Pengembangan Aplikasi Web Layanan Kesehatan Fisioterapi Dengan Penerapan Sistem Autentikasi Json Web Token (JWT) Untuk Manajemen Role-Based Access Control (RBAC)

Adi Indra Pratama[1], I Made Suartana[2]

[1,2] Program Studi S1Teknik Informatika, Universitas Negeri Surabaya
[1]adi.22045@mhs.unesa.ac.id
[2]madesuartana@unesa.ac.id

***Abstrak*— Penelitian Penelitian ini bertujuan untuk merancang dan mengimplementasikan aplikasi web layanan fisioterapi yang aman dan efisien dengan menerapkan autentikasi berbasis JSON Web Token (JWT) serta manajemen hak akses berbasis peran (Role-Based Access Control/RBAC). Latar belakang penelitian ini adalah kebutuhan pengelolaan data pasien yang sensitif dan pentingnya kontrol akses yang terstruktur untuk menjaga kerahasiaan dan integritas informasi medis. Sistem dikembangkan menggunakan Laravel sebagai backend, Vite/React sebagai frontend, serta MySQL sebagai basis data, dan diuji melalui unit testing, API testing, dan end-to-end testing menggunakan Mock Service Worker. JWT memungkinkan pengelolaan sesi secara stateless, sementara RBAC mengatur hak akses sesuai peran pengguna (admin, terapis, pasien). Hasil implementasi menunjukkan aplikasi mampu menyediakan autentikasi yang aman, pengelolaan hak akses yang tepat, serta interaksi real-time antara pengguna. Evaluasi menggunakan metrik keamanan dan fungsionalitas mengindikasikan bahwa kombinasi JWT dan RBAC efektif meningkatkan keamanan data serta efisiensi operasional aplikasi. Dengan demikian, penelitian ini memberikan kontribusi pada pengembangan layanan kesehatan digital yang aman, terkontrol, dan sesuai standar perlindungan data.**

Kata Kunci— : *Fisioterapi, JSON Web Token, RBAC, Laravel, Vite/React, Keamanan Data, Aplikasi Web.*

I. PENDAHULUAN

Perkembangan teknologi informasi telah memberikan dampak signifikan pada berbagai sektor kehidupan, termasuk sektor Kesehatan. Salah satu bidang Kesehatan yang semskin memanfaatkan kemajuan teknologi Adalah fisioterapi, yaitu layanan rehabilitas yang berfokus pada pemulihan fungsi dan mobilitas tubuh pasien. Pemnfaatkan aplikasi berbasis web pada layanan fisioterapi memungkinkan proses pelayanan dilakukan secara lebih efisien melalui kemudahan akses informasi, pengelolaan data, serta interaksi antara pasien dan tenaga medis[1].

Meskipun memberikan berbagai kemudahan, penerapan layanan Kesehatan berbasis web juga menghadirkan tantangan, khususnya dalam menjaga keamanan data pasien. Data medis merupakan informasi yang bersifat sensitive sehingga rentan terhadap ancaman pencurian maupun penyalahgunaan apabila tidak dilindungi dengan mekanisme keamanan yang memadai. Oleh karena itu, diperlukan system control akses yang mampu memastikan bahwa hanyak pihak yang berwenang yang dapat mengakses data pasien[2]. Selain itu, pengelolaan identitas yang baik juga berperan penting dalam meningkatkan keamanan data medis pada system digital[3].

Salah satu pendekatan yang dapat digunakan untuk meneglola hak akses pengguna Adalah Role-Based Access Control (RBAC). Metode ini membatasi hak akses berdasarkan peran yang dimiliki pengguna dalam system sehingga setiap pengguna hanya dapat mengakses informasi sesuai dengan kewenangannya. Pada layanan fisioterapi, peran seperti admin, terapis dan pasien memiliki kebutuhan akses yang berbeda sehingga diperlukan mekanisme pengaturan hak akses yang jelas dan terstruktur[4]. Di sisi lain, proses autentikasi pengguana dapat diperkuat melalui penerapan JSON Web Token (JWT). JWT memungkinkan sitem melakukan autentikasi secara aman dan efisien tanpa menyimpan sesi pengguna di server. Melalui token yang dikirimkan pada setiap permintaan, identitas dan hak akses pengguna dapat diverifikasi sehingga hanya pengguna yang terautentikasi yang dapat mengakses layanan yang tersedia[5].

Beberapa penelitian sebelumnya telah membahas penerapan RBAC maupun tokenisasi akses dalam system digital. Penelitian yang dilakukan oleh[6] menunjukkan bahwa implementasi RBAC dapat diperkuat melalui tokenisasi akses untuk setiap pengguna guna meningkatkan keandalan distribusi hak akses. Penelitian lain oleh[7] mengemukakan bahwa token individu yang dienkripsi mampu mendukung mekanisme otorisasi yang lebih dinamis pada basis data relasional. Selain itu, penelitian oleh[8] menawarkan pendekatan token terdistribusi berbasis skema berbagi rahasi untuk meningkatkan keamanan akses data. Meskipun demikian, penerapan JWT sebagai personal access token yang terintegrasi dengan RBAC pada layanan Kesehatan berbasis web, khususnya layanan fisioterapi, masih belum banyak diterapkan secara komprehensif. Kondisi tersebut menunjukkan adanya peluang untuk mengembangkan system yang mampu menggabungkan autentikasi dan pengelolaan hak akses secara lebih aman dan efisien.

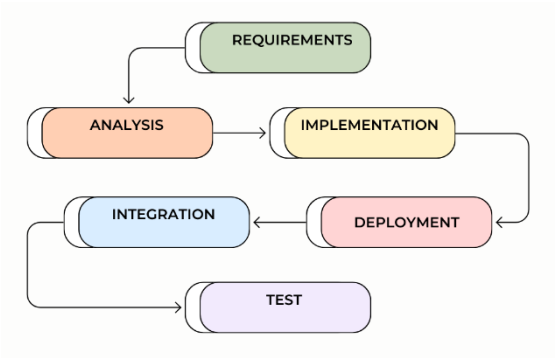
Berdasarkan permasalahan tersebut, penelitian ini berfokus pada penerapan system autentikasi menggunakan JSON Web Token (JWT) untuk menjamin keamanan akses pengguna pada aplikasi layanan fisioterapi berbasis web serta penerapan Role-Based Access Control (RBAC) untuk mengelola hak akses pengguan sesuai dengan perannya dalam system. Penelitian ini bertujuan untuk merancang dan mengimplementasikan autentikasi berbasis JWT sehingga hanya pengguna yang sah,

yaitu admin, terapis, dan pasien yang dapat mengakses data dan layanan yang tersedia. Selain itu, penelitian ini juga bertujuan menerapkan RBAC guna membedakan hak akses setiap pengguna sehingga resiko akses tidak sah dapat diminimalkan dan kerahasiaan data pasien tetap terjaga.

Untuk mencapai tujuan tersebut, penelitian ini mengembagkan aplikasi layanan fisioterapi berbasis web yang menerapkan JSON Web Token (JWT) sebagai mekanisme autentikasi dan Role-Based Access Control (RBAC) sebagai mekanisme manajemen hak akses. Penerapan kedua metode tersebut diharapkan mampu meningkatkan keamanan akses, melindungi data medis pasien dari penyalahgunaan, serta mendukung pengelolaan layanan fisioterapi yang lebih efektif, aman, dan terstruktur.

II. METODE PENELITIAN

A. *Pendekatan Penelitian*



Gbr. 1 Alur Pendekatan Penelitian

Pendekatan penelitian yang digunakan untuk menganalisis dan mengevaluasi penggunaan JSON Web Token (JWT) dalam aplikasi fisoterapi, dengan penekanan pada keamanan dan implementasi autentikasi serta otorisasi berbasis JWT. Pendekatan ini meliputi jenis penelitian, desain penelitian, dan teknik pengumpulan data yang digunakan untuk mendapatkan informasi yang valid dan reliabel.

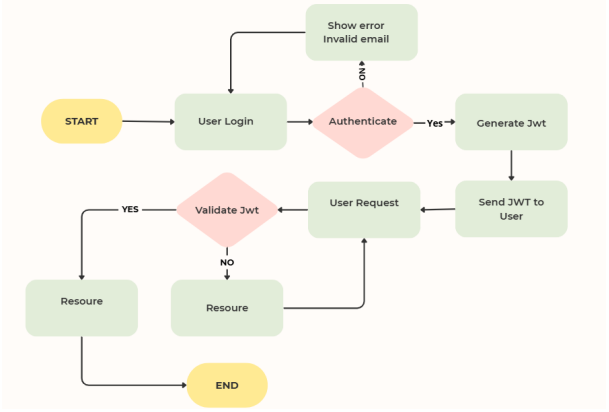
Penelitian ini menggunakan pendekatan kualitatif deskriptif yang bertujuan untuk menggambarkan secara rinci penggunaan JWT dalam konteks aplikasi fisoterapi, khususnya pada aspek keamanan dan autentikasi. Pendekatan ini dipilih karena memberikan kesempatan untuk mengeksplorasi berbagai faktor yang mempengaruhi implementasi JWT, serta menganalisis kelemahan dan tantangan yang dihadapi dalam penerapannya dan evaluasi hasil klasifikasi untuk menjawab rumusan masalah yang telah ditetapkan.

B. *Alur Penelitian*

Alur penelitian ini mencakup lima langkah utama, yaitu: perencanaan, pengumpulan data, analisis data, evaluasi temuan, dan penarikan Kesimpulan. Aplikasi TerapiCare dikembangkan menggunakaqn arsitektur tiga Tingkat (three-tier architecture) yang terdiri dari frontend berbasis React/Vite, backend menggunakan Laravel, dan database MySQL. Frontend berkomunikasi dengan backend melalui REST API untuk proses autentikasi dan manajemen data, sedangkan komunikasi real-time antara pasien dan terapis didukung oleh Socket.IO melalui WebSocket. Pada proses autentikasi, Laravel memverifikasi kredensial pengguna dan menghasilkan JSON Web Token (JWT) yang memuatt informasi peran pengguna, yaitu admin, terapis, dan pasien. Token tersebut selanjutnya digunakan dalam mekanisme Role-Based Access Control (RBAC) untuk mengatur hak akses terhadap fitur dan data sesuai peran masing-masing pengguna. Seluruh data penting, termasuk data pasien dan rekam medis, disimpan pada database MySQL.

Setelah sistem dikembangkan, dilakukan analisis terhadap implementasi JWT menggunakan teknik analisis tematik untuk mengidentifikasi pola-pola yang berkaitan dengan autentikasi dan otorisasi. Selain itu, analisis SWOT digunakan untuk mengevaluasi kekuatan, kelemahan, peluang, dan ancaman dari penerapan JWT pada aplikasi layanan fisioterapi [9]. Selanjutnya, hasil analisis dievaluasi dengan membandingkan implementasi yang dilakukan terhadap standar keamanan dan praktik terbaik yang terdapat pada penelitian terdahulu. Untuk memastikan kualitas sistem, dilakukan pengujian menggunakan Unit Testing, API Testing dengan Postman, dan End-to-End Testing menggunakan Cypress. Tahap akhir penelitian dilakukan dengan menarik kesimpulan berdasarkan hasil analisis dan evaluasi yang diperoleh serta memberikan rekomendasi untuk pengembangan sistem di masa mendatang.

C. *Perancangan Autentikasi Json Web Token dalam RBAC*



Gbr. 2 Alur Perancangan Autentikasi Json Web Token dalam RBAC

1) *Implementasi proses Autentikasi dengan JWT*

Implementasi autentikasi pada aplikasi TerapiiCare menggunakan JSON Web Token (JWT) sebagai mekanisme verifikasi identitas pengguna dan pengelola hak akses. Jwt merupakan standar terbuka yang digunakan untuk mengirimkan informasi secara aman dalam format JSON dan terdiri dari tiga bagian utama, yaitu header, payload, dan signature [10]. Proses autentikasi dimulai Ketika pengguna memasukkan kredensial berupa username dan password melalui halaman login. Server kemudia memverifikasi data tersebut dengan data yang tersimpan

pada basis data. Apabila kredensial valid, sitem akan menghasilkan token JWT yang memuat informasi identitas pengguna beserta perannya, seperti admin, terapis, atau pasien. Token yang telah dibuat kemudia dikirimkan kepada pengguna dan disimpan pada sisi klien untuk digunakan pada permintaan berikutnya.

Pada setiap permintaan akses, token JWT dikirimkan melalui *header Authorization* dengan format Bearer Token. Server akan melakukan validasi token untuk memastikan keaslian, integritas, dan masa berlaku token sebelum memproses permintaan pengguna[11]. Setelah token dinyatakan valiud, system akan memeriksa informasi peran yang tersimpan didalam token untuk menentukan hak akses sesuai mekanisme *Role-Based Access Control* (RBAC). Keamanan proses autentikasi diperkuat melalui penggunaan protocol HTTPS untuk melindungi data selama tranmisi serta algoritma penandatanganan seperti HMAC SHA256 untuk mencegah manipulasi token[12]. Selain itu, system juga menerapkan pengelolaan token yang aman melalui mekanisme masa berlaku token dan pembaruan akses guna meminimalkam Risiko penyalahgunaan apabila token hilang atau dicuri[13]

D. Testing

1) Pengujian Kinerja Sistem

Pengujian performa pada aplikasi TerapiCare dilakukan menggunakan Grafana K6 untuk mengetahui kemampuan sistem dalam menangani request pengguna pada beberapa fitur utama. Pengujian ini difokuskan pada proses yang berhubungan langsung dengan integrasi backend dan frontend, seperti login pengguna, pengambilan data jadwal, pemesanan layanan fisioterapi, unggah bukti pembayaran, verifikasi pembayaran, dan akses dashboard terapis. Grafana K6 digunakan karena mampu melakukan load testing terhadap endpoint API dan menampilkan metrik performa seperti durasi request, jumlah request, tingkat kegagalan request, jumlah iterasi, serta penggunaan virtual users atau VUs. Dalam dokumentasi Grafana K6, metrik utama yang umum digunakan untuk membaca hasil pengujian meliputi http_req_duration sebagai waktu total request, http_req_failed sebagai jumlah request gagal, dan iterations sebagai jumlah pengulangan skenario pengujian.

a Perhitungan Kinerja

$$\text{Throughput: } \frac{x \text{ requests}}{60 \text{ detik}} = x \text{ requests/sec}$$

b Access Violation Rate

Pengujian dilakukan untuk memverifikasi bahwa peran yang diberikan pada pengguna sesuai dengan akses yang diberikan dalam sistem.

$$\text{Access Violation Rate: } \frac{x}{100} \times 100 = x\%$$

c Misconfiguration Rate

Sistem audit trail digunakan untuk memonitor dan mencatat aktivitas akses pengguna, memastikan bahwa pelanggaran akses dapat dideteksi dan dicatat.

$$\text{Misconfiguration Rate: } \frac{x}{50} \times 100 = x\%$$

2) Pengujian Keamanan Sistem

Pengujian keamanan website pada aplikasi TerapiCare dilakukan menggunakan Xray Web Scanner. Pengujian ini bertujuan untuk mengetahui potensi celah keamanan pada aplikasi web, khususnya pada endpoint yang berkaitan dengan autentikasi, otorisasi, akses data pengguna, dan komunikasi antara frontend dengan backend. Pengujian dilakukan setelah sistem berhasil menerapkan autentikasi menggunakan JSON Web Token (JWT) dan pembatasan hak akses menggunakan Role-Based Access Control (RBAC). Aspek-aspek yang diuji meliputi potensi *SQL Injection*, *Cross-Site Scripting* (XSS), kelemahan konfigurasi *security header*, akses endpoint tanpa otorisasi, *directory traversal* atau *path traversal*, *sensitive information disclosure*, serta kemungkinan terjadinya kesalahan konfigurasi pada server. Objek pengujian dalam penelitian ini adalah website aplikasi TerapiCare yang telah diimplementasikan dan dapat diakses melalui alamat aplikasi yang telah ditentukan. Pemindaian dilakukan terhadap halaman dan endpoint yang tersedia pada sistem untuk mengamati respons aplikasi terhadap serangkaian permintaan dan *payload* pengujian yang dikirimkan secara otomatis oleh alat pemindai. Melalui pendekatan tersebut, pengujian tidak hanya menilai keberadaan kerentanan, tetapi juga mengamati stabilitas respons sistem selama proses pemindaian berlangsung.

3) Prosedur Pengujian Keamanan Sistem

Prosedur pengujian keamanan sistem dalam penelitian ini dilakukan secara bertahap agar proses evaluasi keamanan dapat berjalan secara terstruktur.

a. menentukan target pengujian, yaitu website aplikasi TerapiCare yang telah selesai diimplementasikan.
b. melakukan konfigurasi alat pengujian, yaitu Xray Web Scanner, sesuai dengan kebutuhan pengujian..
c. pelaksanaan pemindaian otomatis terhadap sistem.
d. pengumpulan dan analisis log hasil pemindaian.
e. melakukan interpretasi terhadap hasil pengujian.

Indikator keberhasilan pada pengujian keamanan sistem dalam penelitian ini ditentukan berdasarkan beberapa kondisi. Pertama, seluruh *request* pengujian yang dikirimkan oleh alat pemindai dapat diproses dengan baik oleh sistem sehingga proses evaluasi dapat berlangsung secara menyeluruh. Kedua, sistem menunjukkan tingkat stabilitas respons yang baik selama pengujian berlangsung, yang dapat diamati melalui nilai *latency* rata-rata dan *failed ratio*. Ketiga, tidak terdapat log yang menunjukkan bahwa *payload* yang dijalankan berhasil mengeksploitasi aplikasi, baik pada pengujian *file read*, *information leak*, *SQL Injection*, *path traversal*, maupun *authentication bypass*.Selain itu, keberhasilan pengujian keamanan juga ditinjau dari kemampuan sistem dalam mempertahankan pembatasan akses terhadap endpoint yang diuji. Dalam hal ini, implementasi JWT diharapkan mampu memastikan bahwa hanya pengguna dengan token yang valid yang dapat mengakses sumber daya tertentu, sedangkan RBAC diharapkan mampu membatasi akses terhadap fitur sesuai dengan peran pengguna.

III. HASIL DAN PEMBAHASAN

A. *Implementasi Autentikasi JWT*

Autentikasi JWT (JSON Web Token) diterapkan pada aplikasi TerapiCare untuk mengamankan akses pengguna dan menjaga integritas data. Prosesnya dimulai saat pengguna memasukkan username dan password pada halaman login. Backend memverifikasi kredensial tersebut terhadap database, dan jika valid, server menghasilkan JWT yang berisi informasi identitas pengguna dan perannya.

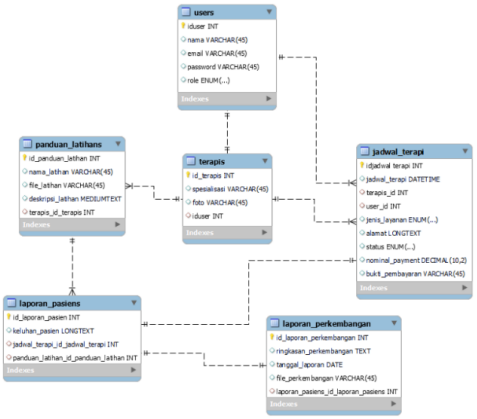
a. Persiapan Sistem

Tahap awal yang dilakukan adalah persiapan sistem agar lingkungan pengembangan dan produksi siap mendukung keamanan serta integritas data. Tahap ini mencakup beberapa langkah penting.

1. Setup Backend Laravel

Framework Laravel dipilih karena memiliki ekosistem yang lengkap dan dukungan library untuk autentikasi berbasis token. Seluruh paket yang dibutuhkan, termasuk tymon/jwt-auth, diinstal agar mendukung pembuatan, verifikasi, dan refresh token JWT. Dengan cara menggunakan commad pada terminal laragon.

Gbr. 3 Setup Backend Laravel



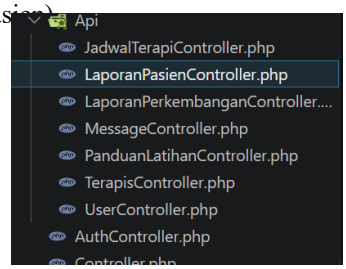
2. Konfigurasi Database (MySQL)

Gbr. 4 Entity Attribute Relationship

Database MySQL digunakan untuk menyimpan data pengguna, peran (role), serta histori login. Tabel-tabel utama, seperti users dan roles, dibuat dengan struktur yang mendukung relasi one-to-many dan foreign key, sehingga integritas data tetap terjaga.

3. Konfigurasi JSON Web Token

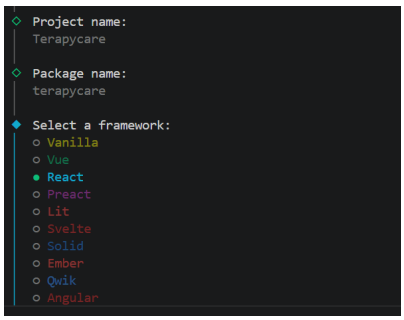
Library JWT diatur dengan secret key yang unik dan aman untuk menandatangani token. Parameter tambahan seperti masa berlaku token (TTL), algoritma enkripsi (HS256), serta klaim tambahan (role, iat, exp) disiapkan agar token dapat digunakan secara fleksibel untuk berbagai tipe user (Admin, Terapis, Pasien).



Gbr. 5 Controller

4. Setup Frontend (React/Vite)

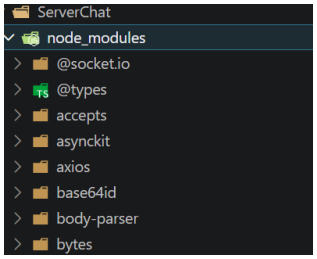
Project diinisiasi dengan struktur modular yang memisahkan komponen, halaman, dan hooks. Library tambahan seperti Axios digunakan untuk komunikasi dengan backend. Pengaturan environment di frontend juga dilakukan agar API URL dapat dikonfigurasi sesuai deployment.



Gbr. 6 Setup Frontend (React/Vite)

5. Setup Socket.io

Untuk mendukung komunikasi real-time, Socket.IO diintegrasikan pada backend Laravel dan frontend React. Backend menyediakan endpoint WebSocket menggunakan pusher atau laravel-websockets, sedangkan frontend menggunakan Socket.IO client untuk menerima dan mengirim pesan secara real-time. Hal ini memungkinkan fitur chat pasien-terapis berjalan



lancar tanpa menunggu refresh halaman.

Mekanisme pada Server chat dapat di gambarkan melalui gambar di bawah ini :

Gbr. 7 Socket.io

b. Pembuatan Token dan Validasi

Pembuatan token JWT dan mekanisme validasinya untuk mengamankan akses pengguna. Setelah pengguna berhasil login, backend Laravel membuat token JWT menggunakan library tymon/jwt-auth yang berisi payload seperti iduser, nama, email, dan role, serta klaim standar seperti iat dan exp untuk menentukan masa berlaku token.

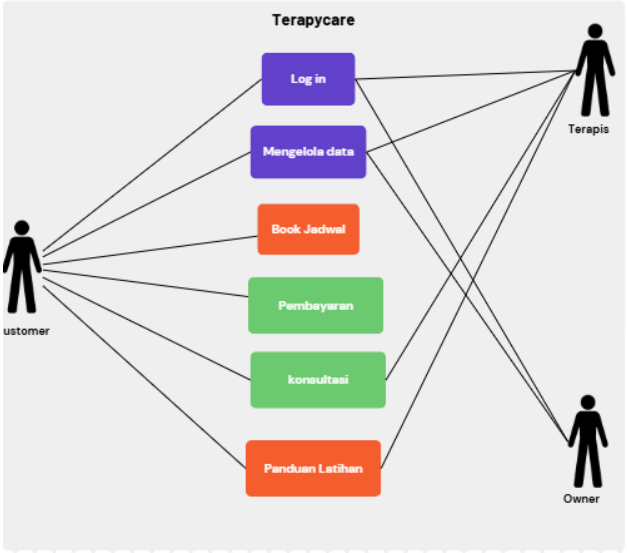
c. Integrasi JWT dengan Frontend

Setelah token JWT berhasil dibuat dan dikirim dari backend, tahap berikutnya adalah integrasi token tersebut dengan frontend aplikasi. Frontend React/Vite menerima token setelah login dan menyimpannya di local storage atau HTTP-only cookie agar dapat digunakan untuk setiap request ke API backend melalui header Authorization: Bearer <token>. Token ini memastikan bahwa setiap permintaan ke server hanya dapat diakses oleh pengguna yang sah sesuai hak akses yang dimiliki.

B. *Hasil Implementasi Role-Based Access Control (RBAC)*

Implementasi Role-Based Access Control (RBAC) pada aplikasi TerapiCare dilakukan dengan memanfaatkan informasi role yang tersimpan pada token JSON Web Token (JWT). Sistem membedakan hak akses pengguna menjadi tiga peran utama, yaitu Admin, Terapis, dan Pasien.

Admin memiliki akses penuh terhadap seluruh modul sistem, Terapis dapat mengakses data pasien yang ditangani, jadwal terapi, serta verifikasi pembayaran, sedangkan Pasien hanya dapat mengakses layanan yang berkaitan dengan dirinya sendiri. Setelah proses login berhasil, backend menghasilkan token JWT yang berisi identitas pengguna beserta informasi perannya. Token tersebut kemudian dikirim pada setiap request API melalui *Authorization Header* dan divalidasi oleh middleware untuk memeriksa keaslian, masa berlaku, serta hak akses pengguna. Hasil implementasi menunjukkan bahwa sistem mampu membatasi akses sesuai peran masing-masing dan menolak akses yang tidak memiliki otorisasi, sehingga keamanan data sensitif serta integritas aplikasi dapat terjaga dengan baik.



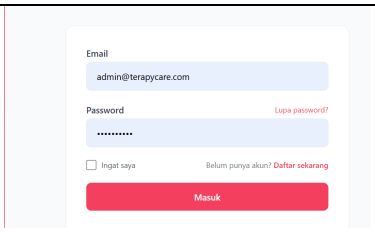
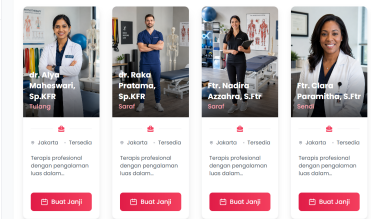
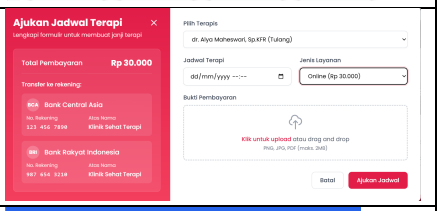
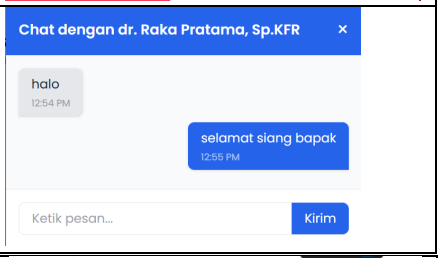
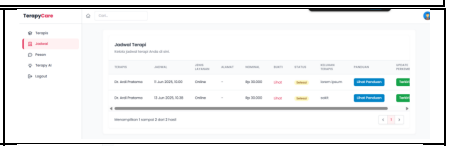
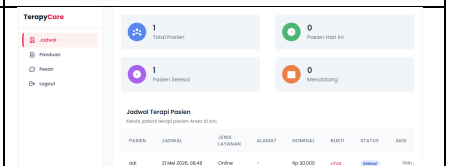
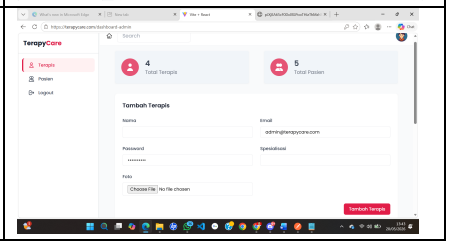
Gbr. 8 Hasil Implementasi Role bassed Access

C. *Implementasi Sistem pada Aplikasi TerapiCare*

Implementasi sistem pada aplikasi TerapiCare dilakukan dengan mengintegrasikan frontend React/Vite, backend Laravel, database MySQL, autentikasi berbasis JSON Web Token (JWT), dan mekanisme Role-Based Access Control (RBAC). Frontend berkomunikasi dengan backend melalui REST API untuk mengelola proses login, pemesanan layanan, pengelolaan jadwal, pembayaran, serta akses data pengguna. Setelah proses login berhasil, system menghasilkan token JWT yang digunakan untuk memverifikasi identitas pengguna pada setiap request.

TABEL I

TABEL IMPLEMENTASI SISTEM PADA APLIKASI TERAPICARE

Halaman	Hasil Antarmuka
Login	
Display Terapis	
Proses Pembayaran Terapycare	
Konsultasi real time	
Panduan Latihan	
Dashboard Terapis	
Dashboard Owner	

Informasi peran yang tersimpan pada token kemudian digunakan oleh RBAC untuk membatasi hak akses sesuai peran pengguna, yaitu Admin, Terapis, dan Pasien.

Hasil implementasi menunjukkan bahwa seluruh fitur utama aplikasi dapat berjalan dengan baik, meliputi proses login, pengelolaan data terapis, pemesanan layanan fisioterapi, pembayaran, konsultasi online, panduan latihan, serta dashboard pengguna. Setiap akses terhadap fitur dan data sensitif divalidasi menggunakan JWT dan RBAC sehingga pengguna hanya dapat mengakses fungsi yang sesuai dengan kewenangannya. Selain itu, integrasi backend dan frontend melalui REST API mampu mendukung pertukaran data secara terstruktur dan responsif, sehingga proses layanan fisioterapi dapat berjalan secara aman, efektif, dan sesuai dengan alur bisnis yang telah dirancang.

D. *Hasil Pengujian Mengguanakan Grafana K6*

Pengujian sistem dilakukan untuk mengevaluasi aspek performa dan keamanan aplikasi TerapiCare. Pengujian performa menggunakan Grafana K6 dengan skenario yang mensimulasikan beberapa pengguna mengakses sistem secara bersamaan melalui fitur utama aplikasi.

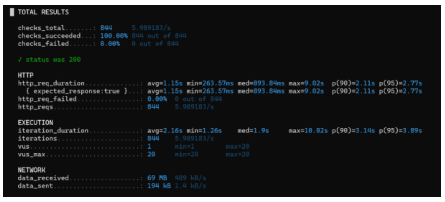
TABEL II

TABEL HASIL PENGUJIAN MENGGUNAKAN GRAFANA K6

Alur	Skenario Pengujian

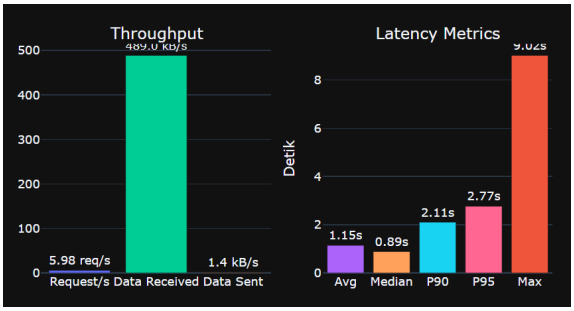
Grafana K6	`import http from 'k6/http';`
	`import { check, sleep } from 'k6';`
	
	`export const options = {`
	`stages: [`
	`{ duration: '30s', target: 20 },`
	`{ duration: '1m30s', target: 10 },`

Grafana K6	`{ duration: '20s', target: 0 },`
	`],`
	`};`
	
	`export default function () {`
	`const res =`
	`http.get('https://api.terapycare.com/');`
	`check(res, { 'status was 200': (r) =>`
	`r.status == 200 });`
	`sleep(1);`
	`}`

Hasil Testing	

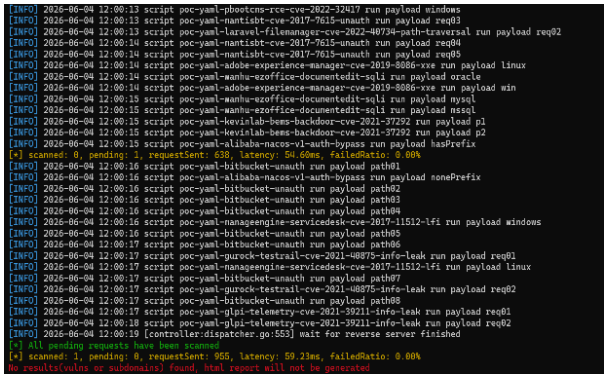
Hasil pengujian menunjukkan bahwa sistem mampu memproses 844 request dalam 60 detik dengan throughput sebesar 9,4 request/second. Nilai rata-rata waktu respons tercatat 1,15 detik dengan median 0,89 detik, sedangkan 90% dan 95% permintaan berhasil diproses masing-masing dalam waktu 2,11 detik dan 2,77 detik. Selain itu, pengujian kontrol akses menunjukkan nilai Access Violation Rate sebesar 0%, yang menandakan bahwa seluruh mekanisme Role-Based Access Control (RBAC) berjalan sesuai dengan hak akses yang telah ditetapkan dan tidak ditemukan pelanggaran akses selama pengujian berlangsung.

Pengujian keamanan dilakukan menggunakan Xray Web Scanner dengan melakukan pemindaian otomatis terhadap halaman dan endpoint aplikasi. Hasil pemindaian menunjukkan 638 request berhasil diproses, rata-rata latency sebesar 54,60 ms, serta failed ratio 0,00%.



Gbr. 9 Hasil Kinerja Website

Pengujian terhadap berbagai potensi kerentanan seperti SQL Injection, Cross-Site Scripting (XSS), authentication bypass, information disclosure, directory traversal, dan kesalahan konfigurasi server tidak menunjukkan adanya indikasi eksploitasi yang berhasil.



Gbr. 10 Hasil Pengujian Menggunakan Xray

Hasil tersebut menunjukkan bahwa implementasi JSON Web Token (JWT) dan Role-Based Access Control (RBAC) mampu mendukung keamanan aplikasi dengan baik melalui pembatasan akses berdasarkan peran dan validasi pengguna yang terautentikasi. Meskipun demikian, pengujian lanjutan secara berkala tetap diperlukan untuk memastikan keamanan sistem tetap terjaga ketika aplikasi digunakan dalam lingkungan produksi dengan jumlah pengguna yang lebih besar.

IV. KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian yang telah dilakukan, penerapan JSON Web Token (JWT) dan Role-Based Access Control (RBAC) pada aplikasi layanan fisioterapi berbasis web TerapiCare berhasil meningkatkan keamanan autentikasi dan pengelolaan hak akses pengguna. JWT mampu mendukung proses autentikasi secara aman dan efisien melalui penggunaan token yang memuat identitas serta peran pengguna, sedangkan RBAC berhasil membatasi akses sesuai dengan peran admin, terapis, dan

pasien sehingga kerahasiaan data pasien dapat terjaga. Integrasi frontend React/Vite dengan backend Laravel melalui REST API juga mampu mendukung seluruh fitur utama aplikasi, seperti pemesanan layanan, pengelolaan jadwal, pembayaran, dan konsultasi antara pasien dan terapis. Hasil pengujian menggunakan Grafana K6 menunjukkan bahwa sistem mampu memproses 844 request dalam 60 detik dengan throughput sebesar 9,4 request/second, sedangkan pengujian keamanan menunjukkan bahwa mekanisme autentikasi dan kontrol akses yang diterapkan berjalan sesuai dengan kebutuhan sistem. Dengan demikian, implementasi JWT dan RBAC pada aplikasi TerapiCare dapat menjadi solusi yang efektif untuk meningkatkan keamanan akses dan perlindungan data pada layanan fisioterapi berbasis web.

REFERENSI

[1] R. S. Aiswarya, "MediLock A Token Driven Encryption Framework for Privacy Preserving Healthcare Data Access," *ResearchGate*, 2023, [Online]. Available: https://www.researchgate.net/publication/392803195_MediLock_A_Token_Driven_Encryption_Framework_for_Privacy_Preserving_Healthcare_Data_Access

[2] S. Almohammad Alsaleh, "Permission-Based Dynamic Access Control Models for Enhanced Data Security: Integrating Contextual Awareness and Role Flexibility for Secure Healthcare Data," *Diva Portal*, 2024, [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1900749/FULLTEXT01.pdf

[3] S. Sutradhar, S. Karforma, R. Bose, and S. Roy, "Enhancing identity and access management using hyperledger fabric and OAuth 2.0: A blockchain-based approach for security and scalability for healthcare," *Elsevier*, 2024, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667345223000470

[4] H. F. Atlam and Y. Yang, "Enhancing Healthcare Security: A Unified RBAC and ABAC Risk-Aware Access Control Approach," *Future Internet*, vol. 17, no. 6, 2025, [Online]. Available: https://www.mdpi.com/1999-5903/17/6/262

[5] M. Albayati and A. Murjan, "Profile Based Access Control Model Using JSON Web Tokens," *Lund Univ. Res.*, 2023, [Online]. Available: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9129494&fileOId=9135487

[6] S. Fries and R. Falk, "Handling Role-Based Access Control in the Digital Grid," 2017.

[7] C. Harper, "Role-Based Access Control (RBAC) and Encryption Techniques for Enhancing Relational Database Security," 2025.

[8] J. R. Amalraj and R. Lourdusamy, "A Novel Distributed Token-Based Access Control Algorithm Using a Secret Sharing Scheme for Secure Data Access Control," 2022.

[9] S. Ameer, J. Benson, and R. Sandhu, "Handling Role-Based Access Control in the Digital Grid," *Information*, vol. 13, no. 2, p. 60, 2022.

[10] A. Samadhiya, A. El Jaouhari, and A. Kumar, "Tokenization and the future of property investment: A new paradigm for real estate," *J. Strateg. Prop. Manag.*, 2025, [Online]. Available: PDF

[11] E. D. S. Akhtar, M. U. Rehman, and M. Soomro, "CYBERSECURITY STRATEGIES FOR THE METAVERSE PROTECTING DIGITAL ASSETS, VIRTUAL ECONOMIES, AND USER PRIVACY IN IMMERSIVE ENVIRONMENTS," *Kashf J. Manag. Res.*, 2025, [Online]. Available: PDF

[12] A. Alqudah, "FinTech's AML Reality, 2020–2025: How Digital Rails Enable—and Deter—Money Laundering," *Lex Localis-J. Local Self-Gov.*, 2025, [Online]. Available: PDF

[13] S. Abdullah, "Implementasi Blockchain untuk Keamanan Data Akademik dalam Sistem Informasi Perguruan Tinggi," *Go Infotech J. Ilm. STMIK AUB*, 2025, [Online]. Available: PDF