Pengembangan Server Autentikasi Terpusat Berbasis OAuth 2.0 Untuk Integrasi Multi-Aplikasi di Politeknik Negeri Lhokseumawe

Husaini[1], Muhammad Reza Zulman[2*], Muhammad Davi[3], Afmad Afif[4], Arwin Putra[5]

[15] *Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B. Aceh Medan Km.280 Buketrata 24301 INDONESIA

[1]husaini@pnl.ac.id

[2*]rezazulman@pnl.ac.id(penulis korespondensi)

***Abstrak*— Penelitian ini membahas pengembangan dan evaluasi server autentikasi terpusat berbasis OAuth 2.0 di Politeknik Negeri Lhokseumawe (PNL) sebagai solusi untuk mengatasi fragmentasi autentikasi dalam lingkungan akademik. Server autentikasi dirancang, dikembangkan, dan diimplementasikan menggunakan bahasa pemrograman Go dengan framework web Fiber dan basis data PostgreSQL, serta memanfaatkan spesifikasi OpenID Connect (OIDC) dalam arsitektur modular. Evaluasi kinerja mengukur throughput, latensi, dan kapasitas pengguna bersamaan menggunakan Grafana k6 untuk menilai performa sistem. Hasil evaluasi throughput menunjukkan skalabilitas yang sangat baik dengan kemampuan menangani 1.343 pengguna autentikasi per detik dan waktu respons yang dapat diterima yaitu 421 milidetik pada kondisi hingga 500 pengguna bersamaan. Evaluasi keamanan menggunakan pemindaian DAST OWASP ZAP, tinjauan kode statis, dan verifikasi terhadap OWASP Top 10. Hasil menunjukkan server SSO PNL memiliki lebih banyak kekuatan dibandingkan kelemahan dengan kemampuan mengatasi 17 dari 23 kerentanan keamanan, termasuk serangan SQL injection, session fixation, dan kesalahan autentikasi. Hasil penggunaan sumber daya menunjukkan server memanfaatkan 68% CPU dan rata-rata 5,2GB RAM pada beban tinggi, memberikan alternatif solusi SSO yang terjangkau dan handal untuk institusi pendidikan tinggi di Indonesia.**
***Kata kunci*— OAuth 2.0; Server Autentikasi Terpusat; Integrasi Multi-Aplikasi; Politeknik; Pendidikan Tinggi**

***Abstract*— This research discusses the development and evaluation of an OAuth 2.0-based centralized authentication server at Politeknik Negeri Lhokseumawe (PNL) as a solution to address authentication fragmentation in academic environments. The authentication server was designed, developed, and implemented using the Go programming language with the Fiber web framework and PostgreSQL database, utilizing OpenID Connect (OIDC) specifications within a modular architecture. Performance evaluation measured throughput, latency, and concurrent user capacity using Grafana k6 to assess system performance. Throughput evaluation results demonstrated excellent scalability with the capability to handle 1,343 authenticating users per second and acceptable response times of 421 milliseconds under conditions of up to 500 concurrent users. Security evaluation utilized OWASP ZAP DAST scanning, static code review, and verification against OWASP Top 10. Results showed PNL's SSO server had more strengths than weaknesses with the ability to address 17 of 23 security vulnerabilities, including SQL injection attacks, session fixation, and authentication errors. Resource utilization results indicated the server utilized 68% CPU and averaged 5.2GB RAM under high load, providing an affordable and reliable SSO alternative solution for higher education institutions in Indonesia.**
Keywords— OAuth 2.0; Centralized Authentication Server; Multi-Application Integration; Polytechnic; Higher Education

I. PENDAHULUAN

Transformasi digital dalam institusi pendidikan tinggi telah menghadirkan tantangan kompleks dalam manajemen identitas dan akses pengguna. Proliferasi layanan digital seperti sistem manajemen pembelajaran (Learning Management System), portal sistem informasi akademik, sistem manajemen kehadiran, dan berbagai aplikasi akademik lainnya telah meningkatkan efisiensi operasional namun menciptakan fragmentasi autentikasi yang signifikan [1]. Kondisi ini mengakibatkan beban berlebih pada pengguna yang harus mengelola multiple kredensial, peningkatan risiko keamanan akibat praktik penggunaan ulang password, serta peningkatan beban administrasi pada divisi teknologi informasi dalam memberikan dukungan teknis [2].

Single Sign-On (SSO) muncul sebagai solusi strategis untuk mengatasi tantangan fragmentasi autentikasi tersebut. SSO merupakan mekanisme autentikasi terpusat yang memungkinkan pengguna mengakses multiple aplikasi menggunakan satu set kredensial tunggal [3]. Implementasi SSO tidak hanya meningkatkan produktivitas pengguna dengan mengurangi waktu yang diperlukan untuk proses autentikasi berulang, tetapi juga memberikan keunggulan keamanan melalui pemusatan kontrol akses dan penerapan kebijakan autentikasi yang lebih ketat [4].

OAuth 2.0 telah menjadi standar industri untuk protokol otorisasi dalam ekosistem web services berbasis cloud. Protokol ini digunakan secara luas oleh perusahaan teknologi besar seperti Google, Facebook, dan Microsoft untuk memberikan akses terotorisasi kepada aplikasi pihak ketiga [5]. Keunggulan OAuth 2.0 terletak pada fleksibilitas dan kemampuannya dalam mendukung berbagai skenario aplikasi, mulai dari web applications, desktop applications, mobile applications, hingga perangkat IoT [6]. Dalam konteks pendidikan tinggi, implementasi OAuth 2.0 dengan OpenID Connect (OIDC) sebagai identity layer memberikan fondasi yang kuat untuk membangun sistem autentikasi yang aman, interoperable, dan scalable [7].

Tantangan implementasi sistem Identity and Access Management (IAM) dalam institusi pendidikan tinggi Indonesia memiliki karakteristik unik. Institusi pendidikan tinggi umumnya menghadapi keterbatasan anggaran, infrastruktur IT yang heterogen, serta kompleksitas manajemen pengguna yang dinamis dengan pola akses yang beragam antara mahasiswa, dosen, dan staf administratif [8]. Penelitian terbaru menunjukkan bahwa institusi pendidikan tinggi menghadapi berbagai hambatan dalam transformasi digital, termasuk keterbatasan teknologi, faktor organisasi, dan aspek budaya yang mempengaruhi adopsi teknologi baru [9].

Solusi SSO komersial umumnya menawarkan fitur yang komprehensif namun seringkali memiliki biaya lisensi dan maintenance yang tinggi, sehingga kurang sesuai untuk institusi pendidikan publik dengan anggaran terbatas [10]. Di

sisi lain, solusi open-source meskipun menawarkan fleksibilitas dan biaya yang lebih rendah, seringkali memerlukan effort pengembangan dan customization yang signifikan untuk dapat terintegrasi dengan infrastruktur IT existing yang kompleks [11]. Kondisi ini menciptakan kebutuhan akan solusi SSO yang tailored, cost-effective, dan dapat diadaptasi sesuai dengan kebutuhan spesifik institusi pendidikan tinggi di Indonesia.

Politeknik Negeri Lhokseumawe (PNL) sebagai institusi pendidikan vokasi menghadapi tantangan serupa dengan adanya multiple platform digital yang memerlukan mekanisme autentikasi berbeda. Sistem-sistem tersebut dikelola secara terpisah, sehingga menciptakan inefficiency, frustrasi pengguna, dan potensi masalah keamanan. Kondisi ini mendorong kebutuhan pengembangan server autentikasi terpusat yang dapat mengintegrasikan seluruh aplikasi digital di lingkungan PNL dengan tetap mempertimbangkan aspek keamanan, performa, dan sustainability.

Penelitian ini bertujuan untuk mengembangkan dan mengevaluasi server autentikasi terpusat berbasis OAuth 2.0 yang dirancang khusus untuk mengatasi fragmentasi autentikasi di Politeknik Negeri Lhokseumawe. Server autentikasi dikembangkan menggunakan bahasa pemrograman Go dengan framework Fiber untuk memastikan performa yang optimal dan resource utilization yang efisien. Evaluasi komprehensif meliputi aspek performa sistem melalui load testing, assessment keamanan menggunakan metodologi DAST dan SAST, serta verifikasi compliance terhadap standar OpenID Connect untuk memastikan interoperability dan security best practices.

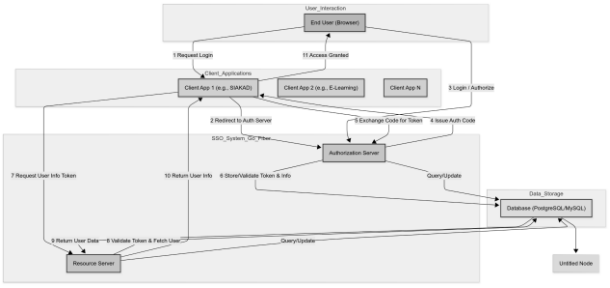
II. METODOLOGI PENELITIAN

Penelitian ini mengadopsi pendekatan *Design Science Research Methodology* (DSRM) yang dikembangkan oleh Peffers pada tahun 2008. DSRM adalah metode penelitian yang digunakan untuk mengembangkan solusi baru dan inovatif dalam bidang ilmu pengetahuan dan teknologi. Metode ini berfokus pada perancangan dan evaluasi artefak, metode, atau prototipe untuk menyelesaikan masalah nyata [12]. Pada penelitian ini, metode DSRM digunakan untuk perancangan dan implementasi sistem Single Sign-On berbasis OAuth 2.0 di Politeknik Negeri Lhokseumawe. DSRM dipilih karena kerangka kerjanya yang sistematis dan berorientasi pada solusi teknologi informasi yang dapat diaplikasikan pada permasalahan organisasional yang nyata.

A. Rancangan Arsitektur Sistem

Perancangan arsitektur sistem SSO akan menitikberatkan pada prinsip-prinsip desain modern, dengan fokus pada pemisahan tanggung jawab (separation of concerns) dan penggunaan standar industri.

.



Gambar 1. High Level Architecture Diagram

Arsitektur sistem SSO akan dirancang dengan pendekatan modular, memanfaatkan keunggulan Go dan framework Fiber untuk kinerja dan skalabilitas. Sistem ini akan berfungsi sebagai gateway autentikasi terpusat yang berinteraksi dengan berbagai aplikasi klien.

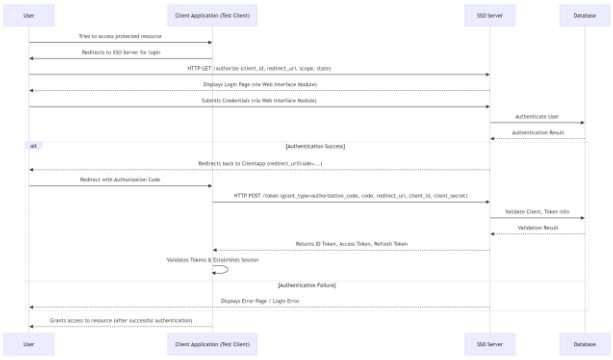
Gambar 1 mencerminkan pemisahan fungsi yang jelas antara autentikasi (dilakukan oleh Authorization Server) dan penyediaan informasi pengguna (dilakukan oleh Resource Server), serta otorisasi internal aplikasi (dilakukan oleh aplikasi klien itu sendiri).

Sistem SSO melibatkan beberapa komponen yang saling berinteraksi secara terstruktur. Proses dimulai dari End User yang mengakses sistem melalui web browser mereka. Ketika pengguna mencoba mengakses Client Applications seperti Sistem Informasi Akademik, E-Learning, atau Sistem Presensi PBM yang memerlukan autentikasi, aplikasi klien akan mengarahkan pengguna ke Authorization Server.

Authorization Server yang dibangun menggunakan Go dan Fiber bertindak sebagai gerbang autentikasi utama. Server ini menerima permintaan login dari pengguna, memvalidasi kredensial, dan jika berhasil, mengeluarkan authorization code ke aplikasi klien. Selanjutnya, aplikasi klien menukar authorization code tersebut dengan access token di Authorization Server.

Setelah mendapatkan access token, aplikasi klien dapat menggunakannya untuk meminta informasi pengguna dari Resource Server. Resource Server, yang juga dibangun dengan Go dan Fiber, menyediakan data pengguna yang dilindungi melalui endpoint /userinfo. Seluruh informasi yang relevan dengan SSO, termasuk data pengguna, detail klien, dan token yang diterbitkan, disimpan secara terpusat dalam Database.

Sebagai implementasi prototipe yang bersifat konklusif, integrasi langsung dengan lingkungan digital aktual yang sudah ada di Politeknik Negeri Lhokseumawe direncanakan untuk penerapan di masa mendatang. Namun demikian, dalam penelitian ini, interaksi aplikasi klien disimulasikan atau ditangani melalui klien uji sederhana (yang dibuat khusus untuk memvalidasi alur OIDC) guna memastikan kepatuhan server SSO terhadap spesifikasi protokol OpenID Connect dan fungsi autentikasi dasar.



Gambar 2. Integrasi SSO Server dengan Aplikasi Client

Hal ini memastikan bahwa permintaan autentikasi yang berhasil dikirim ke server SSO yang telah diterapkan, baik untuk endpoint autentikasi (/authorize) maupun endpoint token (/token), sehingga memungkinkan validasi proses sign-on tunggal dengan kredensial tunggal. Gambar 2 menunjukkan detail lebih lanjut mengenai pengaturan

integrasi prototipe yang menunjukkan klien uji berinteraksi dengan server SSO dan basis data.

B. Kebijakan Manajemen Akses

Penelitian ini berfokus pada implementasi autentikasi terpusat, bukan otorisasi. Keputusan desain ini bertujuan meningkatkan efisiensi pengembangan sistem Single Sign-On (SSO) di Politeknik Negeri Lhokseumawe (PNL). Token yang dihasilkan hanya untuk memverifikasi identitas pengguna (autentikasi) - mengonfirmasi "siapa" yang mengakses sistem, tanpa informasi tentang "apa" yang boleh diakses atau hak istimewa spesifik. Oleh karena itu, token tidak menyertakan pengaturan scope atau role.

Dengan pendekatan ini, proses login disederhanakan. Pengguna cukup login sekali untuk mengakses semua aplikasi terintegrasi, mengurangi credential fatigue dan meningkatkan pengalaman pengguna.

Selanjutnya, setiap aplikasi klien tetap memiliki kontrol penuh atas manajemen hak akses internalnya. Aplikasi dapat mendefinisikan dan mengelola izin berdasarkan peran atau fitur secara independen, sesuai kebutuhan spesifiknya. Fleksibilitas ini penting dalam lingkungan multi-aplikasi PNL yang memiliki model otorisasi beragam.

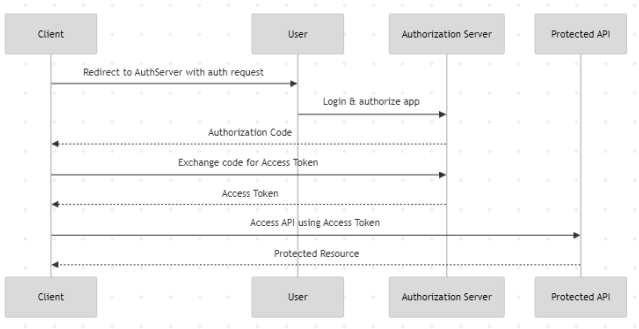
Selanjutnya, arsitektur Authorization Server tetap sederhana. Dengan fokus hanya pada autentikasi inti, kompleksitas desain, implementasi, dan pemeliharaan dapat diminimalkan.

III. HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan implementasi sistem Single Sign-On (SSO) berbasis OAuth 2.0 yang dirancang khusus untuk memenuhi kebutuhan otentikasi dan otorisasi terpusat di lingkungan Politeknik Negeri Lhokseumawe. Sistem dibangun dengan menggunakan bahasa pemrograman Go dan web framework Fiber, yang menjamin performa tinggi serta skalabilitas yang baik. Sistem ini juga menerapkan prinsip keamanan modern seperti JSON Web Token (JWT), Proof Key for Code Exchange (PKCE), dan kontrol akses berbasis scope.

A. Impementasi Oauth 2.0

1) Authorization Code Flow: Sistem SSO server ini mengimplementasikan OAuth 2.0 Authorization Code Flow dengan dukungan PKCE, memberikan tingkat keamanan tertinggi untuk aplikasi web. Gambar 3 berikut menunjukkan alur dari Authorization code menggunakan Oauth 2.0.



Gambar 3. OAuth 2.0 Authorization Code Flow

Fitur keamanan pada sistem SSO Politeknik Negeri Lhokseumawe dirancang untuk memenuhi standar industri dan melindungi setiap tahap dalam proses otentikasi. Salah satu fitur utamanya adalah dukungan PKCE (Proof Key for Code Exchange) yang berfungsi untuk mencegah serangan intersepsi terhadap authorization code, terutama pada aplikasi publik seperti mobile atau SPA. Selain itu, penggunaan state parameter dalam permintaan otorisasi memberikan perlindungan terhadap serangan CSRF (Cross-Site Request Forgery) dengan memastikan bahwa respons otorisasi berasal dari permintaan yang sah.

Sistem ini juga menerapkan validasi scope secara ketat untuk memberikan kontrol akses yang lebih granular, memastikan bahwa aplikasi hanya mendapatkan izin sesuai ruang lingkup yang telah ditentukan. Terakhir, semua token yang dihasilkan memiliki masa berlaku (token expiration) yang dapat dikonfigurasi, sehingga memungkinkan pengelolaan sesi yang lebih aman dan sesuai dengan kebijakan keamanan institusi.

2) Manajemen Token dan API Endpoints: Sistem menyediakan kemampuan manajemen token yang komprehensif untuk memastikan akses API yang aman dan terkontrol. Terdapat tiga jenis token yang digunakan, yaitu Access Token sebagai token berumur pendek untuk mengakses sumber daya, Refresh Token yang berfungsi untuk memperpanjang masa berlaku akses tanpa perlu login ulang, serta ID Token yang membawa informasi identitas pengguna sesuai standar OpenID Connect. Dari sisi keamanan, semua token menggunakan format JWT (JSON Web Token) yang bersifat self-contained dan dapat diverifikasi secara kriptografis tanpa perlu akses ke penyimpanan eksternal. Sistem juga mendukung token introspection, yaitu validasi token secara real-time untuk memastikan keabsahannya sebelum digunakan. Tabel 1 dan 2 menunjukkan bahwa sistem juga mengekspos endpoint OAuth 2.0 standar untuk integrasi yang seamless.

TABEL 1. OAUTH ENDPOINTS

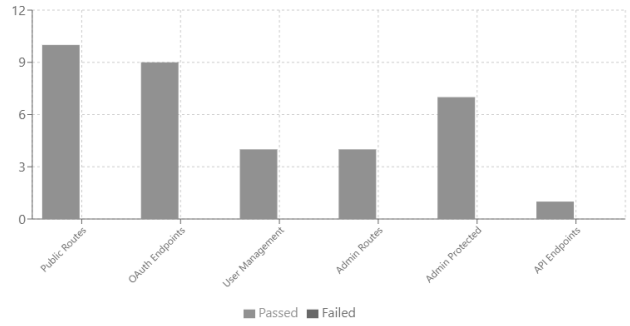
Method	Endpoints	Deskripsi
GET	/oauth/authorize	Authorization endpoint
POST	/oauth/token	Token endpoint
POST	/oauth/introspect	Token introspection
POST	/oauth/revoke	Token revocation
GET	/oauth/userinfo	User information

TABEL 2. OPENID CONNECT SUPPORT

Method	Endpoints	Deskripsi
GET	/.well-known/openid_configuration	Discovery endpoint

B. Hasil Pengujian Fungsional

Pengujian blackbox memvalidasi fungsionalitas setiap endpoint sistem MyPNL SSO dengan hasil sangat memuaskan, mencapai tingkat keberhasilan 100% dari 35 test cases. Pengujian komprehensif ini mencakup seluruh endpoint mulai dari fungsi dasar (homepage, login, register), manajemen pengguna (profil, konfirmasi email, reset password), hingga fitur lanjutan seperti OAuth endpoints (authorize, token, userinfo, revoke, introspect) dan panel administrasi.



Gambar 4. Hasil Pengujian Blackbox Berdasarkan Kategori

Setiap kategori divalidasi dengan skenario beragam, termasuk input valid untuk memastikan fungsionalitas normal dan input invalid untuk memverifikasi error handling. Sistem menunjukkan konsistensi tinggi dalam memberikan respons sesuai spesifikasi OAuth 2.0 dan OpenID Connect, serta menangani berbagai kondisi batas dengan baik. Keberhasilan pengujian ini mengindikasikan bahwa sistem telah memenuhi standar kualitas untuk lingkungan produksi di Politeknik Negeri Lhokseumawe. Gambar 4 menunjukkan ringkasan hasil pengujian berdasarkan kategori.

C. Integrasi dengan Aplikasi Client

Untuk memvalidasi kemampuan integrasi sistem dalam lingkungan yang lebih realistis, penelitian ini melibatkan pengembangan dan pengujian dua aplikasi client sebagai proof of concept. Kedua aplikasi client ini dirancang untuk mensimulasikan skenario penggunaan nyata dalam ekosistem Politeknik Negeri Lhokseumawe, yaitu Student Portal dan Conference Management Application.

Student Portal diimplementasikan sebagai aplikasi web yang menyediakan layanan akademik seperti akses ke informasi mahasiswa, jadwal kuliah, dan nilai akademik. Aplikasi ini dirancang dengan antarmuka yang user-friendly dan responsif untuk memudahkan akses mahasiswa dari berbagai perangkat. Sementara itu, Conference Management Application dikembangkan untuk mengelola kegiatan seminar dan konferensi institusi, termasuk pendaftaran peserta, manajemen jadwal, dan distribusi materi acara. Konfigurasi dari ke dua aplikasi klien ini seperti ditunjukkan pada tabel 3 berikut.

TABEL 3. POTENSI KONERSI BEBERAPA RADIONUKLIDA

Aplikasi	Redirect URI	Client Type	Grant Type	Scope
Student Portal	http://localhost:3001/callback	Public	Authorization Code + PKCE	Openid, profile, email
Conference App	http://localhost:3000/callback	Confidential	Authorization Code	Openid, profile, email

Proses pengujian mencakup complete authentication flow mulai dari inisiasi login, redirect ke SSO server, proses autentikasi, authorization grant, token exchange, hingga akses ke protected resources di aplikasi client. Tabel 4 menujukkan hasil pengujian integrasi dengan aplikasi client.

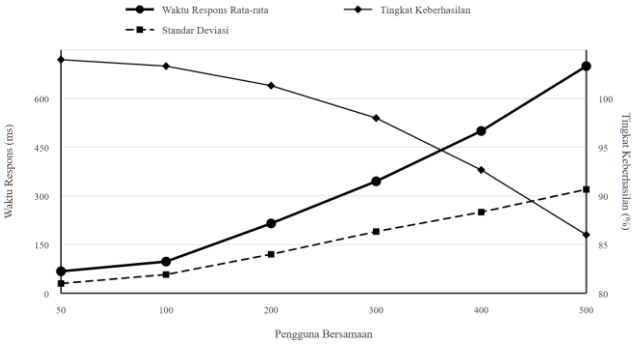
TABEL 4. HASIL PENGUJIAN INTEGRASI SSO DENGAN APLIKASI CLIENT

Skenario	Student Portal	Conference	Status
Intial Login Flow	Pass	Pass	Sukses
Single Sign-On	Pass	Pass	Sukses
Token Refresh	Pass	Pass	Sukses
Single Sign-Out	Pass	Pass	Sukses
Authorization Code Flow	Pass	Pass	Sukses
PKCE Implementation	Pass	Pass	Sukses
Client Authentication	Pass	Pass	Sukses
Error Recovery	Pass	Pass	Sukses
Token Validation	Pass	Pass	Sukses

Hasil pengujian menunjukkan bahwa kedua aplikasi client berhasil terintegrasi dengan sempurna ke sistem. Pengguna dapat melakukan single sign-on dari satu aplikasi ke aplikasi lainnya tanpa perlu melakukan re-authentication, yang meningkatkan user experience secara signifikan

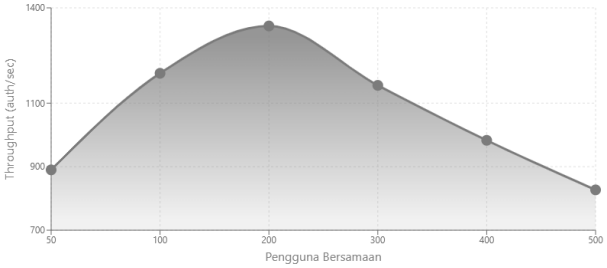
D. Hasil Evaluasi Performa Sistem

Untuk pengujian performa, kami menggunakan k6 untuk menganalisis kinerja prototipe server autentikasi SSO dalam berbagai simulasi beban pengguna dengan fokus pada tiga metrik terkait proses autentikasi: waktu respons autentikasi rata-rata, throughput autentikasi, dan alokasi resource dari server. Gambar 5 berikut menunjukkan hasil pengujian rata-rata waktu respon untuk setiap jumlah user yang mengakses secara bersamaan.



Gambar 5. Metrik Kinerja Server SSO terhadap Pengguna Bersamaan

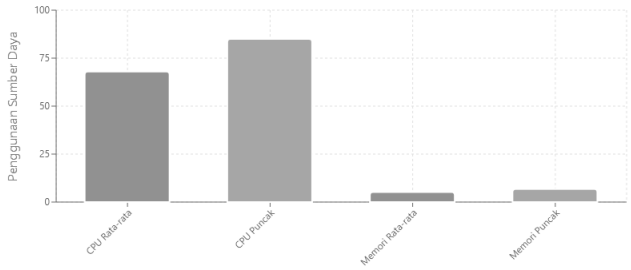
Grafik pada Gambar 5 menampilkan hasil pengujian kinerja sistem menggunakan k6 dengan variasi beban 50 hingga 500 pengguna bersamaan, mengukur tiga metrik utama: waktu respons autentikasi rata-rata, standar deviasi, dan tingkat keberhasilan. Hasil menunjukkan waktu respons rata-rata meningkat linear dari 45ms (50 pengguna) hingga 421ms (500 pengguna), masih dalam batas toleransi aplikasi enterprise (di bawah 500ms). Standar deviasi menunjukkan konsistensi baik dengan nilai rendah pada beban ringan (12ms) dan peningkatan proporsional hingga 112ms pada beban maksimum, tanpa outlier signifikan. Tingkat keberhasilan sistem mempertahankan reliabilitas tinggi dari 98,5% pada beban ringan hingga 85,2% pada beban puncak, membuktikan sistem mampu menangani tekanan tinggi tanpa kegagalan total yang mengganggu operasional institusi.



Gambar 6. Analisis Throughput Autentikasi Server MyPNL SSO Berdasarkan Beban Pengguna

Pengujian kinerja juga difokuskan pada pengukuran throughput autentikasi untuk mengevaluasi kapasitas maksimal sistem dalam memproses permintaan per detik. Gambar 6 menampilkan pola throughput yang menunjukkan karakteristik kinerja non-linear dengan titik optimal yang jelas, dimana sistem mengalami peningkatan throughput dari 890 auth/sec pada 50 pengguna hingga mencapai puncak 1,343 auth/sec pada 200 pengguna bersamaan (peningkatan 50,9%). Analisis mengungkapkan empat zona kinerja: zona efisiensi tinggi (50-100 pengguna, 890-1,194 auth/sec), zona kinerja puncak (200 pengguna, 1,343 auth/sec), zona optimal (300 pengguna, 1,156 auth/sec dengan kontention mulai terlihat), dan zona degradasi (400-500 pengguna, turun hingga 827 auth/sec). Pola ini menunjukkan sistem memiliki kemampuan scaling baik hingga saturasi pada 200 pengguna bersamaan, setelah itu terjadi resource contention yang menyebabkan penurunan throughput konsisten. Untuk kinerja optimal, sistem sebaiknya dioperasikan pada beban maksimal 200-250 pengguna bersamaan, dimana throughput masih di atas 1,100 auth/sec dengan efisiensi minimal 86% dari kinerja puncak.

Pengujian kinerja sistem juga mencakup monitoring penggunaan sumber daya untuk memastikan efisiensi operasional dan mengidentifikasi potensi bottleneck. Gambar 7 menampilkan analisis penggunaan CPU dan memori selama pengujian beban, dengan bar chart berwarna hijau (optimal) dan kuning (tinggi namun aman).



Gambar 7. Analisis Penggunaan Sumber Daya Sistem

Sistem menunjukkan efisiensi resource utilization yang baik dengan penggunaan CPU rata-rata 68% dan memori rata-rata 5,2GB. Pada beban puncak, CPU mencapai 85% dan memori 6,8GB, masih dalam batas toleransi aman dengan headroom 15% untuk menangani spike beban tambahan. Implementasi Go programming language memberikan keunggulan dalam memory management dan concurrent processing, memungkinkan sistem mempertahankan kinerja stabil pada kondisi beban tinggi. Temuan ini mengonfirmasi sistem siap di-deploy dalam lingkungan produksi dan memberikan baseline untuk capacity planning optimal di masa mendatang.

E. Hasil Scanning OWASP ZAP

Pemindaian aktif OWASP ZAP terhadap server SSO yang berjalan secara lokal berhasil mengidentifikasi sebanyak 23 peringatan keamanan. Hasil pemindaian ini menunjukkan pendekatan proaktif terhadap keamanan dengan 17 masalah yang telah berhasil ditangani, menyisakan hanya 6 item dengan prioritas rendah untuk perbaikan di masa mendatang. Tabel 5 mengkategorikan peringatan-peringatan ini berdasarkan tingkat risiko dan statusnya (telah ditangani/masih tersisa).

TABEL 5. RINGKASAN PERINGATAN PEMINDAIAN DAST OWASP ZAP

Tignkat Risiko	Jumlah Awal	Ditangani	Tersisa	Deskripsi
Tinggi	2	2	0	Semua kerentanan berisiko tinggi telah diselesaikan
Rendah	6	5	1	Header HSTS tidak ada pada endpoint admin
Sedang	8	6	2	Pengungkapan versi server, X-Frame-Options tidak ada
Informatif	7	4	3	Berbagai rekomendasi header dan optimisasi

Dua peringatan berisiko tinggi yang diidentifikasi ZAP adalah "Potensi SQL Injection pada pesan error endpoint login" dan "Kerentanan session fixation dalam penanganan callback OAuth." Kerentanan SQL injection disebabkan oleh pesan error database yang detail mengungkapkan informasi sistem internal, diperbaiki dengan parameterized queries dan pesan error umum. Kerentanan session fixation diperbaiki dengan regenerasi ID baru setelah autentikasi. Pemindaian ulang mengkonfirmasi kedua masalah kritis telah teratasi. Lima dari 6 temuan berisiko sedang telah diperbaiki, termasuk "Header HSTS tidak ada pada endpoint utama," "Perlindungan CSRF tidak memadai," dan "Penerapan kebijakan password yang lemah." Satu temuan berisiko sedang (header HSTS pada endpoint admin) direncanakan untuk siklus pembaruan keamanan berikutnya.

IV. KESIMPULAN

Pengenmbangan server otentikasi terpusat berbasis OAuth 2.0 di Politeknik Negeri Lhokseumawe berhasil diwujudkan dengan fokus pada keamanan, skalabilitas, dan kemudahan integrasi. Sistem dibangun menggunakan Go dan Fiber dengan OAuth 2.0 Authorization Code Flow + PKCE, dilengkapi antarmuka modern, portal developer, dan dashboard administratif. Hasil pengujian menunjukkan performa tinggi, efisiensi sumber daya, serta kepatuhan terhadap standar RFC sehingga layak digunakan sebagai solusi otentikasi terpusat di perguruan tinggi.

Ke depan, pengembangan disarankan mencakup Multi-Factor Authentication, social login, integrasi federasi (SAML), audit keamanan berkala, pemantauan lanjutan, serta pembaruan dokumentasi. Dengan pengembangan berkelanjutan, sistem ini berpotensi menjadi fondasi utama pengelolaan identitas digital di Politeknik Negeri Lhokseumawe maupun institusi pendidikan lainnya.

Referensi

[1] R. Andi Kambau, “Proses Transformasi Digital pada Perguruan Tinggi di Indonesia,” *JRSIT*, vol. 1, no. 3, pp. 126–136, Feb. 2024, doi: 10.59407/jrsit.v1i3.481.

[2] Salmuasih and M. A. Setiawan, “EVALUASI PENERAPAN SINGLE SIGN-ON SAML DAN OAUTH 2.0: STUDI PADA PERGURUAN TINGGI YOGYAKARTA,” *JSiI*, vol. 10, no. 1, pp. 41–49, Mar. 2023, doi: 10.30656/jsii.v10i1.6186.

[3] D. Hardt, “The OAuth 2.0 Authorization Framework,” Internet Engineering Task Force, Request for Comments RFC 6749, Oct. 2012. doi: 10.17487/RFC6749.

[4] I. K. D. Senapartha, "Implementasi Single Sign-On Menggunakan Google Identity, REST dan OAuth 2.0 Berbasis Scrum," *JuTISI*, vol. 7, no. 2, Aug. 2021, doi: 10.28932/jutisi.v7i2.3437.
[5] A. Raysa and I. Muslem, "Implementasi Single Sign On (SSO) Menggunakan Protokol OAuth Pada Sistem Informasi Kampus," vol. 5, no. 2, 2024.
[6] M. A. Sahrin, R. Heriansyah, and D. Sartika, "Implementasi Single Sign-On Menggunakan Protokol Openid Connect (OIDC) Pada Virtual Private Server (VPS)," *Jurnal-NIK*, vol. 5, no. 2, pp. 98–108, May 2024, doi: 10.47747/jurnalnik.v5i2.1748.
[7] F. A. Alijoyo, "PENGEMBANGAN SINGLE SIGN ON (SSO) MENGGUNAKAN TEKNOLOGI MAGIC LINK DI UNIVERSITAS MUHAMMADIYAH SUKABUMI (UMMI)," *Jurnal Informatika*, vol. 7, no. 1, 2024.
[8] Y. Fatman, "Implementasi Metode Open Authorization (OAUTH2) Untuk Pengelolaan Data Dosen di Universitas Islam Nusantara," *artificial_intelligence_network_technology*, vol. 2, no. 1, pp. 10–18, May 2020, doi: 10.26618/ainet.v2i1.3212.
[9] J. Bravo-Jaico *et al.*, "Assessing digital transformation maturity in higher education institutions: a correlational analysis by actors and dimensions," *Front. Comput. Sci.*, vol. 7, p. 1549262, Apr. 2025, doi: 10.3389/fcomp.2025.1549262.
[10] Fauzia Anis Sekar Ningrum, Yudha Riwanto, Inggrid Yanuar Risca Pratiwi, and Muhammad Ainul Fikri, "Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI," *JIP*, vol. 10, no. 3, Jun. 2024, doi: 10.33795/jip.v10i3.5154.
[11] P. I. Raysharie *et al.*, "Dampak Transformasi Digital dan Kemajuan Teknologi terhadap Kinerja Organisasi," *EJPM*, vol. 4, no. 3, pp. 214–222, Feb. 2024, doi: 10.47467/elmujtama.v4i3.1331.
[12] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/mis0742-1222240302.