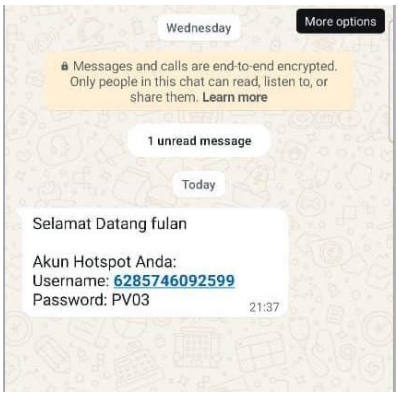
Implementasi captive portal pada penelitian ini berfungsi sebagai gerbang utama autentikasi pengguna sebelum memperoleh akses ke jaringan internet seperti ilustrasi Gambar 6. Ketika perangkat pengguna terhubung ke jaringan Wi-Fi hotspot, sistem secara otomatis melakukan proses *redirection* ke halaman captive portal. Pada tahap ini, pengguna yang belum terdaftar diarahkan untuk melakukan proses registrasi dengan mengisi data nomor WhatsApp dan password pada form yang telah disediakan. Apabila pengguna belum pernah melakukan registrasi,

maka harus melakukan pendaftaran terlebih dahulu dengan melakukan input nama dan nomor WhatsApp.



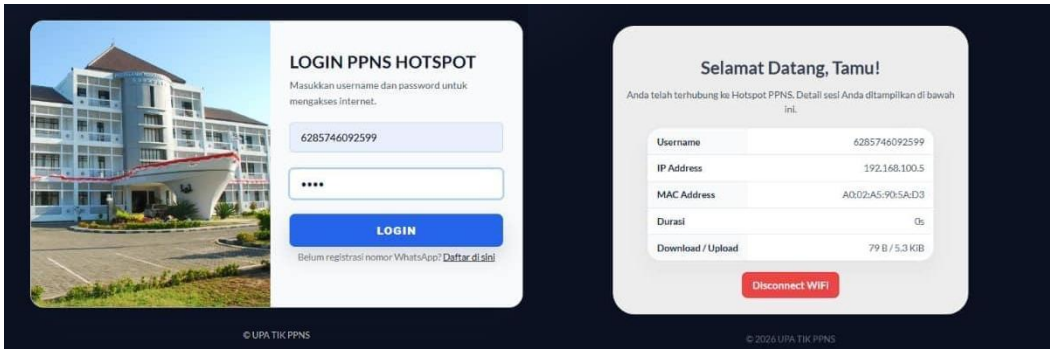
Gambar 6. Proses Login dan Registrasi pada Captive Portal

Setelah pengguna mengirimkan data registrasi, sistem backend yang berjalan pada server Raspberry Pi akan memproses data tersebut dengan melakukan validasi format input, khususnya nomor WhatsApp yang digunakan sebagai identitas unik pengguna. Selanjutnya, data yang telah tervalidasi dikirimkan ke router Mikrotik melalui mekanisme *Application Programming Interface* (API) untuk dilakukan proses pembuatan akun hotspot secara otomatis. Proses ini mencakup pembuatan username dan password yang bersifat unik untuk setiap pengguna, serta penyesuaian profil akses sesuai dengan kebijakan jaringan yang telah ditentukan.



Gambar 7. Pengiriman Kredensial pada Nomor WhatsApp

Setelah menerima kredensial melalui WhatsApp (Gambar 7), pengguna diarahkan kembali ke halaman login captive portal untuk memasukkan *username* dan *password* yang telah diterima. Sistem kemudian melakukan proses verifikasi terhadap data autentikasi tersebut dengan mencocokkannya pada database pengguna yang tersimpan di MikroTik. Apabila proses autentikasi berhasil (Gambar 8), maka sistem akan memberikan otorisasi akses jaringan kepada pengguna, sehingga perangkat dapat terhubung ke internet.



Gambar 8. Proses Autentikasi Berhasil

Sebaliknya, jika proses login gagal, maka akan muncul kode OTP salah (atau peringatan kegagalan autentikasi seperti Gambar 9). Lalu, pengguna diminta untuk memastikan kembali data yang dimasukkan sebelum mencoba kembali.

Gambar 9. Proses Login Gagal

Secara keseluruhan, implementasi ini menunjukkan bahwa integrasi antara *captive portal*, Mikrotik API, dan *WhatsApp Gateway* dapat berjalan secara sinkron dan otomatis. Proses registrasi, pembuatan akun, distribusi kredensial, hingga autentikasi akhir dapat dilakukan dalam satu alur sistem yang terstruktur, sehingga tidak hanya meningkatkan keamanan melalui verifikasi berbasis perangkat pribadi, tetapi juga tetap mempertahankan kemudahan penggunaan bagi pengguna jaringan *Guest Wi-Fi*.

3.3 Hasil Pengujian

Temuan dari validasi sistem disajikan dalam bagian ini, yang disusun berdasarkan metodologi pengujian yang telah ditetapkan: pengujian fungsional, pengujian performa, dan pengujian keamanan. Hasil ini memvalidasi bahwa sistem mampu mencapai keseimbangan optimal antara peningkatan postur keamanan dan kemudahan akses bagi pengguna. Berdasarkan data pada Tabel 1, seluruh parameter pengujian fungsional sistem menunjukkan status “Berhasil”, yang mengonfirmasi bahwa setiap komponen inti sistem beroperasi sesuai dengan spesifikasi yang diharapkan. Sistem berhasil melakukan pengalihan otomatis bagi seluruh pengguna yang belum terautentikasi ke halaman portal masuk dengan tingkat keberhasilan penuh. Pada aspek manajemen identitas, mekanisme registrasi terbukti mampu menangkap data nama dan nomor WhatsApp pengguna secara akurat untuk proses pembuatan akun.

Tabel 1. Hasil Pengujian Fungsional Sistem

ID Tes	Kebutuhan Fungsional	Hasil yang Diharapkan	Hasil Aktual	Hasil
FT1	Pengalihan Captive Portal	Seluruh pengguna yang belum terautentikasi dialihkan ke halaman registrasi	Pengalihan ke form Registrasi berhasil dilakukan	Berhasil
FT2	Pengiriman Kredensial via WhatsApp	Username dan password hotspot dibuat dan dikirim ke pengguna melalui gateway WhatsApp	Kredensial diterima via WhatsApp; Pengguna dibuat pada sisi *backend*	Berhasil
FT3	Logika Manajemen Akun	Sistem membedakan pengguna baru dan lama untuk pembuatan atau pembaruan akun.	*Backend* berhasil mencatat logika '*create new*' (buat baru) dan '*update password*' (perbarui sandi)	Berhasil
FT4	Otorisasi Jaringan	*Login* yang berhasil memberikan akses; pengguna muncul dalam *Active List* di Server Hotspot	Pengguna berhasil masuk, aktif di jaringan, dan tercatat dalam *Active List* Mikrotik	Berhasil
FT5	Registrasi Identitas	Sistem berhasil menangkap nama dan nomor WhatsApp untuk pembuatan akun	Formulir input berhasil menangkap data yang dibutuhkan; Pengguna dibuat berdasarkan nomor	Berhasil
FT6	Otorisasi OTP berdasarkan waktu	Sistem berhasil memberikan batas waktu tertentu mengakses hotspot.	User akan diperintahkan untuk melakukan registrasi kembali.	Berhasil

Berikut pada Tabel 2 merupakan hasil pengujian performa pada server Raspberry Pi yaitu, yang digunakan untuk autentikasi. Pengujian beban server autentikasi dilakukan dengan mensimulasikan Virtual Users (VUs) untuk merepresentasikan jumlah pengguna aktif yang mengakses jaringan secara bersamaan. Hasil pengujian menunjukkan performa optimal dan stabil hingga beban 50 VUs, ditandai dengan peningkatan *throughput* secara linier, *response time* rendah, dan tingkat kesalahan 0%. Namun, degradasi performa mulai terlihat pada beban 75 VUs. Pada beban 100 VUs, sistem melampaui batas toleransi dengan *error rate* mencapai 2,30% yang menunjukkan bahwa kapasitas maksimum sistem berada di bawah angka tersebut.

Tabel 2. Hasil Pengujian Beban Server Raspi (*Authentication Server*)

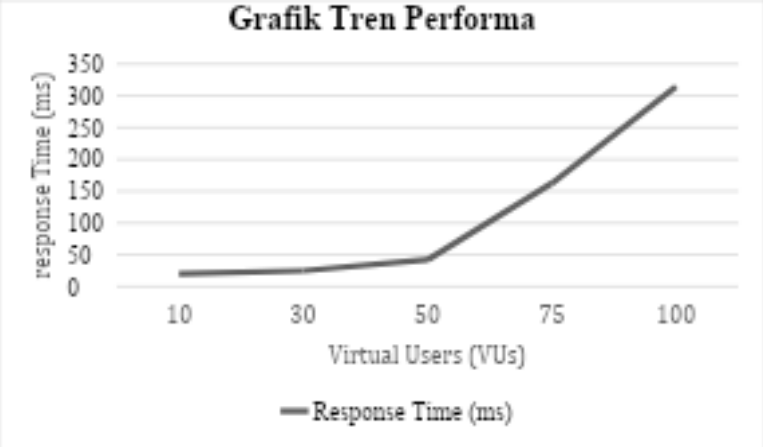
Jumlah Virtual Users	Throughput (req/s)	Rata-Rata Response Time (ms)	Error Rate (%)
10	9,46	20,59	0,00%
30	28,16	24,84	0,00%
50	47,06	42,07	0,00%
75	63,50	162,42	0,15%

100	74,77	314,76	2,30%

Penentuan ambang batas (*threshold*) dalam pengujian ini didasarkan pada standar kenyamanan pengguna dan stabilitas sistem sebagai berikut:

1. Response Time ($p(95) < 2000\,ms$): Merujuk pada standar ITU-T G.1010 [16], batas 2 detik adalah ambang maksimal bagi pengguna untuk merasakan layanan interaktif yang responsif [17].
2. Error Rate ($< 1\%$): Standar reliabilitas sistem untuk menjamin akses autentikasi tetap akuntabel tanpa kegagalan yang masif [18], [19].
3. Receiving Time ($p(95) < 500\,ms$): Menjamin kelancaran transmisi paket data kecil (OTP) pada antarmuka jaringan server.

Sebagaimana diilustrasikan pada tren performa di Gambar 9, sistem memenuhi seluruh parameter kelayakan hingga beban menengah. Namun, pada beban 100 VUs, nilai error rate melampaui ambang batas hingga mencapai 2,30%. Hal ini mengonfirmasi bahwa secara fungsional fitur berjalan sesuai rancangan, namun secara kapasitas, sistem berbasis Raspberry Pi ini memiliki tren performa yang stabil pada rentang 50-75 VUs untuk dijadikan sebagai server autentikasi.



Gambar 10. Grafik Tren Performa Server Autentikasi

4. KESIMPULAN DAN SARAN

Berdasarkan hasil perancangan dan implementasi sistem *Two-Factor Authentication* (2FA) menggunakan *WhatsApp Gateway*, dapat disimpulkan bahwa sistem berhasil meningkatkan keamanan akses jaringan *Guest Wi-Fi* tanpa mengorbankan kemudahan pengguna. Seluruh komponen yang dikembangkan melalui metode NDLC terbukti berjalan sesuai rancangan. Pengujian fungsional mengonfirmasi keberhasilan seluruh skenario, sementara pengujian performa menunjukkan sistem sangat stabil hingga beban 50 VUs dengan response time rendah dan tingkat kesalahan 0%. Namun, kapasitas operasional mulai menurun pada 75 VUs dan melampaui ambang batas kelayakan pada 100 VUs dengan *error rate* sebesar 2,30%.

Sistem ini dinilai layak untuk diterapkan pada lingkungan dengan beban rendah hingga menengah. Untuk pengembangan di masa depan, disarankan melakukan optimasi skalabilitas guna menangani beban tinggi. Peningkatan aspek keamanan dapat difokuskan pada enkripsi data yang lebih kuat dan integrasi metode autentikasi tambahan. Selain itu, eksplorasi platform komunikasi alternatif perlu dipertimbangkan untuk meningkatkan fleksibilitas dan mengurangi ketergantungan pada satu layanan pihak ketiga.

5. DAFTAR RUJUKAN

[1] Bima Yusup Septiana, Yogi Irdes Putra, dan Fitri Yanti, "Wireless Network Security Using Hotspot Login Authentication Method," *Academia Open*, vol. 10, no. 2, Agu 2025, doi: 10.21070/acopen.10.2025.12146.

[2] K. W. Ang, E. G. Chekole, dan J. Zhou, "Unveiling the Covert Vulnerabilities in Multi-Factor Authentication Protocols: A Systematic Review and Security Analysis," *ACM Comput. Surv.*, vol. 57, no. 11, hlm. 1–37, Nov 2025, doi: 10.1145/3734864.

[3] N. Sombatruang, Y. Kadobayashi, M. A. Sasse, M. Baddeley, dan D. Miyamoto, "The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan," dalam *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, IEEE, Agu 2018, hlm. 1–11. doi: 10.1109/PST.2018.8514208.

[4] M. Thankappan, H. Rifà-Pous, dan C. Garrigues, "Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review," *Expert Syst. Appl.*, vol. 210, hlm. 118401, Des 2022, doi: 10.1016/j.eswa.2022.118401.

[5] I. Zulkarnaen, M. Z. M. R, S. Syarifudin, S. Rinaldi, dan U. Akem, "Wireless Fidelity Network Security Threats (Wi-Fi)," *JERIT: Journal of Educational Research and Innovation Technology*, vol. 2, no. 2, hlm. 73–82, Okt 2025, doi: 10.34125/jerit.v2i2.26.

[6] E. al. Rajan Gupta, "The Dangers of Public Wi-Fi: How to Protect Your Device Through Cyber Security," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 9, hlm. 3016–3022, Nov 2023, doi: 10.17762/ijritcc.v11i9.9409.

[7] N. Hakiem *dkk.*, "ASSESSING CYBERSECURITY READINESS AMONG HIGHER EDUCATION INSTITUTIONS IN INDONESIA USING MANAGEMENT PERSPECTIVES," *ICIC Express Letters*, vol. 17, no. 10, hlm. 1151–1158, Agu 2023, doi: 10.24507/icicel.17.10.1151.

[8] S. Peng, B. Han, C. Wu, dan B. Wang, "A Secure Communication System in Self-Organizing Networks via Lightweight Group Key Generation," *IEEE Open Journal of the Computer Society*, vol. 1, hlm. 182–192, 2020, doi: 10.1109/OJCS.2020.3024989.

[9] K. Xue *dkk.*, "A Secure, Efficient, and Accountable Edge-Based Access Control Framework for Information Centric Networks," *IEEE/ACM Transactions on Networking*, vol. 27, no. 3, hlm. 1220–1233, Jun 2019, doi: 10.1109/TNET.2019.2914189.

[10] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, dan S. Guerreiro, "SSIBAC: Self-Sovereign Identity Based Access Control," dalam *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, IEEE, Des 2020, hlm. 1935–1943. doi: 10.1109/TrustCom50675.2020.00264.

[11] A. A. S. AlQahtani, T. Alshayeb, M. Nabil, dan A. Patooghy, "Leveraging Machine Learning for Wi-Fi-Based Environmental Continuous Two-Factor Authentication," *IEEE Access*, vol. 12, hlm. 13277–13289, 2024, doi: 10.1109/ACCESS.2024.3356351.

[12] Z. Wang *dkk.*, "Simple But Not Secure: An Empirical Security Analysis of Two-factor Authentication Systems," *ArXiv*, 2024.

[13] M. Bartłomiejczyk dan I. El Fray, "Device Risk Analysis Protocol for SMS-Based OTP Authentication," *IEEE Access*, vol. 12, hlm. 123177–123192, 2024, doi: 10.1109/ACCESS.2024.3445931.

[14] A. N. Hasan dan G. Purnama, "PERANCANGAN DAN SIMULASI JARINGAN INTERNET DENGAN MENERAPKAN METODE PENGEMBANGAN NDLC (NETWORK DEVELOPMENT LIFE CYCLE) PADA AKSES EDUCATION CENTRE."

[15] S. Amalia Saleha *dkk.*, "OPTIMALISASI JARINGAN WIRELESS MENGGUNAKAN METODE PENGEMBANGAN NETWORK DEVELOPMENT LIFE CYCLE (NDLC)," 2023.

[16] International Telecommunication Union, "ITU-T Recommendation G. 1010: End-user multimedia QoS categories (Quality of service and performance)," 2001. Diakses: 30 April 2026. [Daring]. Tersedia pada: https://www.itu.int/rec/T-RECG. 1010-200111-I/en
[17] H. Z. Jahromi, D. T. Delaney, dan A. Hines, "Beyond First Impressions: Estimating Quality of Experience for Interactive Web Applications," *IEEE Access*, vol. 8, hlm. 47741–47755, 2020, doi: 10.1109/ACCESS.2020.2979385.
[18] J. Nielsen, "Response Times: The 3 Important Limits," *Nielsen Norman Group*, 1993.
[19] Z. Wang, X. Lai, S. Zhang, Q. Meng, dan H. Luo, "Enabling Byzantine Fault Tolerance in Access Authentication for Mega-Constellations," *IEEE/ACM Transactions on Networking*, vol. 32, no. 6, hlm. 5341–5355, Des 2024, doi: 10.1109/TNET.2024.3463609.