JITE, 9 (1) July 2025 ISSN 2549-6247 (Print) ISSN 2549-6255 (Online)

JITE (Journal of Informatics and Telecommunication Engineering)

Available online http://ojs.uma.ac.id/index.php/jite **DOI: 10.31289/jite.v9i1.13750**

Received: 23-December-2024	Accepted: 02-July-2025	Published: 28-July-2025

Simulation of the Single Sign-On Method for Service Provider Applications: A Case Study of Bhayangkara University Surabaya

Vicinthia Veren Sudrajat1) *, R. Dimas Adityo2) & Arif Arizal3)

1,2,3) Prodi atau Jurusan Informatika, Fakultas Teknik, Universitas Bhayangkara Surabaya, Indonesia

*Coresponding Email: vicinveren@gmail.com

Abstrak

Sistem autentikasi di Universitas Bhayangkara Surabaya masih bersifat tradisional, di mana pengguna harus memiliki akun terpisah untuk setiap layanan. Kondisi ini menimbulkan ketidakefisienan, beban administrasi, dan risiko keamanan akibat pengelolaan banyak kredensial. Penelitian ini bertujuan untuk merancang dan mensimulasikan sistem autentikasi tunggal berbasis Single Sign-On (SSO) guna meningkatkan efisiensi dan kemudahan akses pengguna terhadap layanan digital kampus. Sistem dikembangkan dengan pendekatan iteratif menggunakan teknologi JSON Web Token (JWT) dan RESTful API. Simulasi dilakukan melalui pengujian terhadap dua aplikasi, yaitu Identity Provider (IdP) dan Service Provider (SP), yang berinteraksi dalam skenario autentikasi tunggal. Tiga jenis pengujian dilakukan: (1) simulasi alur login dan akses SP setelah otentikasi di IdP, (2) pengujian kompatibilitas antar perangkat Android (multi-device), dan (3) pengujian performa akses RESTful, termasuk waktu respons, throughput, dan validitas token. Hasil menunjukkan bahwa sistem SSO mampu mengintegrasikan layanan kampus secara terpusat, mempercepat autentikasi, dan menjaga keamanan akses. Waktu respons rata-rata tercatat di bawah 1.5 detik, bahkan saat diuji pada 20 perangkat secara simultan. Penerapan SSO terbukti meningkatkan efisiensi operasional dan menyederhanakan manajemen identitas pengguna. Sistem ini memberikan kontribusi terhadap peningkatan pengalaman pengguna serta dapat direplikasi oleh institusi pendidikan lain dengan kebutuhan serupa.

Kata Kunci: Autentikasi, SSO, Android, *Identity Provider*, *Service Provider*

Abstract

The authentication system at Bhayangkara University Surabaya is still traditional, where users must have separate accounts for each service. This condition causes inefficiency, administrative burden, and security risks due to managing multiple credentials. This study aims to design and simulate a single authentication system based on Single Sign-On (SSO) to improve efficiency and ease of user access to campus digital services. The system was developed with an iterative approach using JSON Web Token (JWT) and RESTful API technology. The simulation was carried out by testing two applications, namely Identity Provider (IdP) and Service Provider (SP), which interact in a single authentication scenario. Three types of testing were carried out: (1) simulation of the login flow and SP access after authentication at the IdP, (2) compatibility testing between Android devices (multi-device), and (3) RESTful access performance testing, including response time, throughput, and token validity. The results show that the SSO system is able to centrally integrate campus services, accelerate authentication, and maintain access security. The average response time was recorded below 1.5 seconds, even when tested on 20 devices simultaneously. The implementation of SSO has been proven to improve operational efficiency and simplify user identity management. This system contributes to an improved user experience and can be replicated by other educational institutions with similar needs.

Keywords: Authentication, SSO, Andorid, Identity Provider, Service Provider

How to Cite: Sudrajat, V. V., Adityo, R., & Ariza, A. (2025). Simulation of the Single Sign-On Method for Service Provider Applications: A Case Study of Bhayangkara University Surabaya. *JITE (Journal of Informatics and Telecommunication Engineering), 9*(1), 36-47.

I. PENDAHULUAN

Peran teknologi informasi dalam mendukung sistem informasi di institusi pendidikan telah menjadi krusial dalam menghadapi tuntutan era digital. Teknologi ini memungkinkan efisiensi operasional, peningkatan kualitas layanan, dan aksesibilitas informasi bagi seluruh civitas akademika (Ibrahim, 2024).

Transformasi digital telah mendorong lembaga pendidikan untuk mengadopsi sistem yang lebih terintegrasi dan ramah pengguna. Hal ini terlihat dari menjamurnya aplikasi layanan berbasis smartphone Android yang kini banyak dimanfaatkan oleh berbagai sektor, termasuk perguruan tinggi (Cabaleiro-Cerviño & Vera, 2020).

Namun, sebagian besar aplikasi kampus masih menerapkan autentikasi terpisah untuk setiap layanan, yang mengharuskan pengguna memiliki akun berbeda untuk sistem yang berbeda. Hal ini menimbulkan tantangan seperti rendahnya efisiensi, meningkatnya beban administrasi. Autentikasi dan otorisasi adalah komponen penting dalam manajemen akses pengguna, namun sistem tradisional belum mampu menyatukan proses ini secara terpusat (Kondoj et al., 2023). Misalnya, di Universitas Bhayangkara Surabaya (UBHARA), terdapat berbagai sistem informasi akademik seperti SIM UBHARA, KKN, SIMONTA,dll, masih menggunakan sistem autentikasi yang terpisah. Kondisi ini menuntut pengguna untuk mengingat banyak akun serta melakukan login berulang kali, yang berdampak pada efisiensi, kenyamanan, dan keamanan pengguna (Kondoj et al., 2023).

Untuk mengatasi permasalahan tersebut, Single Sign-On (SSO) hadir sebagai solusi yang tepat. SSO adalah sebuah metode yang memungkinkan pengguna untuk mengakses berbagai sumber daya dan layanan hanya dengan satu proses autentikasi (Pandey & Nisha, 2021). Dengan SSO, seluruh layanan dalam aplikasi dapat diintegrasikan, dan pengelolaan identitas pengguna terpusat, sehingga pengguna tidak perlu melakukan login berulang kali. Dalam konteks UBHARA, implementasi SSO akan memungkinkan mahasiswa, dosen, dan karyawan untuk mengakses seluruh aplikasi dan layanan yang dimiliki, hanya dengan satu akun pengguna. Hal ini tidak hanya akan meningkatkan efisiensi dalam pengelolaan sistem informasi berbasis Android, tetapi juga memberikan kenyamanan akses yang lebih baik bagi seluruh pengguna di lingkungan Universitas Bhayangkara Surabaya.

Penelitian ini bertujuan untuk mengembangkan aplikasi Android yang berfungsi sebagai Identity Provider (IdP) dan diintegrasikan dengan Service Provider (SP) dalam implementasi SSO internal di UBHARA. Sistem ini memungkinkan pengguna kampus mengakses semuaaplikasi dan layanan resmi UBHARA hanya dengan satu akun. Selain itu, kontribusi penelitian ini diharapkan dapat menjadi model dan referensi bagi perguruan tinggi lain dalam mengembangkan dan mengimplementasikan sistem SSO, sehingga secara lebih luas dapat meningkatkan interoperabilitas sistem informasi, efisiensi pengelolaan akun pengguna, dan pengalaman pengguna di lingkungan pendidikan tinggi.

II. METODE PENELITIAN

A. Alur Penelitian

Penelitian ini mengadopsi model pengembangan iteratif untuk membangun sistem Single Sign-On (SSO). Pendekatan ini dipilih karena memungkinkan fleksibilitas, identifikasi masalah dini, dan peningkatan kualitas sistem bertahap. Untuk melaksanakan penelitian ini ada beberapa tahapan dalam penelitian ini yaitu :

Gambar 1. Metode Penelitian Itterative

Tahap Perencanaan

Tahap ini fokus pada penetapan lingkup dan tujuan proyek. Kegiatan meliputi identifikasi kebutuhan fungsional (fitur SSO, manajemen sesi, integrasi SP UBHARA seperti SIM UBHARA, KKN, SIMONTA) dan non-fungsional (kinerja, keamanan, skalabilitas, usability).

Tahap Analisis dan Desain

Pada tahap ini dilakukan:

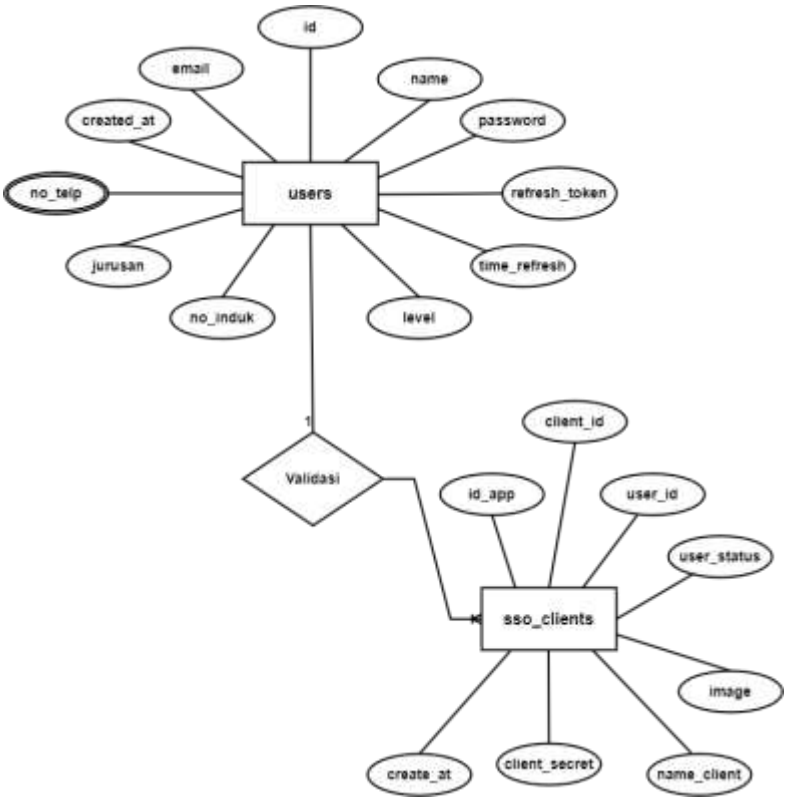
- **Analisis Sistem:** Menganalisis bagaimana mekanisme login tradisional bekerja, serta bagaimana sistem SSO dapat menggantikannya.
- **Analisis Teknologi:**
  - JSON Web Token (JWT) digunakan sebagai mekanisme otorisasi berbasis token untuk menjamin keamanan pertukaran data.
  - RESTful API digunakan sebagai protokol komunikasi antara Identity Provider (IdP) dan Service Provider (SP), karena sifatnya yang ringan dan efisien.
- **Analisis Arsitektur:** Sistem menggunakan model client-server dengan pendekatan microservice sederhana.

Desain teknis mencakup:

- **Data Flow Diagram (DFD)** untuk menggambarkan alur data antar entitas sistem. Berikut DFD (Level 0) sistem SSO yang dirancang.

Gambar 2. Context Diagram (DFD Level 0)

- **Entity Relationship Diagram (ERD)** untuk merancang model database, termasuk tabel user, access_token, dan aplikasi. Berikut ERD pada aplikasi Identity Provider (IdP) :



Gambar 3. Rancangan Entity Relationship Diagram pada Aplikasi IdP

Tahap Implementasi dan Proses Coding

Pada tahap ini, desain diterjemahkan menjadi kode program. Kami menggunakan framework Flutter untuk UI Mobile dan PHP REST API untuk backend. sesi, token JWT, dan API autentikasi/otorisasi. Untuk pengembangan dua aplikasi Android: IdP (Identity Provider) dan SP (Service Provider). Strategi debugging teratur dan dokumentasi kode paralel diterapkan selama proses ini.

Tahap Testing atau Rencana Pengujian

Pengujian dilakukan dengan pendekatan:

- **Black-box Testing:** untuk menguji fungsionalitas sistem tanpa melihat kode, Memastikan semua fitur SSO (login, redirect, validasi token) berfungsi. Kriteria Keberhasilan: Semua test case fungsional 100% berhasil.
- **Pengujian Multi-Device:** Aplikasi diuji pada 20 perangkat secara bersamaan (tablet dan smartphone Android) untuk melihat konsistensi performa.
- **RESTful API Performance:** Mengukur response time metode GET, POST, PUT, DELETE. Hasil menunjukkan rata-rata di bawah 1.5 detik.
- **Pengujian Keamanan:**
  - **Sniffer Test** untuk memantau lalu lintas jaringan (dengan Wireshark) dan memastikan token tidak dikirim dalam bentuk plaintext.
  - **Penetration Testing** pada endpoint API untuk mengecek kerentanan akses ilegal.
- **Acceptance Criteria** mencakup:
  - Waktu respons API < 2 detik.
  - Login sekali sukses harus memberi akses ke semua SP
  - Token harus terenkripsi

Tahap Evaluasi

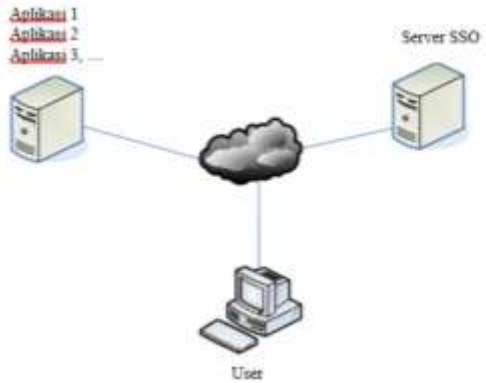
Evaluasi bertujuan menilai keberhasilan sistem dan mengidentifikasi area perbaikan. Metode evaluasi mencakup Uji Coba Pengguna (UAT) dan review internal tim teknis. Feedback yang terkumpul akan didokumentasikan dan dianalisis untuk menjadi dasar perbaikan dan pengembangan sistem pada iterasi atau versi berikutnya.

III. HASIL

Masalah utama dalam penelitian ini adalah membangun sistem autentikasi yang memungkinkan login tunggal untuk berbagai aplikasi penyedia layanan di lingkungan Universitas Bhayangkara Surabaya (UBHARA). Tujuan ini diwujudkan melalui implementasi sistem Single Sign-On (SSO), yang terdiri dari dua aplikasi: Identity Provider (IdP) dan Service Provider (SP).

A. Deskripsi Sistem Single Sign-On (SSO)

Single Sign-On adalah sebuah metode kontrol akses dengan proses autentikasi pengguna atau sesi yang mengizinkan pengguna memasukkan satu kredensial untuk mengakses beberapa aplikasi (Waluyo & Sutarman, 2022).



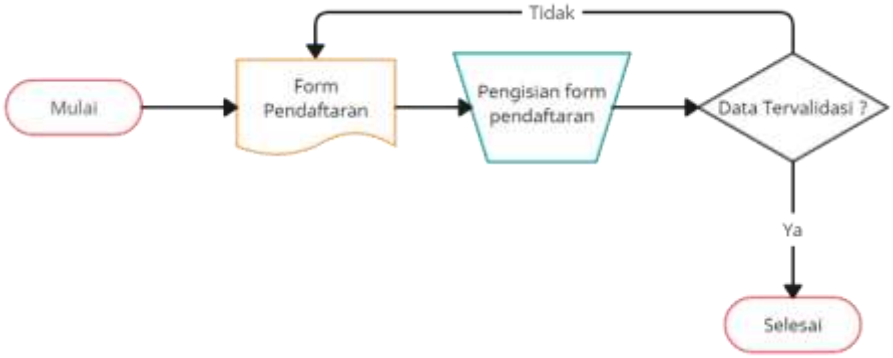
Gambar 4. Sistem *Single Sign-On*

Pada Gambar 4 merupakan topologi sistem SSO yang terdiri atas tiga komponen utama:

1. **Identity Provider**
Menyediakan layanan autentikasi dan otorisasi, menghasilkan token berbasis JSON Web Token (JWT).
2. **Service Provider**
Menerima dan memverifikasi token JWT untuk memberikan akses layanan kepada pengguna.
3. **User (Pengguna)**
Melakukan login satu kali melalui IdP untuk mengakses seluruh aplikasi SP terdaftar.

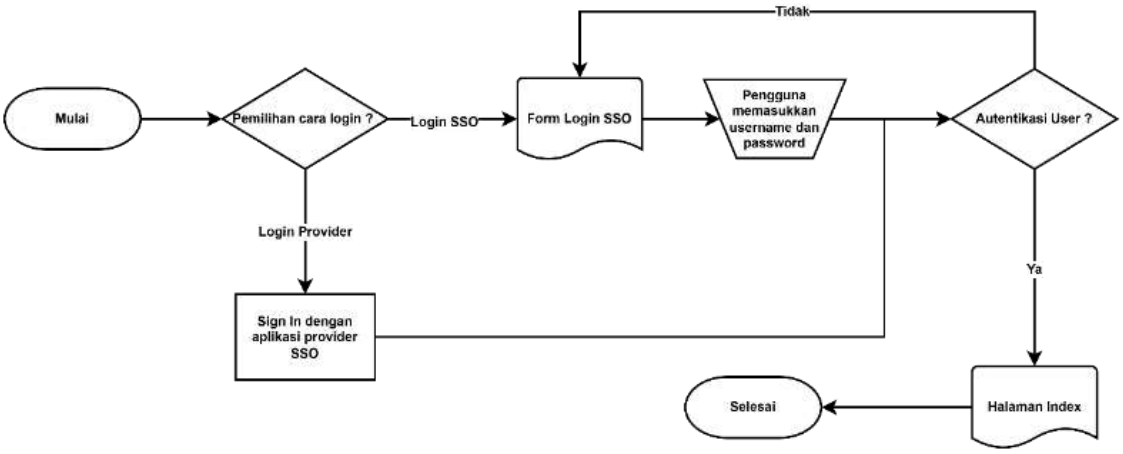
Contoh penggunaan dalam konteks di UBHARA, saat mahasiswa login ke aplikasi IdP untuk mengakses SIM, sistem secara otomatis juga memberikan akses ke SIMONTA dan layanan laboratorium tanpa proses login ulang. Hal yang sama berlaku untuk dosen dan staf saat mengakses sistem akademik dan manajemen internal lainnya

B. Analisis Sistem dan Proses Autentikasi SSO



Gambar 5. Diagram Alir Pendaftaran *Single Sign-On*

Gambar 5 menunjukkan alur pendaftaran pengguna. Pengguna melakukan registrasi pada IdP untuk mendapatkan kredensial yang digunakan dalam login ke aplikasi SP. Proses login kemudian mengikuti diagram alir pada Gambar 6, di mana pengguna dapat login secara manual atau otomatis melalui SSO.



Gambar 6. Diagram Alir Login Aplikasi Penyedia Layanan (SP) Bersistem *Single Sign-On*

Setelah login berhasil, token JWT dibuat dan dikirim ke SP. SP akan memverifikasi token menggunakan signature dan parameter exp untuk menentukan apakah token masih valid. Jika valid, pengguna diberikan akses. Jika token tidak valid atau sudah kedaluwarsa, pengguna diarahkan kembali ke IdP untuk login ulang. Sistem juga mengimplementasikan logout simultan: ketika pengguna logout dari IdP, semua aplikasi SP juga akan otomatis keluar. Ini menjaga konsistensi sesi dan keamanan akses lintas aplikasi.

C. Keamanan Token dan Algoritma Enkripsi

Keamanan sistem Single Sign-On (SSO) diperkuat melalui kombinasi penggunaan JSON Web Token (JWT) dan algoritma enkripsi lokal. JWT digunakan sebagai mekanisme otorisasi utama, di mana token berisi informasi pengguna yang dienkripsi dan ditandatangani secara digital menggunakan algoritma HMAC-SHA256. Token divalidasi oleh aplikasi Service Provider (SP) dengan memverifikasi struktur, masa berlaku (exp), dan signature-nya. Untuk menjaga sesi yang aman, sistem menangani token kedaluwarsa dengan mekanisme refresh token dan error handling.

Sebagai lapisan tambahan, data kredensial pengguna dienkripsi menggunakan dua metode klasik:

1. **Algoritma Pergeseran (Caesar Cipher):** Menggeser posisi karakter dalam alfabet sejauh nilai k. Digunakan untuk menyulitkan pembacaan langsung terhadap input login.
2. **Transposisi Zig-Zag**: Menyusun karakter secara zig-zag berdasarkan pola tertentu untuk mengacak urutan pesan. Menyusun plaintext ke dalam pola baris dan kolom (seperti rel kereta api zig-zag) berdasarkan kunci tertentu. Karakter-karakter disusun secara diagonal menurun dan naik, kemudian dibaca berdasarkan urutan kolom tertentu untuk menghasil- kan ciphertext

Gabungan keduanya memberikan perlindungan dasar terhadap sniffing dan manipulasi data internal. Implementasi algoritma ini dilakukan di sisi aplikasi Identity Provider (IdP) sebelum data disimpan atau digunakan dalam proses autentikasi.

D. Analisis Protokol REST dan Arsitektur

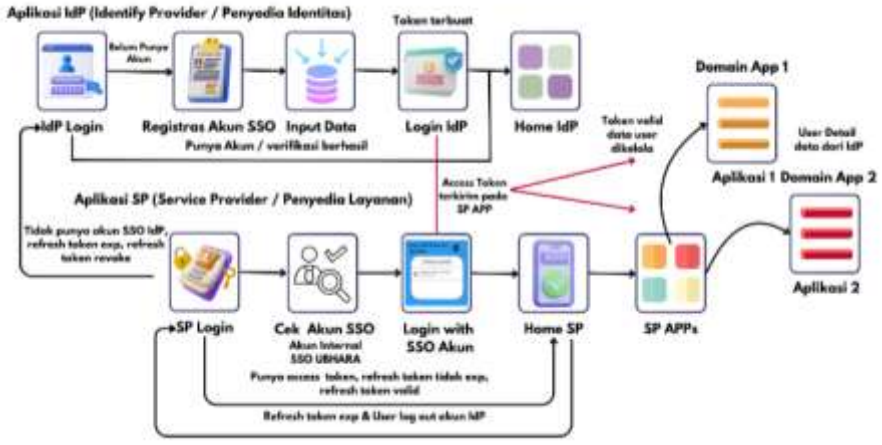
Aplikasi ini menggunakan arsitektur client-server berbasis REST. Backend dibangun dengan PHP (CodeIgniter), dan frontend menggunakan Flutter (Dart). Komunikasi antara client dan server menggunakan HTTP dengan metode:

- **POST :** Untuk login, registrasi, generate token, dan penambahan data
- **GET :** Untuk mengambil data dan validasi token
- **PUT :** Untuk memperbarui data pengguna dan revoke token (admin)
- **DELETE :** Untuk menghapus data pengguna

Metode REST dipilih karena ringan, mudah diimplementasikan, dan efisien dalam pertukaran data JSON antar perangkat mobile.

E. Integrasi Aplikasi IdP dan SP UBHARA

Aplikasi SSO (IdP) dan aplikasi SP saling terintegrasi melalui token JWT. Saat pengguna login di IdP, token dikirim ke SP dan digunakan untuk mengatur hak akses. Sistem memverifikasi token di setiap permintaan, memastikan integritas dan autentikasi pengguna. Logout juga didesain terintegrasi, di mana jika pengguna keluar dari IdP, maka SP akan otomatis menolak token yang sama, sehingga pengguna juga logout dari semua aplikasi.



Gambar 7. Alur Proses Aplikasi SSO (IdP dan SP UBHARA)

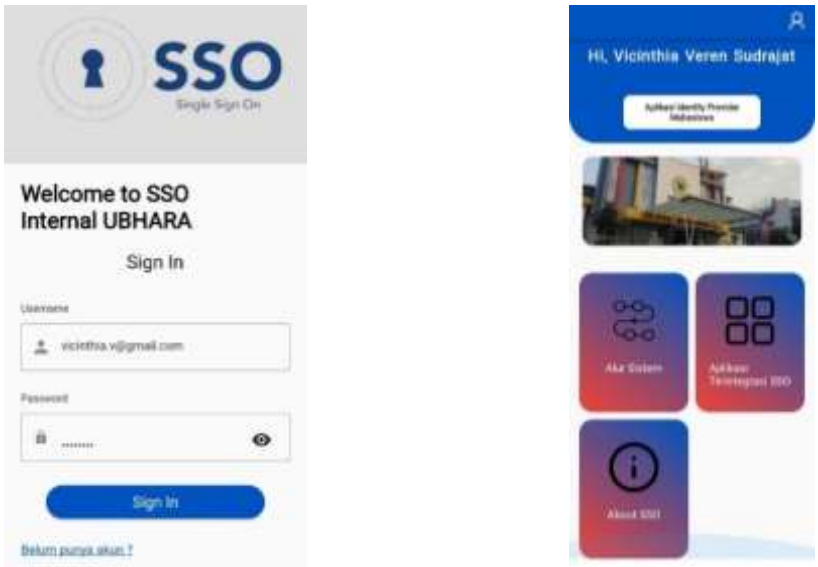
Berdasarkan alur pada Gambar 7, proses kerja sistem SSO dapat dijelaskan sebagai berikut:

1. **Permintaan Akses**: Pengguna mencoba mengakses aplikasi (*Service Provider* - SP).
2. **Pengalihan ke IdP**: Jika belum terautentikasi, pengguna diarahkan ke *Identity Provider* (IdP) untuk login atau registrasi.
3. **Login/Registrasi**: Pengguna mendaftar atau login di aplikasi IdP dengan memasukkan kredensial pada IdP.
4. **Autentikasi di IdP**: Kredensial diverifikasi. Jika berhasil, IdP membuat token JWT.
5. **Token ke SP**: IdP menghasilkan token JWT berisi identitas pengguna, yang ditandatangani secara kriptografi, lalu dikirimkan ke SP melalui API dengan menggunakan header Authorization
6. **Validasi Token di SP**: SP memverifikasi token dan memberikan akses jika valid.
7. **Akses Layanan**: Pengguna mengakses aplikasi SP tanpa login ulang dan SP menggunakan data dalam token untuk pengelolaan pengguna.

F. Pengujian Sistem Single Sign-On

Pengujian aplikasi Android sistem single sign-on melibatkan pengguna yang mengakses aplikasi Service Provider (SP). Pengguna diarahkan ke aplikasi Identity Provider (IdP) untuk login dengan memasukkan kredensial. Setelah berhasil, seluruh layanan aplikasi client yang terdaftar di SP terbuka tanpa perlu login ulang. Tahapannya:

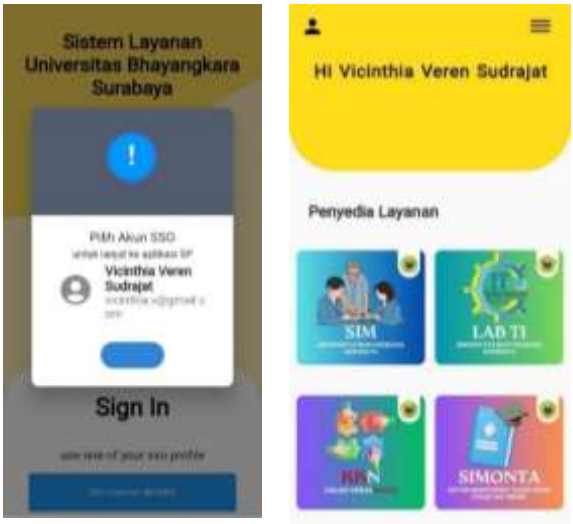
1. Pengguna login ke IdP dengan username dan password, atau registrasi jika belum memiliki akun.
2. Pengguna berhasil masuk dan diarahkan ke halaman utama aplikasi Identity Provider (IdP).



Gambar 8. Tampilan Login Sistem SSO (IdP) dan Beranda Aplikasi IdP

Pengujian sistem Single Sign-On dilakukan melalui proses login menggunakan kredensial pengguna. Jika valid, sistem akan mengarahkan pengguna ke halaman utama aplikasi.

3. Pengguna dapat mengakses aplikasi penyedia layanan (Service Provider) tanpa perlu memasukkan ulang kredensial, karena proses login dilakukan otomatis menggunakan akun SSO (IdP) yang dimiliki.
4. Serta selama token SSO masih aktif, maka pengguna tidak akan melakukan aksi memasukkan username dan password setiap masuk ke alikasi IdP dan SP.



Gambar 9. Tampilan Halaman Sign In dan Halaman Beranda
Aplikasi Penyedia Layanan (SP)

Saat pengguna membuka aplikasi client lain yang terhubung dengan penyedia layanan, sistem secara otomatis sudah dalam kondisi login tanpa perlu autentikasi ulang. Namun, jika pengguna keluar dari aplikasi IdP, maka seluruh aplikasi SP juga akan otomatis keluar

5. Pengguna mendapatkan hak akses yang sesuai dengan akun IdP yang dipunya, berupa layanan internal akademik Universitas Bhayangkara Surabaya yang sering digunakan oleh user mahasiswa, dosen, dan karyawan.
   Diantaranya:
   Mahasiswa : SIM, KKN, Lab Ti/Sipil/Elektro, SIMONTA
   Dosen : SIM, KKN, Lab Ti/Sipil/Elektro, SIMONTA, SIMPEL, SISTER
   Karyawan : SIM, Koperasi

G. Pengujian Sistem SSO pada Multi Device

Dalam konteks *multi-device*, aplikasi SSO mendukung berbagai perangkat seperti tablet dan smartphone di sistem operasi Android. Pengujian ini memastikan: kompabilitas antar perangkat.

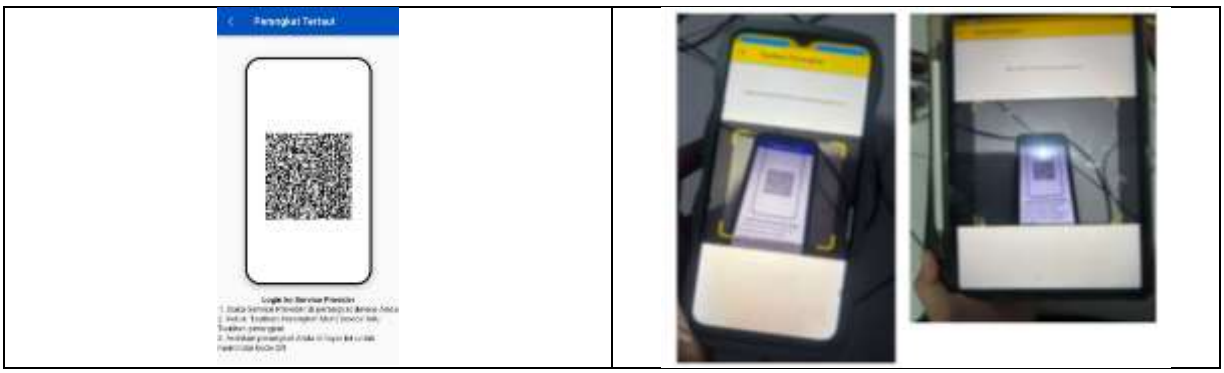
H. Tahapan Pengujian

a. Pengujian Fungsional

Pengujian ini bertujuan untuk memverifikasi bahwa fitur SSO berjalan sesuai dengan spesifikasi.

Skenario Login:

- Pengguna login ke IdP pada satu perangkat, lalu akses aplikasi SP di perangkat lain tanpa login ulang.
- Login menggunakan berbagai perangkat



Gambar 10. Tautkan Perangkat pada IdP dan Akses Aplikasi SP

Pengguna berhasil mengakses aplikasi SP di perangkat lain tanpa harus login ulang aplikasi IdP (scan QR code IdP) dengan user yang meiliki hak atau otoritas yang sama diantara keduanya.

b. Pengujian Kompatibilitas

Memastikan aplikasi SSO dapat berjalan pada berbagai sistem operasi android:

- Perangkat: smartphone dan tablet dengan resolusi layar berbeda
- Tampilan antarmuka harus responsif dan mudah digunakan

Gambar 11. Aplikasi SP pada Berbagai Perangkat

Aplikasi diuji pada berbagai resolusi dan perangkat Android. Tampilan UI menyesuaikan secara responsif berdasarkan ukuran layar dan orientasi perangkat

I. Pengujian Performa RESTful API

Analisa data untuk mengukur *throughput* pada aplikasi IdP dan SP yang meliputi :

- Login (POST), Mencatat data user yang login masuk ke aplikasi, serta dilakukan proses autentikasi dan autorisasi user pada tahap ini
- List Users (GET), Mengambil semua user dengan filter parameter
- Edit User (PUT), Mengubah data users berdasarkan ID
- Delete User (DELETE), Menghapus akun user berdasarkan ID
- SSO Clients (POST), Menambahkan client pada server IdP
- Validasi Token (GET), Mengirimkan token diheader 'Authorization' dengan format 'bearer' untuk divalidasi
- Verify Token (GET), Verifikasi token untuk mendapatkan data

Pengujian pada android dilakukan total sebanyak 315 kali pada RESTful dipenggunaan time, size dan speed_download (throughput). Berikut hasil pengujian data dengan test request yang telah ditentukan dari beberapa kali pengujian. Berikut adalah tabel hasil uji untuk beberapa data layanan aplikasi setiap metode (POST, PUT, DELETE, GET) pada 10, 15, dan 20 perangkat :

Tabel 1. Hasil Pengujian Kecepatan Restful

Metode	Jumlah Device	Rata-rata Waktu (s)	Rata-rata Ukuran Data (bytes)	Kecepatan (bytes/s)
POST	10	1.14	123	103
	15	1.12	122	105
	20	1.15	124	105
GET	10	1.32	281	207
	15	1.31	298	202
	20	1.24	304	237
PUT	10	1.41	50	37

Metode	Jumlah Device	Rata-rata Waktu (s)	Rata-rata Ukuran Data (bytes)	Kecepatan (bytes/s)
	15	1.40	54	35
	20	1.50	55	36
DELETE	10	1.07	0	0
	15	1.46	0	0
	20	1.00	0	0

Hasil: Rata-rata waktu respons seluruh metode berada di bawah 1.5 detik, bahkan pada kondisi 20 perangkat. Throughput meningkat secara konsisten seiring jumlah perangkat, menunjukkan sistem skalabel dan tidak mengalami bottleneck yang signifikan. Dengan waktu respons di bawah 1.5 detik, sistem telah memenuhi pedoman performa yang lazim digunakan, seperti pedoman IBM dan Web Performance Optimization, yang menetapkan batas maksimal untuk interaksi real-time sekitar 2 detik untuk interaksi pengguna yang lancar dan responsif. . Oleh karena itu, capaian ini menunjukkan bahwa sistem mampu merespons permintaan dengan cepat dan sesuai dengan standar yang diterima dalam sistem informasi.

IV. PEMBAHASAN

Sistem SSO yang dikembangkan menunjukkan performa respons cepat (di bawah 1,5 detik) dan stabil hingga 20 perangkat, membuktikan keberhasilan pencapaian tujuan penelitian untuk menciptakan autentikasi terpusat yang efisien di lingkungan Universitas Bhayangkara Surabaya. SSO mempermudah akses ke berbagai layanan dengan satu login, meningkatkan efisiensi dan keamanan sesi pengguna. Dibandingkan metode login terpisah, sistem ini unggul karena cukup menggunakan satu kredensial, mendukung logout otomatis, dan mempercepat validasi lewat token JWT tanpa menyimpan data sensitif di tiap aplikasi. Hal ini menciptakan sistem yang lebih terintegrasi dan user-friendly. Dibanding solusi SSO berbasis OAuth atau SAML, sistem ini lebih ringan dan efisien pada perangkat mobile berkat penggunaan JWT dan REST API. Meskipun tidak mendukung otorisasi pihak ketiga seperti OAuth, sistem ini lebih cocok untuk institusi pendidikan dengan kebutuhan internal. Keamanan awal ditangani dengan Caesar cipher dan transposisi zig-zag, lalu diperkuat dengan JWT berbasis HMAC-SHA256. Sistem juga memverifikasi masa aktif token dan mengarahkan ulang jika token tidak valid, menjaga agar hanya token sah yang digunakan. Pendekatan ini mengurangi proses autentikasi berulang dan memperkuat kontrol otorisasi. Meski berhasil, sistem masih terbatas pada pengujian 20 perangkat. Untuk skala besar dibutuhkan peningkatan infrastruktur. Selain itu, pengujian terhadap ancaman keamanan lanjutan masih perlu dilakukan. Secara praktis, sistem ini mempermudah manajemen akses bagi seluruh sivitas akademika dan dapat direplikasi di institusi lain sebagai fondasi pengembangan SSO pendidikan berskala nasional.

V. KESIMPULAN

Penelitian ini berhasil membangun sistem Single Sign-On (SSO) berbasis Android di lingkungan Universitas Bhayangkara Surabaya, memungkinkan login tunggal ke berbagai layanan kampus. Sistem mengintegrasikan aplikasi melalui autentikasi terpusat menggunakan Identity Provider (IdP) dan token JWT. Keamanan ditingkatkan dengan algoritma enkripsi kombinasi pergeseran dan transposisi, yang cukup efektif menghadapi serangan brute-force dan Known-Plaintext Attack. Pengujian performa menunjukkan waktu respons REST API stabil di bawah 1,5 detik hingga 20 perangkat, serta dilindungi oleh SSL untuk keamanan data. Hasil ini menunjukkan bahwa sistem yang dibangun telah menjawab tujuan penelitian: menyediakan autentikasi yang efisien, aman, dan terintegrasi untuk mendukung layanan digital kampus

DAFTAR PUSTAKA

Agarkar, A. A., Karyakarte, M., Chavhan, G., Patil, M., Talware, R., & Kulkarni, L. (2024). Blockchain aware decentralized identity management and access control system. *Measurement: Sensors*, *31*(February 2023), 101032. https://doi.org/10.1016/j.measen.2024.101032

Anand, D., Khemchandani, V., Sabharawal, M., Cheikhrouhou, O., & Ben Fredj, O. (2021). Lightweight Technical Implementation of Single Sign-On Authentication and Key Agreement Mechanism for

Multiserver Architecture-Based Systems. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/9940183

Benavides, L. M. C., Arias, J. A. T., & Burgos, D. (2023). Digital Transformation in Higher Education Institutions Implementation Model. *Lecture Notes in Educational Technology*, *05*(04), 1211–1219. https://doi.org/10.1007/978-981-99-0942-1_127

Cabaleiro-Cerviño, G., & Vera, C. (2020). The impact of educational technologies in higher education 1 El Impacto de las Tecnologías Educativas en la Educación Superior. *Gist Education and Learning Research Journal*, *2*(20), 155–169.

Ghiffari, A., & Hendradi, P. (2023). Implementasi Single sign on (SSO) Menggunakan Representational State Transfer (REST) dan Open Authorization (OAuth 2.0) (Studi kasus: Universitas Muhammadiyah Magelang). *Smart Comp: Jurnalnya Orang Pintar Komputer*, *12*(2), 356–366. https://doi.org/10.30591/smartcomp.v12i2.4939

Hodapp, D., & Hanelt, A. (2022). Interoperability in the era of digital innovation: An information systems research agenda. *Journal of Information Technology*, *37*(4), 407–427. https://doi.org/10.1177/02683962211064304

Ibrahim, U. (2024). Assessing the Impact of Mobile Applications on Student Engagement in ICT and Computer Science Education. *International Journal of Applied and Advanced Multidisciplinary Research*, *2*(3), 221–232. https://doi.org/10.59890/ijaamr.v2i3.1533

Kondoj, M., Saroinsong, T., & Polii, A. (2023). *Single Sign On (SSO) System with Application of Central Authentication Service (CAS) at Manado State Polytechnic*. *January*, 698–702. https://doi.org/10.5220/0011863100003575

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

Okoli, K., & Bekeneva, Y. (2024). Balancing security and user experience in the evolving digital landscape. *E3S Web of Conferences*, *471*. https://doi.org/10.1051/e3sconf/202447104007

Pandey, P., & Nisha, T. N. (2021). Challenges in Single Sign-On. *Journal of Physics: Conference Series*, *1964*(4). https://doi.org/10.1088/1742-6596/1964/4/042016

Parama, R. A., Studiawan, H., & Akbar, R. J. (2022). Implementasi Continuous Integration dan Continuous Delivery Pada Aplikasi myITS Single Sign On. *Jurnal Teknik ITS*, *11*(3). https://doi.org/10.12962/j23373539.v11i3.99436

Paramartha, I. G. A., Sudana, A. A. K. O., & Putra, I. M. S. (2021). Perancangan User Interface dan User Experience Sistem Informasi Manajemen Rumah Sakit Modul Single Sign On. *JITTER : Jurnal Ilmiah Teknologi Dan Komputer*, *1*(2), 199–210. https://ojs.unud.ac.id/index.php/jitter/article/view/69540

Patent, U. S. (2022). *United States Patent : 7215786 United States Patent : 7215786*. *November 1999*, 1–18.

Prasad, R. V., Dave, A., Arulkumaran, R., Goel, O. M., Kumar, L., & Jain, P. A. (2023). *Integrating Secure Authentication Across Distributed Systems*. *7*(3), 498–516.

Senapartha, I. K. D. (2021). Implementasi Single Sign-On Menggunakan Google Identity, REST dan OAuth 2.0 Berbasis Scrum. *Jurnal Teknik Informatika Dan Sistem Informasi*, *7*(2), 307–320. https://doi.org/10.28932/jutisi.v7i2.3437

Sophonhiranrak, S. (2021). Features, barriers, and influencing factors of mobile learning in higher education: A systematic review. *Heliyon*, *7*(4), e06696. https://doi.org/10.1016/j.heliyon.2021.e06696

Sunaringtyas, S. U., & Prayoga, D. S. (2021). Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada Layanan Single Sign-On. *Edu Komputika Journal*, *8*(1), 48–56. https://doi.org/10.15294/edukomputika.v8i1.47179

Utama, J. S., & Indriyanti, A. D. (2023). Pengamanan Restful API Web Service Menggunakan Json Web Token (Studi Kasus: Aplikasi Siakadu Mobile Unesa). *Journal of Emerging Information …*, *04*(01), 8–17.https://ejournal.unesa.ac.id/index.php/JEISBI/article/view/50534%0Ahttps://ejournal.unesa.ac.id/index.php/JEISBI/article/download/50534/41454

Waluyo, T., & Sutarman. (2022). Comparative Analysis of the Performance of Single Sign-On Authentication Systems with OpenID and OAuth Protocols. *International Journal of Computer and Information Technology(2279-0764)*, *11*(3), 100–107. https://doi.org/10.24203/ijcit.v11i3.277

Waluyowati, N. P., Riandi, M. H., & Province, E. J. (2025). *Evaluating the Impact of Servicescape and Information Systems on University Students ' Academic Performance in Malang*. *10*(1), 121–140.

Yusuf, M., Yusup, M., Dani Pramudya, R., Yadi Fauzi, A., & Rizky, A. (2024). Enhancing User Login Efficiency via Single Sign-On Integration in Internal Quality Assurance System (eSPMI). *International Transactions on Artificial Intelligence (ITALIC)*, *2*(2), 164–172. https://doi.org/10.33050/italic.v2i2.556

Zhang, Y. (2025). *A Study of the Digital Transformation and Improvement Path of University Administration*. *01001*.

Zidan, M., Nur'aini, S., Wibowo, N. C. H., & Ulinuha, M. A. (2022). Black Box Testing pada Aplikasi Single Sign On (SSO) di Diskominfostandi Menggunakan Teknik Equivalence Partitions. *Walisongo Journal of Information Technology*, *4*(2), 127–137. https://doi.org/10.21580/wjit.2022.4.2.12135

Ziliwu, K. B., Maslan, A., & Kremer, H. (2022). Implementasi Caesar Cipher pada Algoritma Kriptografi dalam Penyandian Pesan Whatsapp. *Jurnal Comasie*, *7*(2), 117–125.

Zukarnain, Z. A., Muneer, A., & Ab Aziz, M. K. (2022). Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges. *Symmetry*, *14*(4). https://doi.org/10.3390/sym14040821