P-ISSN: 2774-4574 ; E-ISSN: 363-4582
TRILOGI, 6(4), Okt-Desember 2025 (1-16)

DOI: 10.33650/trilogi.v6i4.13049

SSO dan Single Logout Berbasis JWT untuk Sistem Informasi Universitas Nurul Jadid

Ahmad Halimi
Universitas Nurul Jadid, Indonesia
ahmadhalimi@unuja.ac.id

Aisatur Ridho
Universitas Nurul Jadid, Indonesia
aisahoppo3@gmail.com

Amelia Silvia Putri
Universitas Nurul Jadid, Indonesia
ekaindriawati3@gmail.com

Vina Yusrolana
Universitas Nurul Jadid, Indonesia
vyusrolana@gmail.com

Abstract

Digital transformation in Indonesian universities requires reliable identity and access management as more campus systems are introduced. At Universitas Nurul Jadid (UNUJA), this study identifies three main problems: (1) low user efficiency because users must log in repeatedly (average 6.8 minutes to access four systems with a 14% login error rate), (2) higher security risk due to scattered credentials and uncoordinated logout across systems, and (3) heavy administrative workload for creating and maintaining accounts in multiple applications. This research aims to design, build, and evaluate an integrated Single Sign-On (SSO) and Single Logout (SLO) solution that meets both functional and non-functional requirements in a pesantren-based university environment. A Waterfall method is applied in five stages: analysis (literature review and field study with 35 participants), design (modular architecture and UML), implementation (Laravel 12, PHP 8.3, MySQL 8.4, Redis 7.0, JWT-based authentication), testing (functional, security, performance, and extreme-scenario tests), and maintenance (monitoring with Laravel Telescope and Redis Monitor). The proposed system uses a centralized Identity Provider (IdP) that supports OpenID Connect for modern applications and SAML 2.0 for legacy systems. SLO is implemented through both front-channel and back-channel methods, supported by Redis-based token blacklisting. Test results show the system meets all functional requirements, withstands the tested security scenarios, and remains stable under load (average latency 1.2–2.1 s; P95 1.8–3.2 s; success rate 98.7–99.9%; throughput up to 850 req/s). This study contributes: (1) a "session cycle" framework that combines SSO and SLO for Indonesian higher education, (2) a mixed evaluation rubric covering technical, security, usability, and administrative metrics, and (3) practical guidance on protocol choices, legacy integration, MFA options, and SLO patterns with recovery mechanisms. The results can serve as a blueprint for other institutions facing multi-system authentication challenges.

Keywords: higher education; integrated authentication; Laravel; OpenID Connect; SAML 2.0; Single Logout; Single Sign-On.

Abstrak
Transformasi digital di perguruan tinggi Indonesia menuntut pengelolaan identitas dan akses yang andal seiring bertambahnya sistem informasi kampus. Di Universitas Nurul Jadid (UNUJA), penelitian ini menemukan tiga masalah utama: (1) efisiensi pengguna rendah karena harus login berulang kali (rata-rata 6,8 menit untuk mengakses empat sistem dengan error login 14%), (2) risiko keamanan meningkat akibat kredensial tersebar dan logout tidak terkoordinasi, serta (3) beban admin tinggi untuk pembuatan dan pemeliharaan akun lintas sistem. Penelitian ini bertujuan merancang, membangun, dan mengevaluasi solusi Single Sign-On (SSO) dan Single Logout (SLO) terintegrasi yang memenuhi kebutuhan fungsional dan non-fungsional dalam konteks kampus berbasis pesantren. Metode Waterfall digunakan melalui lima tahap: analisis (studi pustaka dan studi lapangan dengan 35 responden), desain (arsitektur modular dan pemodelan UML), implementasi (Laravel 12, PHP 8.3, MySQL 8.4, Redis 7.0, autentikasi berbasis JWT), pengujian (fungsi, keamanan, performa, dan skenario ekstrem), serta pemeliharaan (monitoring dengan Laravel Telescope dan Redis Monitor). Arsitektur yang diusulkan memakai Identity Provider (IdP) terpusat yang mendukung OpenID Connect untuk aplikasi modern dan SAML 2.0 untuk sistem lama. Mekanisme SLO menggunakan front-channel dan back-channel, ditambah blacklist token berbasis Redis. Hasil uji menunjukkan sistem memenuhi seluruh kebutuhan fungsional, aman terhadap skenario serangan yang diuji, dan tetap stabil saat dibebani trafik (latensi rata-rata 1,2–2,1 detik; P95 1,8–3,2 detik; success rate 98,7–99,9%; throughput hingga 850 req/s). Kontribusi penelitian ini meliputi: (1) kerangka "session cycle" yang menggabungkan konsep SSO dan SLO untuk konteks perguruan tinggi Indonesia, (2) rubrik evaluasi gabungan yang menilai aspek teknis, keamanan, usability, dan administrasi, serta (3) panduan implementasi praktis terkait pemilihan protokol, integrasi sistem lama, opsi kebijakan MFA, dan pola SLO beserta mekanisme pemulihan. Hasilnya dapat menjadi acuan bagi kampus lain yang menghadapi masalah autentikasi di banyak sistem.

Kata Kunci: autentikasi terintegrasi; Laravel; OpenID Connect; perguruan tinggi; SAML 2.0; Single Logout; Single Sign-On..

1 Pendahuluan

Transformasi digital di perguruan tinggi saat ini bukan lagi sekadar inovasi tambahan(Andi Kambau, 2024), tetapi sudah menjadi kebutuhan utama untuk menjalankan layanan kampus secara efektif. Kegiatan akademik dan administratif—seperti pengisian KRS, pengelolaan nilai, pembelajaran daring, pembayaran, hingga layanan perpustakaan—umumnya ditopang oleh berbagai sistem informasi(Zulfa, Ibrahim, & Arifudin, 2025). Semakin banyak sistem yang digunakan, semakin besar manfaatnya bagi kampus, karena layanan menjadi lebih cepat, mudah diakses, dan data lebih terstruktur (Qur'aini & Firdaus, 2024). Namun, pertumbuhan sistem yang cepat juga menimbulkan tantangan baru yang sering tidak direncanakan sejak awal, yaitu bagaimana identitas pengguna dan hak aksesnya dikelola secara konsisten di seluruh sistem(Setiawan, 2024).

Pada banyak perguruan tinggi di Indonesia, sistem informasi berkembang secara bertahap dan terpisah, sesuai kebutuhan pada masa tertentu. Akibatnya, setiap sistem sering memiliki basis data pengguna sendiri, halaman login sendiri, dan aturan pengelolaan sesi sendiri. Kondisi ini menyebabkan satu pengguna memiliki beberapa akun yang tidak saling terhubung di dalam institusi yang sama (Tarigan, Dwiatma, & Wibowo, 2021). Dalam kajian manajemen identitas digital, kondisi tersebut dikenal sebagai fragmentasi identitas, yaitu ketika identitas digital seseorang terpecah menjadi banyak akun di berbagai aplikasi. Masalah ini terlihat sederhana, tetapi dampaknya luas: pengguna harus mengingat banyak username dan password, sering terjadi kesalahan saat login, dan unit TI harus menangani lebih banyak permintaan bantuan terkait akses akun.

Permasalahan fragmentasi identitas ini terjadi secara nyata di Universitas Nurul Jadid (UNUJA), sebuah perguruan tinggi berbasis pesantren di Probolinggo, Jawa Timur, dengan lebih dari 3.000 mahasiswa aktif. UNUJA mengoperasikan empat sistem utama yang digunakan setiap hari oleh

civitas akademika, yaitu SIAKAD untuk layanan akademik, SIMKEU untuk layanan keuangan, E-Learning berbasis Moodle untuk pembelajaran daring, dan Sistem Manajemen Perpustakaan untuk layanan pustaka(Karyaningtiyas, Yamin, & Hermanto, 2022). Keempat sistem ini berkembang pada waktu dan teknologi yang berbeda, sehingga masing-masing berdiri sendiri dalam hal autentikasi(Arianto, Witanti, & Ashaury, 2025). Akibatnya, mahasiswa maupun dosen yang membutuhkan beberapa layanan dalam satu aktivitas harus melakukan login berulang pada sistem yang berbeda-beda, walaupun mereka masih berada dalam konteks layanan kampus yang sama.

Observasi awal pada pengguna representatif (Anjar Riana, Ismail, & Irawan, 2025) menunjukkan bahwa rata-rata waktu yang dibutuhkan untuk login dan mengakses keempat sistem mencapai 6,8 menit per sesi, termasuk waktu berpindah halaman, memasukkan kredensial, menangani kesalahan, dan menunggu proses verifikasi. Tingkat kesalahan login tercatat 14 persen, terutama karena pengguna tertukar memasukkan username atau password antar sistem (Nugroho et al., 2023). Jika kondisi ini terjadi berulang setiap hari pada ribuan mahasiswa dan dosen, maka akumulasi waktu yang terbuang menjadi sangat besar, dan pada akhirnya mengurangi produktivitas serta menurunkan kepuasan pengguna terhadap layanan digital kampus.

Dari sisi keamanan, fragmentasi akun juga menciptakan risiko yang lebih serius. Survei internal menunjukkan bahwa banyak pengguna cenderung menggunakan password yang sama atau sangat mirip di beberapa sistem(Pardosi & S.Kom., M.Sc., Bernadete Deta, M.Kom., Fifto Nugroho, 2024). Praktik ini meningkatkan risiko karena jika salah satu sistem mengalami kebocoran, kredensial yang sama dapat dicoba untuk mengakses sistem lain(Novianto, Heri Ujianto, & Rianto, 2023). Risiko lain yang sangat nyata di lingkungan kampus adalah sesi yang tidak berakhir dengan benar. Saat pengguna logout dari satu sistem, sesi pada sistem lain masih tetap aktif karena tidak ada mekanisme logout yang terkoordinasi(Leasa & Prassida, 2024). Pada perangkat bersama seperti komputer laboratorium atau komputer perpustakaan, hal ini berbahaya karena pengguna berikutnya dapat mengakses akun yang masih terbuka. Data internal UNUJA mencatat adanya laporan akun diakses tanpa izin dalam periode tertentu, dan sebagian besar kasus berkaitan dengan sesi yang tidak ditutup secara sempurna.

Dari sisi administrasi, dampaknya terasa pada beban kerja unit TI. Helpdesk menerima banyak tiket terkait autentikasi, seperti lupa password, akun terkunci, atau gagal login(Bagus Priyatna, Nurrohman, & Yuliana, 2023). Selain itu, proses pembuatan akun mahasiswa baru menjadi pekerjaan yang berat karena akun harus dibuat di beberapa sistem secara terpisah. Pada periode penerimaan mahasiswa baru dengan jumlah yang besar, pekerjaan ini menyita waktu staf IT dan meningkatkan kemungkinan terjadinya ketidakkonsistenan akun, misalnya akun aktif di satu sistem tetapi belum aktif di sistem lain(Putra & Hendrawan, 2024). Hal serupa juga terjadi pada proses penonaktifan akun ketika mahasiswa lulus atau tidak lagi aktif, yang berisiko meninggalkan akun terlantar (orphan account) dan menjadi celah keamanan(Sevara Humaira Putri & Fajar Nugraha, 2024).

Dalam solusi yang umum digunakan untuk mengatasi masalah tersebut adalah Single Sign-On (SSO). SSO memungkinkan pengguna cukup melakukan login satu kali untuk mengakses beberapa aplikasi yang terintegrasi(Saputri & Adytia, 2023). Agar keamanan lebih terjaga, SSO idealnya dilengkapi Single Logout (SLO), yaitu mekanisme logout yang mengakhiri sesi secara serentak pada semua aplikasi terkait. Tanpa SLO, pengguna bisa merasa sudah keluar, padahal sesi di layanan lain masih aktif. Pada implementasi modern, SSO sering menggunakan token berbasis JSON Web Token (JWT) karena formatnya ringkas dan mudah diverifikasi lintas sistem(Prasetyo & Nugraha, 2023). Namun, JWT bersifat stateless, sehingga token yang sudah diterbitkan dapat tetap berlaku sampai masa kadaluarsanya habis. Karena itu, diperlukan mekanisme tambahan seperti pencabutan token (revocation), misalnya melalui daftar blokir (blacklist), agar logout dan perubahan status akses dapat benar-benar ditegakkan(Darmawan, Umar Mansyur, Zulfana Imam, Moh. Syahdan, & Fawaid, 2023).

Walaupun SSO telah banyak diterapkan, masih terdapat beberapa gap yang relevan dengan konteks kampus seperti UNUJA. Banyak implementasi dan penelitian lebih menekankan keberhasilan SSO pada tahap login, tetapi kurang memberi perhatian besar pada SLO, padahal risiko sesi yang tertinggal aktif sangat tinggi pada perangkat bersama. Selain itu, dokumentasi mengenai tantangan integrasi sistem lama (legacy) dengan arsitektur SSO modern masih terbatas, sementara ini adalah kondisi umum di perguruan tinggi yang sistemnya berkembang bertahap. Evaluasi implementasi SSO juga sering parsial, misalnya hanya menilai aspek teknis atau

hanya menilai kepuasan pengguna, sehingga diperlukan evaluasi yang lebih menyeluruh yang mencakup aspek kinerja, keamanan, pengalaman pengguna, dan efisiensi administratif.

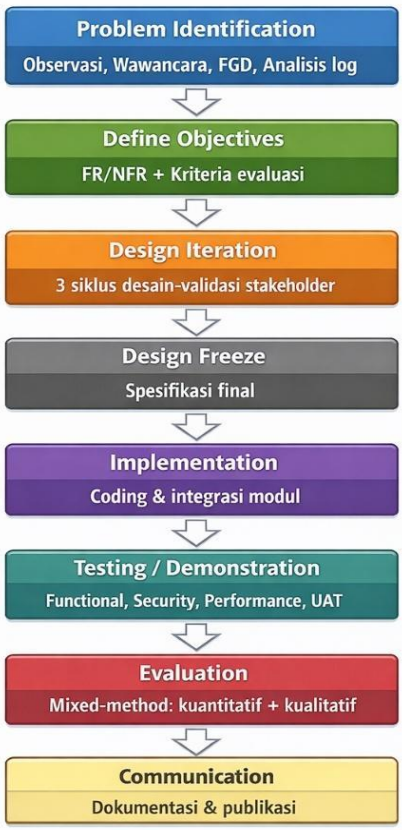
Berdasarkan kondisi tersebut, penelitian ini bertujuan merancang, mengimplementasikan, dan mengevaluasi solusi SSO dan SLO terintegrasi di Universitas Nurul Jadid dengan menggunakan JWT sebagai mekanisme autentikasi utama, serta mendukung pencabutan token melalui mekanisme blacklist agar logout dan perubahan akses dapat berjalan konsisten. Implementasi difokuskan pada integrasi dengan empat sistem utama, yaitu SIAKAD, SIMKEU, E-Learning Moodle, dan Sistem Perpustakaan. Evaluasi dilakukan dari beberapa sisi, yaitu kinerja teknis, keamanan sesi dan audit, pengalaman pengguna, serta dampak administratif seperti penurunan tiket helpdesk dan percepatan pembuatan maupun penonaktifan akun. Dengan demikian, penelitian ini diharapkan tidak hanya menghasilkan solusi yang berjalan secara teknis, tetapi juga memberikan manfaat nyata berupa akses yang lebih mudah, layanan yang lebih aman, dan pengelolaan identitas yang lebih efisien bagi seluruh civitas akademika UNUJA.

2 Metode

Penelitian ini merupakan penelitian pengembangan sistem informasi (IT artifact) yang berfokus pada perancangan, implementasi, dan evaluasi Single Sign-On (SSO) dan Single Logout (SLO) pada ekosistem sistem informasi Universitas Nurul Jadid. Metodologi pengembangan yang digunakan adalah model Waterfall karena setelah fase analisis dan desain, kebutuhan sistem relatif stabil dan perlu diturunkan ke proses implementasi yang terdokumentasi dengan baik, mudah ditelusuri (traceable) dari kebutuhan hingga pengujian, serta sesuai untuk sistem yang bersifat security-critical(Nur Adiya, Anggraeni, & Ilham Albana, 2024).

Model Waterfall pada penelitian ini mencakup lima tahapan utama yang dijalankan secara runtut(Rahayu, Saputra, & Irawan, 2024). Tahap pertama adalah requirements analysis, yang mencakup studi literatur, observasi lapangan, wawancara stakeholder, Focus Group Discussion (FGD), serta triangulasi dengan analisis log historis untuk merumuskan problem statement dan kebutuhan pengguna. Tahap kedua adalah system design, yang menerjemahkan kebutuhan ke rancangan arsitektur dan spesifikasi desain melalui arsitektur modular dan pemodelan UML (Wayahdi & Ruziq, 2023). Tahap ketiga adalah implementation (pemrograman), yaitu pembangunan prototipe menggunakan Laravel, serta integrasi MySQL dan Redis untuk kebutuhan penyimpanan data, sesi, dan blacklist token(Nur Ramadhan & Saraswati, 2023). Tahap keempat adalah testing, meliputi pengujian fungsional, keamanan, performa, dan user acceptance pada lingkungan staging. Tahap kelima adalah maintenance, yang mencakup monitoring dan review menggunakan Laravel Telescope dan Redis Monitor untuk memastikan sistem berjalan stabil serta mendukung perbaikan berbasis temuan operasional.

Untuk membantu replikasi prosedur, alur kerja penelitian berikut menggambarkan tahapan Waterfall secara runtut.



Gambar 1. Research and development

Berikut mempertahankan pemetaan fase, aktivitas, output, dan durasi penelitian sebagaimana rancangan penelitian ini. Akan disajikan pada tabel 1, yang menggambarkan Pemetaan Fase Waterfall dan Aktivitas Penelitian secara rinci. Tabel ini akan memaparkan setiap fase dalam metode Waterfall yang diterapkan, beserta aktivitas yang dilakukan pada setiap tahap, output yang dihasilkan, dan estimasi durasi waktu yang dibutuhkan untuk masing-masing aktivitas tersebut. Penyajian informasi dalam tabel ini diharapkan dapat memberikan gambaran

yang jelas dan terstruktur mengenai alur penelitian yang akan dilakukan.

Tabel 1. Pemetaan Fase Waterfall dan Aktivitas Penelitian

No	Waterfall	Aktivitas Utama	Output
1	Requirements Analysis	Observasi, wawancara, FGD, analisis log historis	Problem statement, stakeholder needs
2	System Design	Definisi FR/NFR, arsitektur, UML modeling	SRS document, design specification
3	Implementation	Coding Laravel, integrasi Redis/MySQL	Source code, API documentation
4	Testing	Functional, security, performance testing	Test reports, bug fixes
5	Maintenance	Survei kepuasan, analisis matrik, monitoring/review	Evaluation report, monitoring log

Pada fase implementasi teknis (Implementation), prototipe dibangun dengan pendekatan web application dan komponen penyimpanan sesi/blacklist token sesuai rancangan sistem. Implementasi dilakukan menggunakan framework Laravel, serta integrasi penyimpanan data menggunakan MySQL dan penyimpanan cepat untuk kebutuhan session/blacklist menggunakan Redis. Integrasi juga mencakup dukungan terhadap platform E-Learning berbasis Moodle sebagai salah satu service provider dalam skenario SSO/SLO. Pemilihan komponen ini tidak mengubah rancangan metodologi, tetapi dicantumkan untuk memenuhi ketentuan replikasi serta penelusuran sumber komersial.

Pengumpulan data dilakukan melalui tiga teknik utama, yaitu observasi terstruktur, wawancara terstruktur (semi-structured), dan Focus Group Discussion (FGD), serta dilengkapi triangulasi dengan analisis log sistem historis. Observasi dilakukan terhadap 20 pengguna yang dipilih secara purposive untuk mewakili variasi profil pengguna: mahasiswa semester awal (4 orang), mahasiswa semester akhir (4 orang), dosen tetap (4 orang), dosen luar biasa (2 orang), staf akademik (3 orang), dan staf TI (3 orang). Observasi berlangsung selama 2 hari kerja, dengan cakupan waktu Hari 1 pada jam sibuk 08:00–11:00 dan jam normal 13:00–15:00, serta Hari 2 pada jam normal 09:00–12:00 dan sore 14:00–16:00. Observasi mencatat berbagai skenario penggunaan, meliputi login rutin, login setelah lama tidak mengakses, login bersamaan ke multiple sistem, pemulihan dari error, dan perilaku logout. Untuk memperkaya pemahaman terhadap pain points yang tidak selalu terlihat dari perilaku, sebagian sesi menerapkan think-aloud protocol, yaitu pengguna memverbalisasi apa yang mereka pikirkan saat melakukan login dan logout. Keterbatasan durasi observasi 2 hari dimitigasi melalui triangulasi dengan analisis log historis 6 bulan untuk memastikan pola yang teramati konsisten secara longitudinal; peneliti juga secara eksplisit mencatat bahwa observasi ini belum menangkap variasi musiman (misalnya periode UTS/UAS atau registrasi), dan merekomendasikan studi longitudinal sebagai penelitian lanjutan.

Wawancara dilakukan kepada 15 key stakeholders menggunakan protokol semi-structured agar tetap terarah namun memungkinkan eksplorasi tema yang muncul di lapangan. Kriteria inklusi responden mencakup pengalaman aktif menggunakan minimal 2 dari 4 sistem kampus dan telah menggunakan sistem minimal 6 bulan serta bersedia berpartisipasi dengan informed consent. Kriteria eksklusi meliputi pengguna yang baru bergabung (<6 bulan), pengguna yang hanya mengakses satu sistem, serta individu yang terlibat langsung dalam pengembangan sistem SSO untuk menghindari bias. Durasi wawancara berkisar 45–60 min, dilakukan tatap muka, direkam, dan di transkrip verbatim untuk analisis. Distribusi responden wawancara dipertahankan sebagaimana berikut:

Tabel 2. Distribusi Responden Wawancara

Kategori	Peran Spesifik	Alasan Pemilihan
Administrator TI	System Admin (2), Security Officer (1)	Perspektif teknis dan operasional
Manajemen Akademik	Wakil Dekan (1), Kepala Program Studi (1)	Perspektif governance dan kebijakan

Dosen	Dosen tetap dari 3 fakultas berbeda	Perspektif pengguna akademik
Staf Administratif	Keuangan (2), Akademi (1), Perpustakaan (1)	Perspektif pengguna administratif
Mahasiswa	S1 (2), Pascasarjana (1)	Perspektif pengguna utama

FGD dilaksanakan sebanyak tiga sesi dengan pengelompokan homogen untuk mendorong diskusi yang lebih terbuka dan relevan sesuai peran. FGD 1 melibatkan mahasiswa (n=10) dan berfokus pada pengalaman daily use, frustration points, serta ekspektasi terhadap kemudahan akses. FGD 2 melibatkan dosen (n=8) dengan fokus integrasi workflow akademik, concern keamanan data penelitian, dan harapan reliability. FGD 3 melibatkan tenaga kependidikan (n=7) dengan fokus efisiensi kerja administratif, penanganan masalah pengguna, dan kebutuhan audit trail. Setiap sesi FGD berdurasi 90–120 min, difasilitasi oleh peneliti dengan asisten notetaker, dan direkam untuk analisis tematik.

Data yang dikumpulkan terdiri dari data kualitatif dan kuantitatif. Data kualitatif berasal dari catatan observasi, transkrip wawancara, dan transkrip FGD. Data kuantitatif berasal dari log sistem (baseline historis 6 bulan), hasil pengujian prototipe (functional, security, performance), serta survei kepuasan pengguna. Analisis data kualitatif dilakukan dengan thematic analysis menggunakan pendekatan hybrid deduktif–induktif; tema deduktif diturunkan dari kerangka kualitas perangkat lunak ISO/IEC 25010, sedangkan tema induktif dibiarkan muncul dari data lapangan. Data kuantitatif dianalisis menggunakan statistik deskriptif dan perbandingan pre–post implementation untuk melihat perubahan sebelum dan sesudah penerapan SSO/SLO pada indikator yang diukur (misalnya metrik log, survei, dan hasil pengujian).

3 Hasil dan Diskusi

a) Analisis

Tahap analisis menunjukkan masalah utama autentikasi di ekosistem UNUJA (SIAKAD, SIMKEU, E-Learning, Library) adalah fragmentasi identitas dan autentikasi berulang yang berdampak pada efisiensi, keamanan, dan beban administrasi. Temuan dari observasi, wawancara, dan FGD saling menguatkan, lalu disintesis menjadi kebutuhan fungsional (FR) dan non-fungsional (NFR) yang terukur.

1) Temuan Kunci per Sumber Data

A. Observasi

Indikasi kuantitatif:

- Rata-rata waktu login ke 4 sistem: 6,8 menit (min 4,2; max 12,5).
- Error login per sesi: 0,9 dengan tingkat kesalahan 14%.
- Waktu pemulihan error: rata-rata 45 detik (hingga 180 detik).

Indikasi kualitatif yang dominan:

- Credential confusion: 40% pengguna salah kredensial (umum saat pindah SIAKAD → E-Learning).
- Tab accumulation: 75% membuka tab terpisah persistem → "menjaga banyak sesi" karena tidak ada koordinasi sesi.
- Incomplete logout: 60% menutup browser tanpa logout eksplisit → risiko sesi tertinggal (krusial di perangkat bersama).
- Frustration indicators: 70% sesi dengan error memunculkan frustasi.

Makna: masalah bukan hanya "lupa password", tapi pola penggunaan menunjukkan kebutuhan SSO + manajemen sesi terpusat + single logout.

B. Wawancara

Muncul 5 tema utama:

1. Fragmentasi pengalaman: semua responden merasa tidak nyaman karena banyak kredensial; keluhan login sering karena password tertukar antar sistem.
2. Trade-off keamanan vs kenyamanan: pengguna paham risikonya, tetapi mengulang password dianggap paling praktis.
3. Risiko perangkat bersama: sesi tertinggal aktif dipandang berbahaya (terutama layanan publik seperti perpustakaan).
4. Beban administratif: pembuatan akun lintas 4 sistem saat PMB membebani TI/akademik.
5. Ekspektasi solusi: dukungan kuat terhadap satu akun untuk semua

sistem; 87% menyatakan dukungan eksplisit untuk SSO.

Makna: kebutuhan SSO bukan sekadar fitur, tapi solusi untuk pain point operasional dan risiko keamanan nyata.

C. FGD(Mahasiswa, Dosen Dan Tendik)

- Mahasiswa: dominan "lupa password/salah sistem", butuh akses mobile lebih mudah; khawatir single point of compromise jika satu password bocor.
- Dosen: menuntut reliabilitas tinggi (terutama masa deadline), serta notifikasi proaktif bila ada isu keamanan.
- Tendik: menekankan audit trail & akuntabilitas ("siapa melakukan apa kapan") untuk compliance.

Makna: selain SSO, perlu kontrol keamanan (MFA opsional, lockout), monitoring, audit log, dan kebijakan sesi yang jelas.

2) Sintesis Masalah Inti

Dari triangulasi data, masalah inti dapat diringkas menjadi:

- Inefisiensi akses akibat login berulang lintas aplikasi.
- Kesalahan autentikasi tinggi karena multi-kredensial → menurunkan produktivitas dan meningkatkan frustasi.
- Risiko keamanan dari reuse password + sesi tidak tertutup di perangkat bersama.
- Beban administrasi pembuatan dan pengelolaan akun lintas sistem.
- Kebutuhan tata kelola: audit trail, monitoring, dan konfigurasi sesi untuk compliance & operasional.

3) Sintesis Kebutuhan Sistem

A. Functional Requirements (FR)

Kelompok kebutuhan fungsional yang paling "mengikat" dari temuan adalah:

1. **Autentikasi terstandar**
   Login username/email dan password (must). Lockout setelah 5 kali gagal (must). MFA opsional (should) untuk menjawab kekhawatiran keamanan "satu akun untuk semua".
2. **Single Sign-On (SSO) sebagai core**
   Akses aplikasi lain tanpa login ulang (must). Session timeout terkonfigurasi (must). Redirect mulus antar aplikasi (should).
3. **Single Logout (SLO)**
   Logout dari satu aplikasi memutus sesi semua aplikasi (must). Konfirmasi logout jelas (must). Penanganan kegagalan propagasi logout secara graceful (should).
4. **Manajemen pengguna & akses**
   Admin CRUD user (must). RBAC (must). Self-service reset password (should) untuk menurunkan error & beban helpdesk.
5. **Integrasi sistem**
   REST API integrasi (must). Kompatibel dengan sistem legacy (must).
6. **Administrasi, monitoring, dan audit**
   Dashboard monitoring (must). Audit log semua aktivitas autentikasi (must).

Benang merah FR: desain harus mengutamakan SSO + kontrol sesi + auditability, bukan hanya "login satu pintu".

B. Non Functional Requirements (NFR)

NFR disusun terukur (mengacu ISO/IEC 25010) dan menegaskan kualitas layanan:

- **Performance**: latency autentikasi ≤ 2 detik; ≥ 1000 concurrent users; throughput ≥ 500 req/sec.
- **Reliability**: uptime ≥ 99,5%; MTTR ≤ 30 menit.
- **Security**: path OWASP Top 10; TLS ≥ 1.2; password hashing **bcrypt** cost ≥ 10; token RS256/HS256.
- **Usability**: SUS ≥ 75; kejelasan pesan error ≥ 80% dipahami.
- **Maintainability**: coverage ≥ 70%; dokumentasi lengkap.
- **Scalability**: mendukung horizontal scaling.

Makna NFR: solusi SSO harus tetap cepat, stabil, aman, mudah dipakai, dan siap skala untuk beban kampus.

Hasil analisis menunjukkan autentikasi di empat sistem UNUJA memunculkan biaya waktu (rata-rata 6,8 menit untuk login ke semua sistem), kesalahan login (14%), serta risiko keamanan (logout tidak tuntas pada 60% pengguna) dan beban operasional. Wawancara dan FGD menguatkan kebutuhan SSO dengan kontrol keamanan (lockout, MFA opsional), manajemen sesi (timeout, single logout), integrasi sistem legacy via API, serta penguatan tata kelola melalui monitoring dan audit log. Semua itu dipagari target mutu NFR yang terukur pada aspek performa, reliabilitas, keamanan, usability, maintainability, dan scalability.

b) Perancangan

1) **Formulasi Arsitektur Sistem**

Berdasarkan hasil analisis kebutuhan, sistem autentikasi terpusat dirancang dengan pendekatan modular dan terintegrasi, menggunakan Laravel 12 sebagai *Identity Provider (IdP)* utama yang mengelola autentikasi, otorisasi, dan propagasi sesi ke berbagai *Service Provider (SP)* kampus seperti SIAKAD, SIMKEU, E-Learning, dan Library System. Arsitektur ini mengadopsi prinsip federated identity management dengan dukungan protokol OIDC untuk aplikasi modern dan SAML 2.0 untuk aplikasi legacy.

Secara garis besar, arsitektur terdiri dari empat komponen utama:

a. **Identity Provider (IdP)**
menangani login, otorisasi token, manajemen sesi, dan Single Logout (SLO).

b. **Service Provider (SP)**
aplikasi kampus yang berintegrasi melalui API atau SSO middleware.

c. **Redis Cache Layer**
menyimpan *blacklist token* dan *session data* untuk efisiensi logout dan validasi cepat.

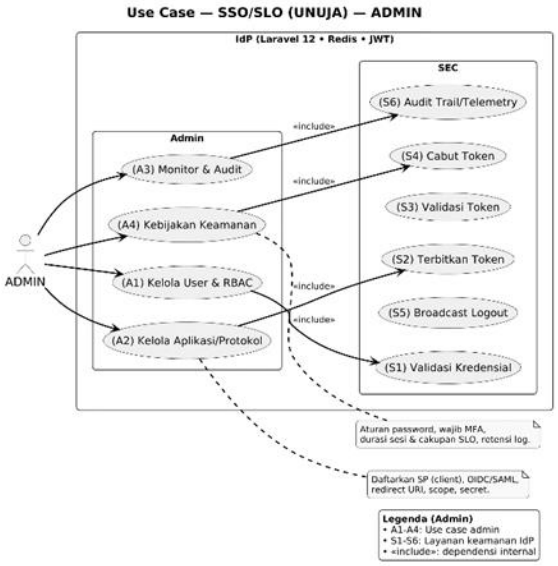
d. **Database MySQL**
menyimpan data pengguna, role, aplikasi, token, log autentikasi, dan konfigurasi keamanan.

2) **Pemodelan UML**

Untuk memastikan keterlacakan kebutuhan terhadap rancangan teknis, digunakan beberapa diagram UML berikut:

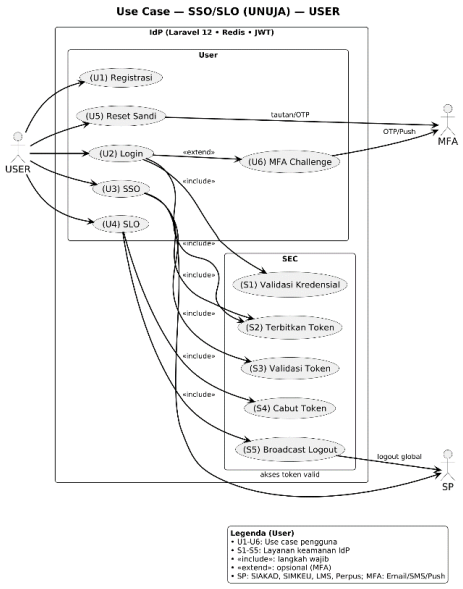
a. Use Case Diagram

Admin: mengelola aplikasi terintegrasi, pengguna, dan monitoring log.



Gambar 1. Use Case Diagram Admin

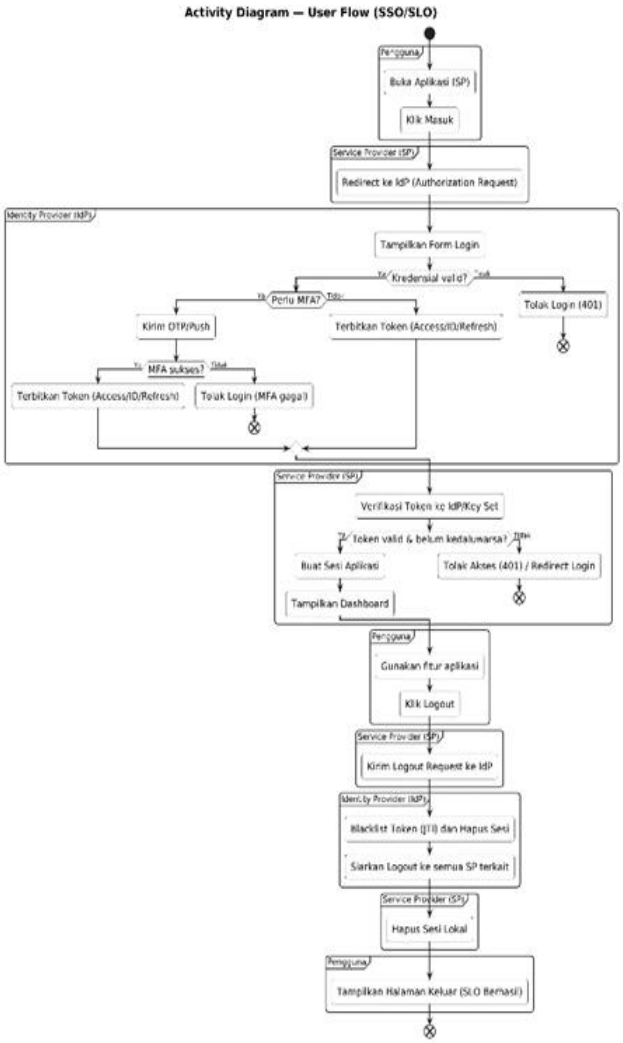
User: login, mengakses sistem melalui SSO, dan logout secara serentak (SLO).



Gambar 2. Use Case Diagram *User*

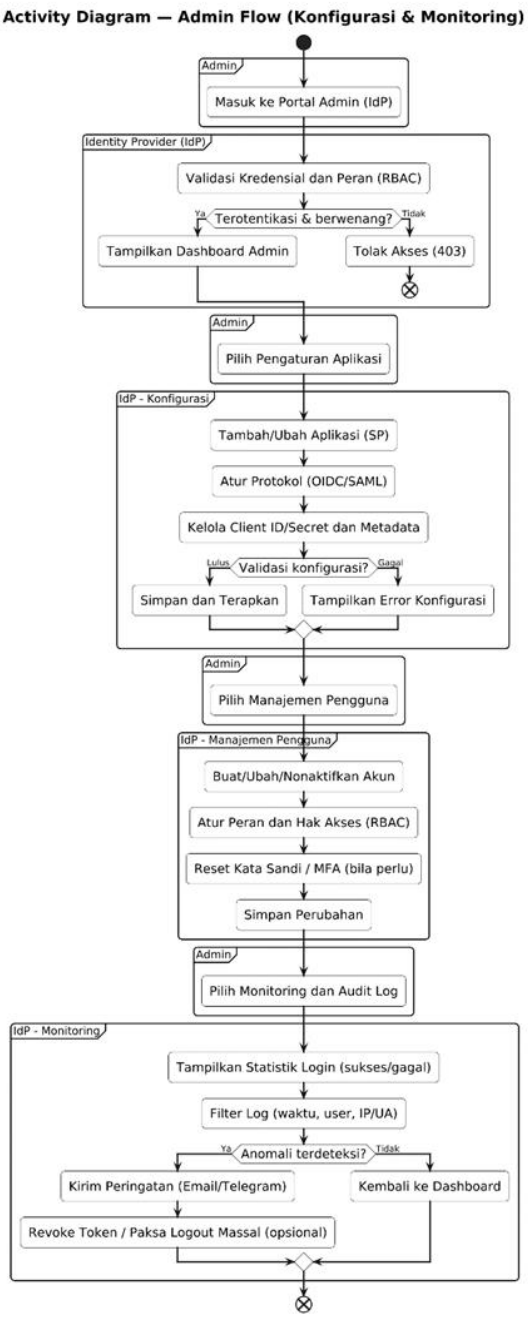
b. Activity Diagram

User Flow: proses login → autentikasi via IdP → menerima token → akses aplikasi → logout global.



Gambar 3. Activity Diagram *User*

Admin Flow: pengaturan aplikasi dan protokol → manajemen user → pemantauan log aktivitas.

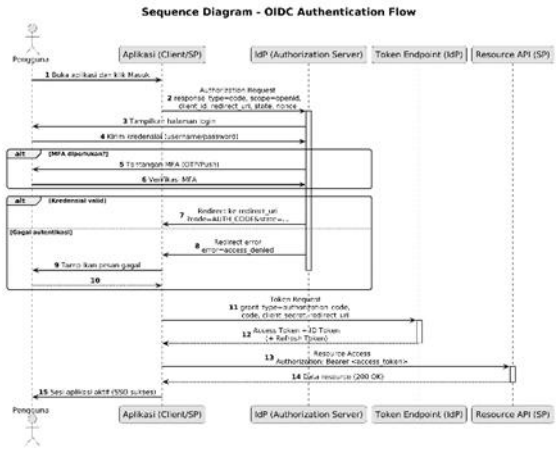


Gambar 4. Activity Diagram *Admin*

c. Sequence Diagram

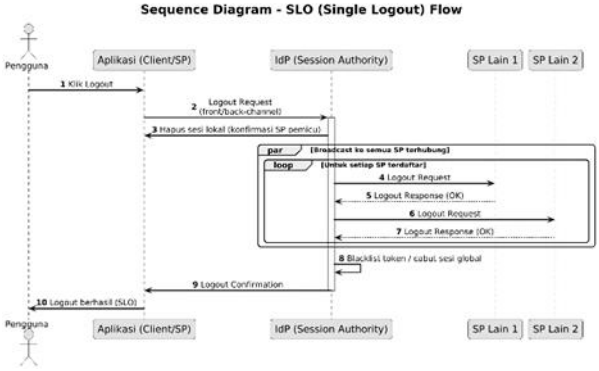
- *Authentication Flow (OIDC)*

  User → Authorization Request → IdP → Authentication → Authorization Code → Token Request → Access Token + ID Token → Resource Access.



Gambar 5. Sequence Diagram *Authentication Flow*

Logout Flow (SLO): User → Logout Request (SP) → IdP → Broadcast ke semua SP → Hapus sesi → Logout Confirmation.

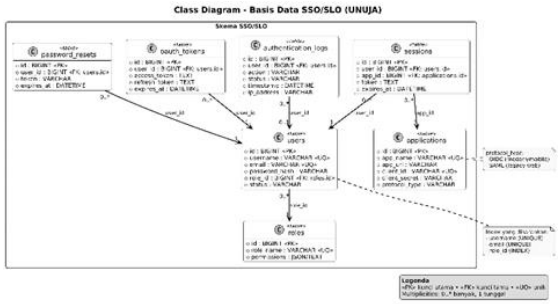


Gambar 6. Sequence Diagram *Logout Flow*

d. Class Diagram

Struktur basis data utama meliputi:

- users(id, username, email, password_hash, role_id, status)
- roles(id, role_name, permissions)
- applications(id, app_name, app_url, client_id, client_secret, protocol_type)
- sessions(id, user_id, app_id, token, expires_at)
- authentication_logs(id, user_id, action, status, timestamp, ip_address)
- oauth_tokens(id, user_id, access_token, refresh_token, expires_at)
- password_resets(id, user_id, token, expires_at)



Gambar 7. Sequence Diagram *Logout Flow*

Relasi antar tabel dirancang *one-to-many* dengan *foreign key constraint* untuk menjamin integritas data, sedangkan audit aktivitas tercatat secara otomatis dalam tabel authentication logs

3) **Evaluasi Desain Sistem**

Desain sistem dievaluasi melalui review sesi internal yang melibatkan tim pengembang dan perwakilan stakeholder. Hasil evaluasi menunjukkan tiga perbaikan utama:

- Penambahan Multi-Factor Authentication (MFA) untuk meningkatkan keamanan login.
- Penyesuaian *schema database* agar kompatibel dengan protokol SAML dan OIDC secara bersamaan.
- Optimalisasi session management dengan Redis untuk mempercepat proses verifikasi token dan logout massal.

Optimalisasi session management dengan Redis untuk mempercepat proses verifikasi token dan logout massal

4) **Detail Desain Teknis**

a. Alur Autentikasi SSO (OIDC)

- Pengguna mengakses aplikasi → diarahkan ke IdP → login → verifikasi kredensial.
- IdP menghasilkan *access token* dan *ID token (JWT)*.
- Token diserahkan ke SP → SP memverifikasi token → mengizinkan akses.

b. Mekanisme Single Logout (SLO)

- Saat pengguna logout dari satu aplikasi, SP mengirimkan *logout request* ke IdP.

- IdP menandai token terkait di Redis sebagai *blacklisted*.
- IdP meneruskan *logout request* ke semua SP lain → seluruh sesi pengguna dihapus.

c. Keamanan Sistem

- Semua komunikasi terenkripsi dengan TLS 1.3.
- Token menggunakan JWT dengan tanda tangan digital (RS256).
- Password disimpan menggunakan bcrypt hashing.
- Mekanisme *brute-force protection* membatasi login gagal maksimal 5 kali.

d. Manajemen Admin

- Panel admin berbasis Laravel Blade: memantau pengguna aktif, log autentikasi, dan performa token.
- Sistem *role-based access control (RBAC)* memastikan hanya admin berhak mengakses konfigurasi IdP dan SP.

5) **Ringkasan**

Rancangan sistem ini menegaskan bahwa desain SSO/SLO berbasis Laravel 12 + Redis + JWT mampu menjawab kebutuhan efisiensi autentikasi dan keamanan pengguna di lingkungan multi-aplikasi Universitas Nurul Jadid. Arsitektur modular, dukungan multi-protokol (SAML & OIDC), serta penerapan praktik keamanan modern menjadikannya siap untuk tahap pengkodean dan implementasi.

c) Pemrograman

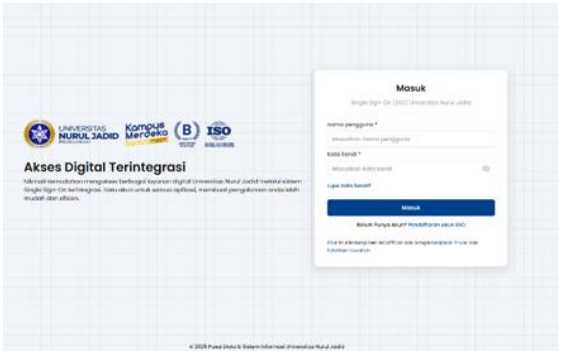
1) **Environment**

- **Framework:** Laravel 12.x
- **Package:**
  tymon/jwt-auth — digunakan untuk autentikasi berbasis JWT (JSON Web Token)
  Laravel/telescope — digunakan untuk debugging dan monitoring aplikasi
- **Web Server / Runtime:** Nginx + PHP-FPM
- **Basis Data:** MySQL 8.4
- **Cache / Queue:** Redis 7
- **Sistem Operasi Server:** Ubuntu 22.04 LTS

2) **Halaman User**

Halaman ini merupakan titik masuk utama (login interface) bagi seluruh pengguna sistem SSO Universitas Nurul Jadid.
Fungsi utamanya adalah melakukan autentikasi tunggal dengan kredensial kampus.
Elemen utama halaman:

- Form login dengan input *username* dan *password*.
- Validasi sisi server menggunakan AuthController::login().
- Notifikasi jika kredensial salah atau akun tidak aktif.
- Setelah sukses login, sistem membuat JWT access token dan refresh token yang tersimpan sementara di sesi browser.
- Redirect otomatis ke halaman Menu User atau aplikasi tujuan (jika ada parameter redirect_uri).



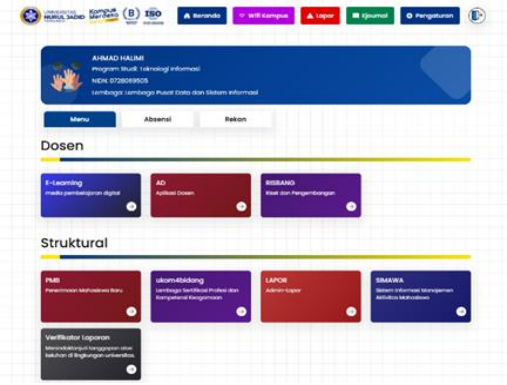
Gambar 8. Halaman User

3) **Halaman Menu User**

Halaman ini menampilkan daftar aplikasi terintegrasi dengan sistem SSO. Berfungsi sebagai *hub dashboard* bagi pengguna yang telah login.
Fitur dan elemen utama:

- Menampilkan nama pengguna dan peran (role).
- Tabel atau kartu daftar aplikasi (SIAKAD, SIMKEU, E-Learning, Perpustakaan, dan lainnya).
- Tombol *Open App* yang melakukan redirect ke aplikasi tujuan dengan membawa authorization code / token sesuai protokol SSO.

- Tombol *Logout* untuk keluar dari seluruh aplikasi terhubung (implementasi SLO).

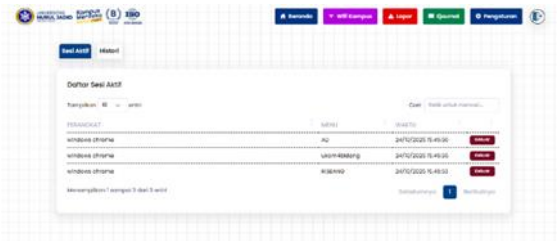


Gambar 9. Halaman Menu User

4) **Halaman Session Manager User**

Halaman ini digunakan untuk melihat dan mengelola sesi login aktif pengguna. Fungsi utama:

- Menampilkan daftar perangkat dan lokasi login (IP, waktu login, status token).
- Memberikan opsi "Logout dari perangkat ini" atau "Logout semua perangkat".
- Data ditarik dari tabel sessions dan oauth_tokens di basis data.
- Setiap logout akan memanggil endpoint /api/auth/logout atau /api/auth/logout-all untuk mencabut token terkait di Redis blacklist. Halaman ini membantu pengguna memahami aktivitas login dan meningkatkan keamanan akun.



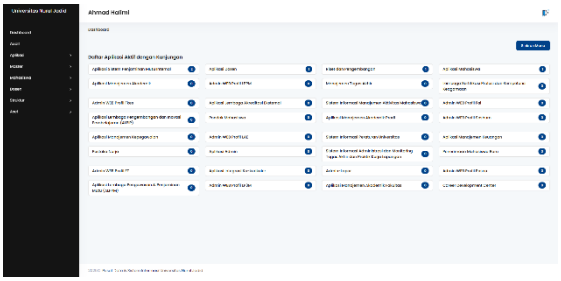
Gambar 10. Session Manager User

5) **Halaman Admin**

Halaman ini hanya dapat diakses oleh pengguna dengan peran Administrator. Berfungsi sebagai panel kontrol utama untuk pengelolaan identitas dan integrasi aplikasi.

Menu dan fungsi utama:

- Manajemen Pengguna: tambah, ubah, hapus akun; reset password; ubah peran (role).
- Manajemen Aplikasi: registrasi aplikasi baru (nama, URL callback, client ID, client secret).

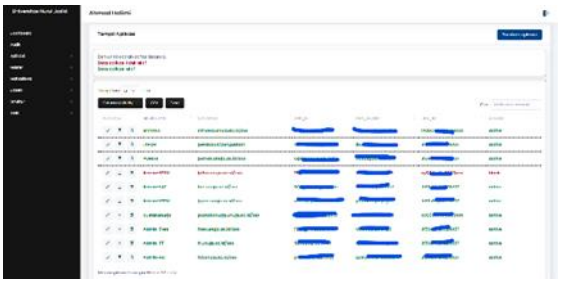


Gambar 11. Halaman Admin

6) **Halaman Setting Aplikasi**

Halaman ini menyediakan konfigurasi global sistem IdP (Identity Provider) dan parameter integrasi aplikasi.
Elemen utama:

- Pengaturan protokol SAML / OIDC, termasuk URL issuer, endpoint authorize/token, serta *public key certificate*.
- Konfigurasi JWT Secret Key, masa berlaku token (TTL), dan algoritma enkripsi (RS256).



Gambar 12. Halaman Seting Aplikasi

d) Pengujian

Pengujian bertujuan memastikan sistem memenuhi FR/NFR, aman, dan stabil dalam kondisi realistis maupun ekstrem. Pengujian terdiri dari: fungsional, keamanan, performa.

1) Pengujian Fungsional

Table 3. Pengujian Fungsional

TC-ID	Pengujian (ringkas)	Status

TC-A01	Login valid (JWT returned, redirect dashboard)	✓ PASS
TC-A02	Login password salah (Invalid credentials, no token)	✓ PASS
TC-A03	Login username tidak ada (Invalid credentials)	✓ PASS
TC-A04	Brute-force protection (5x gagal → lockout 15 menit, HTTP 429)	✓ PASS
TC-A05	Login setelah lockout habis (login berhasil)	✓ PASS
TC-S01	Akses API dengan token valid (/api/profile → 200 OK + user data)	✓ PASS
TC-S02	Akses API tanpa token (/api/profile → 401 Unauthorized)	✓ PASS
TC-S03	Akses API dengan token expired (401 Token Expired)	✓ PASS
TC-S04	Akses API dengan token malformed (401 Invalid Token)	✓ PASS
TC-S05	Seamless redirect SIAKAD → E-Learning (tanpa re-login)	✓ PASS
TC-S06	Token refresh (access expired + refresh valid → token baru terbit)	✓ PASS
TC-L01	Logout dari satu SP (token blacklisted; SP lain terminated)	✓ PASS
TC-L02	Akses setelah logout (token revoked → 401 Token Revoked)	✓ PASS
TC-L03	Logout all devices (semua sesi invalid via token version)	✓ PASS
TC-L04	SLO saat SP unavailable (back-channel queued retry)	✓ PASS

2) Pengujian Keamanan

Table 4. Pengujian Keamanan

No	Skenario Uji Keamanan (ringkas)	Status
1	Token integrity: payload diubah tanpa re-sign → token ditolak (401 invalid signature)	✓ SECURE
2	Token replay: pakai token yang sudah blacklisted → ditolak (401 token revoked)	✓ SECURE
3	Brute force: >5 gagal login → akun terkunci 15 menit	✓ SECURE
4	SQL injection: ' OR 1=1 -- → query ter parameterisasi, tidak tembus	✓ SECURE
5	XSS: input berisi script → disanitasi/di-encode, tidak dieksekusi	✓ SECURE
6	CSRF: request tanpa token → request ditolak/blocked	✓ SECURE
7	Session fixation: reuse session ID setelah login → session baru, ID lama ditolak	✓ SECURE
8	TLS downgrade: akses HTTP ke endpoint HTTPS → dipaksa HTTPS/redirect	✓ SECURE
9	Sensitive data exposure: password muncul di response/log → tidak dikembalikan & tidak di log	✓ SECURE
10	IDOR: akses data user lain → dicegah oleh AuthZ (403), akses ditolak	✓ SECURE

3) Pengujian Performa

Table 5. Pengujian Performa

No	Skenario & Beban (ringkas)	Hasil Utama
1	Baseline (100 user)	Avg 1.2s; P95 1.8s; SR 99.9%; 450 req/s
2	Medium (300 user)	Avg 1.4s; P95 2.1s; SR 99.8%; 620 req/s
3	High (500 user)	Avg 1.8s; P95 2.5s; SR 99.5%; 780 req/s
4	Stress (1000 user)	Avg 2.1s; P95 3.2s; SR 98.7%; 850 req/s
5	Endurance 1 jam (200 user)	Avg 1.3s; P95 1.9s; SR 99.7%; 520 req/s

Berdasarkan seluruh rangkaian pengujian (fungsional, keamanan, performa, skenario ekstrim, serta rekap kegagalan), dapat disimpulkan bahwa sistem telah memenuhi kebutuhan FR/NFR, aman, dan stabil pada kondisi operasional normal hingga beban tinggi. Seluruh pengujian fungsional dinyatakan berhasil, yaitu Authentication 5/5 PASS, SSO 6/6 PASS, SLO 4/4

PASS, dan Admin Features 7/7 PASS, yang menunjukkan mekanisme inti—login, validasi token, seamless redirect, refresh token, single logout lintas SP, serta fungsi administrasi (CRUD user, reset password, monitoring dan ekspor log, terminasi sesi)—berjalan sesuai ekspektasi. Dari sisi keamanan, hasil pengujian mencapai 10/10 SECURE yang mencakup integritas token, pencegahan token replay, brute force protection (lockout), SQL injection, XSS, CSRF, session fixation, TLS downgrade, pencegahan paparan data sensitif, serta kontrol otorisasi (IDOR), sehingga kontrol keamanan utama terbukti efektif dan konsisten. Dari sisi performa, pada beban 100–500 concurrent users rata-rata latency berada pada 1,2–1,8 detik dengan P95 1,8–2,5 detik dan success rate ≥99.5%; sementara pada stress test 1000 users terjadi peningkatan latency (avg 2,1 detik; P95 3,2 detik) dan penurunan success rate menjadi 98.7%, namun sistem tetap mampu melayani trafik dengan throughput tertinggi 850 req/s, sehingga degradasi pada kondisi stres masih terkendali dan dapat diterima.

e) Pemeliharaan

Pemantauan kinerja, keamanan, dan kesehatan layanan dilakukan berkala (request/exception, kueri lambat, Redis, dan log autentikasi) untuk menjaga stabilitas serta efektivitas. Pembaruan fitur diprioritaskan berdasarkan masukan pengguna dan temuan monitoring, sehingga sistem adaptif terhadap kebutuhan dan ekspektasi.

Rutinitas perawatan meliputi pencadangan basis data harian, uji pemulihan bulanan, pembaruan dependensi terjadwal, serta rotasi kunci JWT triwulanan. Tinjauan akses/role dan simulasi pemulihan bencana dilakukan berkala guna memastikan kesiapan operasional. Prosedur rilis mengikuti praktik aman (blue-green/canary) dengan migrasi dua fase dan rencana rollback jelas, sehingga perubahan dapat diterapkan tanpa mengganggu layanan pengguna

4 Kesimpulan

Penelitian ini berhasil merancang, mengimplementasikan, dan mengevaluasi sistem SSO/SLO terintegrasi di Universitas Nurul Jadid (UNUJA) dengan Laravel 12 sebagai Identity Provider (IdP), mendukung OpenID Connect untuk aplikasi modern dan SAML 2.0 untuk sistem legacy, sehingga mengatasi fragmentasi identitas yang sebelumnya menyebabkan login berulang, error autentikasi, risiko sesi tertinggal, serta beban administrasi akun lintas sistem. Pengujian menunjukkan FR/NFR terpenuhi dengan latensi autentikasi ≤2 detik pada beban 100–500 pengguna simultan dan success rate ≥99,5% (pada stres 1000 pengguna mencapai 98,7%), serta meningkatkan efisiensi karena akses multi-aplikasi yang semula rata-rata 6,8 menit menjadi jauh lebih singkat berkat sekali login untuk berpindah sistem tanpa re-login. Keamanan diperkuat melalui JWT RS256, TLS 1.3, bcrypt hashing, brute-force protection (lockout setelah 5 kali gagal), dan pencabutan token via Redis blacklist yang membuat SLO efektif mengakhiri sesi lintas aplikasi, termasuk saat salah satu service provider tidak tersedia melalui mekanisme back-channel/queue; secara operasional, sentralisasi dengan RBAC, audit log, dan monitoring mendukung tata kelola yang lebih baik, berpotensi menurunkan beban helpdesk, serta meningkatkan pengalaman pengguna. Penelitian lanjutan disarankan melakukan evaluasi pasca-implementasi di kondisi nyata (mis. PMB/UTS/UAS) lewat studi longitudinal untuk mengukur dampak produktivitas, keamanan, dan ROI, melakukan uji skala lebih besar (puluhan ribu pengguna simultan) untuk validasi skalabilitas horizontal, memperkuat fitur keamanan (MFA/adaptif berbasis risiko, deteksi anomali dari log, kebijakan sesi untuk perangkat bersama), serta memperkuat tata kelola melalui manajemen perubahan, pelatihan, peningkatan aksesibilitas (rujukan WCAG), dan kebijakan perlindungan data serta privasi yang konsisten dengan kebutuhan audit dan manajemen identitas kampus.

5 Referensi

Andi Kambau, R. (2024). Proses Transformasi Digital pada Perguruan Tinggi di Indonesia. *Jurnal Rekayasa Sistem Informasi Dan Teknologi*, *1*(3), 126–136. https://doi.org/10.59407/jrsit.v1i3.481

Anjar Riana, M., Ismail, I., & Irawan, D. (2025). Analisis Sistem Absensi Berbasis Web Untuk Peningkatan Efisiensi Operasional Di Pt Sumber Naungan Global (Sunago). *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(2), 3231–3236. https://doi.org/10.36040/jati.v9i2.13302

Arianto, I. G., Witanti, W., & Ashaury, H. (2025). Sistem Keamanan Otentikasi Pengguna Pada Modul Single Sign On Menggunakan OAuth 2.0 dan One Time Password. *Jurnal Ilmu Komputer Dan Teknologi*, *6*(1), 25–31. https://doi.org/10.35960/ikomti.v6i1.1768

Bagus Priyatna, D., Nurrohman, M. A., & Yuliana, M. E. (2023). Penanganan Keluhan Melalui Sistem Informasi Dan Komunikasi Helpdesk

Pt. Kinarya Tunas Artha Handling Complaints Through the Helpdesk Information and Communication System Pt. Kinarya Tunas Artha. *Sibatik Journal | Volume*, *2*(12), 3709–3720. Retrieved from https://publish.ojs-indonesia.com/index.php/SIBATIK

Darmawan, I., Umar Mansyur, M., Zulfana Imam, K., Moh. Syahdan, & Fawaid, A. (2023). Evaluasi Keamanan Privilege Terintegerasi JSON Web Token pada Sistem Informasi Akademik. *Jurnal Informasi Dan Teknologi*, *5*(2), 120–128. https://doi.org/10.37034/jidt.v5i2.368

Karyaningtiyas, D. P., Yamin, A., & Hermanto, K. (2022). Analisis Pengaruh Minat Pemanfaatan dan Penggunaan SIAKAD sebagai Media E-learning di Universitas Teknologi Sumbawa. *JIIP - Jurnal Ilmiah Ilmu Pendidikan*, *5*(8), 2921–2927. https://doi.org/10.54371/jiip.v5i8.783

Leasa, Z. V., & Prassida, G. F. (2024). Manajemen Risiko pada Sistem Informasi Akademik Universitas XYZ menggunakan ISO 27005:2018. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *6*(4), 649–656. https://doi.org/10.47233/jteksis.v6i4.1459

Novianto, E., Heri Ujianto, E. H., & Rianto, R. (2023). Keamanan Informasi (Information Security) Pada Aplikasi Sistem Informasi Manajemen Sumber Daya Manusia. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *8*(1), 10–15. https://doi.org/10.36341/rabit.v8i1.2966

Nugroho, T. A., Id Hadiana, A., Anggoro, S., Yani, A., Terusan, J., Sudirman, J., … Barat, I. (2023). Keamanan Berbasis Service Oriented Architecture Menggunakan Oauth 2.0 dan Json Web Token. *IJESPG Journal*, *1*(3), 229–236. Retrieved from http://ijespgjournal.org

Nur Adiya, A. Z. D., Anggraeni, D. L., & Ilham Albana. (2024). Analisa Perbandingan Penggunaan Metodologi Pengembangan Perangkat Lunak (Waterfall, Prototype, Iterative, Spiral, Rapid Application Development (RAD)). *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika*, *2*(4), 122–134. https://doi.org/10.61132/merkurius.v2i4.148

Nur Ramadhan, I., & Saraswati, G. (2023). Penerapan Database Redis Sebagai Optimalisasi Pemrosesan Kueri Data Pengguna Aplikasi SIRESMA Berbasis Laravel. *Technomedia Journal*, *8*(3), 64–77. https://doi.org/10.33050/tmj.v8i3.2152

Pardosi, V. B. A., & S.Kom., M.Sc., Bernadete Deta, M.Kom., Fifto Nugroho, A. Y. V. (2024). Sistem Keamanan Informasi. *Sustainability (Switzerland)*, *11*(1), 1–14. Retrieved from http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI

Prasetyo, H., & Nugraha, U. (2023). Optimasi Keamanan dalam Pengembangan Aplikasi Menggunakan Metode Agile Scrum dan JSON Web Token. *JUSTINFO | Jurnal Sistem Informasi Dan Teknologi Informasi*, *1*(1), 34–41. https://doi.org/10.33197/justinfo.vol1.iss1.2023.1228

Putra, I. P. A. S., & Hendrawan, I. K. R. (2024). Analisis Manajemen Risiko SIMRS pada Rumah Sakit Ganesha Menggunakan ISO 31000. *Jurnal Teknologi Dan Informasi*, *14*(1), 88–98. https://doi.org/10.34010/jati.v14i1.12329

Qur'aini, A., & Firdaus, R. (2024). Integrasi Teknologi Bagi Mahasiswa Dalam Sistem Informasi Manajemen Technology Integration For Students In Management Information Systems. *JICN: Jurnal Intelek Dan Cendikiawan Nusantara*, *1*(3), 4429–4436. Retrieved from https://jicnusantara.com/index.php/jicn%0Ahttps://jicnusantara.com/index.php/jicn/article/download/641/723/3538

Rahayu, Y. S., Saputra, Y., & Irawan, D. (2024). Implementasi Metode Waterfall Pada Pengembangan Sistem Informasi Mobile E-Disarpus. *ZONAsi: Jurnal Sistem Informasi*, *6*(2), 523–534. https://doi.org/10.31849/zn.v6i2.20538

Saputri, M. A., & Adytia, P. (2023). Implementasi Single Sign On (SSO) Menggunakan Keycloak pada Sistem Informasi STMIK Widya Cipta Dharma. *Jurnal Elektronika Dan Teknologi Informasi*, *5*(2), 74–90. Retrieved from https://www.ceritahosting.com/

Setiawan, Z. . H. R. C. S. . F. R. . P. I. K. . & S. D. (2024). *Pengantar Sistem Informasi: Konsep Dasar dan Aplikasi Praktis. PT. Sonpedia Publishing Indonesia.* PT. Sonpedia Publishing Indonesia. Retrieved from https://books.google.co.id/books?hl=id&lr=&id=X_X-EAAAQBAJ&oi=fnd&pg=PA1&dq=konsep+sistem+informasi&ots=YcMP5My5F9&sig=bxNtplItWyztSwqwvGHm_SBH8EQ&redir_esc=y

#v=onepage&q=konsep sistem informasi&f=false

Sevara Humaira Putri, & Fajar Nugraha. (2024). Pembangunan Sistem Informasi Berbasis Web Untuk Pendataan Potensi Dan Sumber Kesejahteraan Sosial Di Kabupaten Kudus. *Proficio*, *6*(1), 685–692. https://doi.org/10.36728/jpf.v6i1.4345

Tarigan, R. S., Dwiatma, G., & Wibowo, H. tri. (2021). KEBERMANFAATAN TEKNOLOGI SISTEM INFORMASI PADA DUNIA PENDIDIKAN DI INDONESIA Tuliasan Bersama View project SIPRODI View project. *Universitas Medan Area*. Retrieved from https://doi.org/10.31219/osf.io/vcj87

Wayahdi, M. R., & Ruziq, F. (2023). Pemodelan Sistem Penerimaan Anggota Baru dengan Unified Modeling Language (UML) (Studi Kasus: Programmer Association of Battuta). *Jurnal Minfo Polgan*, *12*(1), 1514–1521. https://doi.org/10.33395/jmp.v12i1.12870

Zulfa, A. A., Ibrahim, T., & Arifudin, O. (2025). Peran Sistem Informasi Akademik Berbasis Web Dalam Upaya Meningkatkan Efektivitas Dan Efisiensi Pengelolaan Akademik Di Perguruan Tinggi. *Jurnal Tahsinia*, *6*(1), 115–134.