Integrated Journal of Applied Technology and Informatics
Journal homepage: https://journal2.uinssc.ac.id/index.php/IJATI

A Single Sign-On Architecture for Integrated Smart City Information Systems

Arsitektur *Single Sign-On* untuk Sistem Informasi Kota Cerdas Terintegrasi

Saluky[1], Aisya Fathima[2]
[1]Jurusan Informatika, Universitas Islam Negeri Siber Syekh Nurjati Cirebon, Cirebon, 45153, Indonesia
[2]Jurusan Teknik Elektro, Universitas Negeri Semarang, Semarang, 50229, Indonesia
[1]saluky@uinssc.ac.id, [2]fathimahaisya1@stundents.unnes.ac.id

ARTICLE INFO
Article history:
Received 2026-06-30
Revised 2026-06-30
Accepted 2026-06-30

CORRESPONDING AUTHOR
Saluky
saluky@uinssc.ac.id

ABSTRACT
The increasing adoption of smart city initiatives has accelerated the development of diverse digital services across government sectors, including public administration, healthcare, transportation, education, and utility management. However, these services are frequently developed as independent systems with separate authentication mechanisms, resulting in fragmented user identities, redundant login processes, increased administrative complexity, and greater exposure to security risks. This study proposes a Single Sign-On (SSO) architecture for integrated smart city information systems to provide unified authentication, centralized identity management, and secure interoperability across heterogeneous applications. The proposed architecture adopts a federated identity management approach based on OAuth 2.0 and OpenID Connect (OIDC), with Keycloak serving as the Identity Provider to facilitate standards-compliant authentication and authorization. The architecture was implemented and evaluated using multiple representative smart city applications to assess functional integration, authentication performance, interoperability, and security. The evaluation results demonstrate that the proposed architecture enables seamless access to multiple services through a single authentication process while reducing authentication redundancy, simplifying user and administrator management, and improving system interoperability. Furthermore, token-based authentication enhances access security by minimizing credential exposure and supporting standardized authorization across interconnected services. The proposed architecture also exhibits low authentication latency, stable performance under concurrent access, and compatibility with heterogeneous technology platforms. This study contributes a scalable, interoperable, and standards-based authentication framework that strengthens identity and access management, improves user experience, and provides a practical foundation for secure and sustainable smart city digital ecosystems.
Keyword: Smart City, Single Sign-On, Identity and Access Management, Federated Identity Management, OAuth 2.0, OpenID Connect.

ABSTRAK
Meningkatnya adopsi inisiatif kota cerdas telah mempercepat pengembangan beragam layanan digital di berbagai sektor pemerintahan, termasuk administrasi publik, perawatan kesehatan, transportasi, pendidikan, dan manajemen utilitas. Namun, layanan-layanan ini sering dikembangkan sebagai sistem independen dengan mekanisme otentikasi terpisah, yang mengakibatkan identitas pengguna yang terfragmentasi, proses login yang berlebihan, peningkatan kompleksitas administratif, dan peningkatan risiko keamanan. Studi ini mengusulkan arsitektur Single Sign-On (SSO) untuk sistem informasi kota cerdas terintegrasi guna menyediakan otentikasi terpadu, manajemen identitas terpusat, dan interoperabilitas yang aman di seluruh aplikasi heterogen. Arsitektur yang diusulkan mengadopsi pendekatan manajemen identitas terfederasi berdasarkan OAuth 2.0 dan OpenID Connect (OIDC), dengan Keycloak sebagai Penyedia Identitas untuk memfasilitasi otentikasi dan otorisasi yang sesuai standar. Arsitektur tersebut diimplementasikan dan dievaluasi menggunakan beberapa aplikasi kota cerdas representatif untuk menilai integrasi fungsional, kinerja otentikasi, interoperabilitas, dan keamanan. Hasil evaluasi menunjukkan bahwa arsitektur yang diusulkan memungkinkan akses tanpa hambatan ke berbagai layanan melalui satu proses otentikasi sekaligus mengurangi redundansi otentikasi, menyederhanakan manajemen pengguna dan administrator, serta meningkatkan interoperabilitas sistem. Selain itu, autentikasi berbasis token meningkatkan keamanan akses dengan meminimalkan paparan kredensial dan mendukung otorisasi standar di seluruh layanan yang saling terhubung. Arsitektur yang diusulkan juga menunjukkan latensi autentikasi yang rendah, kinerja yang stabil di bawah akses bersamaan, dan kompatibilitas dengan platform teknologi heterogen. Studi ini memberikan kerangka kerja autentikasi yang terukur, interoperabel, dan berbasis standar yang memperkuat manajemen identitas dan akses, meningkatkan pengalaman pengguna, dan menyediakan fondasi praktis untuk ekosistem digital kota pintar yang aman dan berkelanjutan.
Kata Kunci: Kota Cerdas, Single Sign-On, Manajemen Identitas dan Akses, Manajemen Identitas Terfederasi, OAuth 2.0, OpenID Connect.

1. PENDAHULUAN

Kemajuan pesat teknologi informasi dan komunikasi telah mempercepat transformasi lingkungan perkotaan menjadi kota pintar, di mana teknologi digital dimanfaatkan untuk meningkatkan layanan publik, tata kelola, keberlanjutan, dan kualitas hidup warga[1], [2]. Ekosistem kota pintar mengintegrasikan beragam sistem informasi dari berbagai lembaga pemerintah, termasuk e-government, transportasi, perawatan kesehatan, pendidikan, keamanan publik, perpajakan, perizinan, dan manajemen utilitas[3], [4]. Sistem-sistem ini menghasilkan nilai yang signifikan dengan memungkinkan berbagi data dan penyampaian layanan yang terkoordinasi; namun, sistem-sistem ini sering dikembangkan secara independen menggunakan platform, basis data, dan mekanisme otentikasi yang heterogen[5], [6]. Akibatnya, warga seringkali diharuskan untuk memelihara banyak akun pengguna dan berulang kali melakukan otentikasi saat mengakses berbagai layanan publik, yang menyebabkan identitas digital yang terfragmentasi, pengalaman pengguna yang buruk, peningkatan kompleksitas administrasi, dan risiko keamanan yang lebih tinggi.

Manajemen Identitas dan Akses (IAM) telah muncul sebagai komponen fundamental dari ekosistem digital yang aman dengan menyediakan mekanisme untuk otentikasi, otorisasi, dan tata kelola identitas di seluruh layanan yang saling terhubung[7], [8]. Di antara teknologi IAM, Single Sign-On (SSO) telah mendapatkan adopsi yang luas karena memungkinkan pengguna untuk melakukan otentikasi sekali dan mengakses banyak aplikasi secara aman tanpa proses login berulang[9]. Implementasi SSO modern umumnya menggunakan protokol federasi identitas standar seperti OAuth 2.0 [10] dan OpenID Connect (OIDC)[11], yang mendukung interoperabilitas antar aplikasi terdistribusi sekaligus mengurangi duplikasi kredensial dan menyederhanakan manajemen akses. Teknologi ini telah berhasil diimplementasikan dalam sistem perusahaan, lembaga pendidikan tinggi, lingkungan komputasi awan, dan sistem informasi kesehatan, yang menunjukkan peningkatan dalam kegunaan, efisiensi operasional, dan keamanan.

Terlepas dari kemajuan ini, implementasi SSO dalam ekosistem kota cerdas masih terbatas. Studi yang ada terutama berfokus pada penerapan SSO di lingkungan organisasi atau perusahaan di mana aplikasi dikembangkan di bawah satu domain administratif[12]. Sebaliknya, platform kota cerdas melibatkan beberapa lembaga pemerintah otonom yang mengoperasikan aplikasi heterogen dengan teknologi, kebijakan keamanan, dan tanggung jawab organisasi yang berbeda. Sebagian besar penelitian yang ada menekankan mekanisme otentikasi atau kinerja protokol tanpa membahas tantangan arsitektur yang lebih luas yang terkait dengan pengintegrasian layanan publik lintas domain ke dalam kerangka manajemen identitas yang terpadu. Lebih lanjut, hanya sejumlah kecil studi yang menyediakan model arsitektur ujung-ke-ujung yang disertai dengan implementasi dan evaluasi dalam lingkungan layanan kota cerdas yang realistis. Akibatnya, pemerintah yang berupaya membangun layanan digital terintegrasi masih kekurangan referensi arsitektur komprehensif yang secara simultan menangani interoperabilitas, skalabilitas, manajemen identitas terpusat, dan otentikasi lintas aplikasi yang aman.

Keterbatasan ini mewakili kesenjangan penelitian yang signifikan. Pertama, penelitian yang mengusulkan arsitektur SSO standar yang dirancang khusus untuk sistem informasi kota cerdas heterogen masih kurang, bukan untuk aplikasi perusahaan konvensional. Kedua, studi sebelumnya jarang mengintegrasikan manajemen identitas terfederasi, protokol otentikasi standar, administrasi terpusat, dan implementasi praktis ke dalam kerangka kerja terpadu yang sesuai untuk ekosistem digital kota. Ketiga, evaluasi empiris yang secara simultan menilai integrasi fungsional, interoperabilitas, kinerja otentikasi, dan keamanan di lingkungan kota cerdas masih langka, sehingga sulit untuk menilai penerapan praktis dari pendekatan yang ada[12].

Untuk mengatasi kesenjangan ini, studi ini mengusulkan arsitektur Single Sign-On untuk sistem informasi kota cerdas terintegrasi berdasarkan manajemen identitas terfederasi menggunakan OAuth 2.0, OpenID Connect (OIDC), dan Keycloak sebagai Penyedia Identitas[13]. Arsitektur yang diusulkan memungkinkan otentikasi terpusat sekaligus memungkinkan aplikasi kota cerdas heterogen untuk tetap independen secara operasional. Berbeda dengan studi sebelumnya yang terutama meneliti protokol otentikasi atau implementasi terisolasi, kerangka kerja yang diusulkan menekankan integrasi arsitektur, interoperabilitas berbasis standar, dan tata kelola identitas terpusat di berbagai layanan digital publik. Arsitektur ini dirancang untuk mendukung skalabilitas, memfasilitasi integrasi aplikasi kota tambahan di masa mendatang, dan memperkuat keamanan akses melalui otentikasi berbasis token dan mekanisme otorisasi standar.

Kebaruan penelitian ini terletak pada empat kontribusi utama. Pertama, penelitian ini mengusulkan arsitektur SSO komprehensif yang dirancang khusus untuk sistem informasi kota cerdas heterogen yang beroperasi di berbagai domain pemerintahan[14], [15]. Kedua, penelitian ini mengintegrasikan manajemen identitas terfederasi dengan standar otentikasi yang diakui secara internasional, yaitu OAuth 2.0 dan OpenID Connect, untuk membangun layanan digital yang

interoperabel dan terukur. Ketiga, penelitian ini mendemonstrasikan implementasi praktis dari arsitektur yang diusulkan menggunakan Keycloak sebagai Penyedia Identitas sumber terbuka yang terintegrasi dengan aplikasi kota cerdas yang representatif. Terakhir, arsitektur yang diusulkan dievaluasi secara komprehensif dalam hal integrasi fungsional, interoperabilitas, kinerja otentikasi, dan keamanan, memberikan bukti empiris tentang kelayakannya untuk penerapan kota cerdas di dunia nyata.

Penelitian ini bertujuan untuk merancang, mengimplementasikan, dan mengevaluasi arsitektur Single Sign-On yang terukur dan aman yang meningkatkan interoperabilitas, meningkatkan manajemen identitas dan akses, menyederhanakan otentikasi pengguna, dan mendukung pengembangan ekosistem digital kota cerdas yang berpusat pada warga. Temuan ini diharapkan dapat memberikan kontribusi baik secara teoritis pada bidang Manajemen Identitas dan Akses untuk kota cerdas maupun secara praktis dengan menyediakan arsitektur referensi yang dapat diadopsi oleh pemerintah yang menerapkan layanan publik digital terintegrasi.

2. METODE

Studi ini mengadopsi metodologi *Design Science Research* (DSR) untuk merancang, mengimplementasikan, dan mengevaluasi arsitektur *Single Sign-On* (SSO) untuk sistem informasi kota cerdas terintegrasi. DSR dipilih karena tujuan utama penelitian ini adalah untuk mengembangkan dan memvalidasi artefak inovatif berupa arsitektur otentikasi yang mampu mengatasi tantangan interoperabilitas dan manajemen identitas dalam lingkungan kota cerdas yang heterogen. Metodologi penelitian terdiri dari lima fase berurutan: identifikasi masalah, desain arsitektur, implementasi prototipe, integrasi sistem, dan evaluasi kinerja.

2.1. Identifikasi Masalah

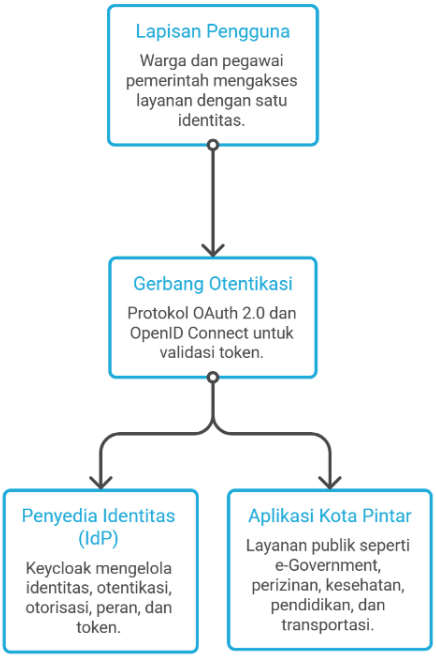
Fase pertama berfokus pada identifikasi tantangan terkait otentikasi dalam sistem informasi kota cerdas yang ada. Beberapa aplikasi layanan publik dianalisis untuk memahami keterbatasan mekanisme otentikasi independen, termasuk akun pengguna yang duplikat, manajemen identitas yang terfragmentasi, kebijakan otorisasi yang tidak konsisten, dan prosedur login yang berulang. Selain itu, tinjauan literatur komprehensif tentang *Identity and Access Management* (IAM), *Single Sign-On* (SSO), OAuth 2.0, OpenID Connect (OIDC), dan manajemen identitas terfederasi dilakukan untuk membangun landasan teoritis bagi arsitektur yang diusulkan. Studi sebelumnya menunjukkan bahwa meskipun OAuth 2.0 dan OpenID Connect telah menjadi standar de facto untuk otentikasi terfederasi, implementasi arsitekturnya di berbagai layanan kota pintar yang heterogen masih terbatas.

2.2. Arsitektur SSO yang Diusulkan

Berdasarkan persyaratan yang telah diidentifikasi, arsitektur SSO dirancang menggunakan model manajemen identitas terfederasi. Arsitektur ini terdiri dari empat komponen utama:

- Penyedia Identitas (IdP): Keycloak mengelola identitas pengguna, otentikasi, otorisasi, manajemen peran, dan pembuatan token.
- Aplikasi Kota Pintar: Beberapa aplikasi heterogen yang mewakili layanan publik digital, seperti e-Government, perizinan, perawatan kesehatan, pendidikan, dan sistem transportasi.
- Gerbang Otentikasi: Protokol OAuth 2.0 dan OpenID Connect mengelola permintaan otentikasi, validasi token, dan proses otorisasi.
- Lapisan Pengguna: Warga dan pegawai pemerintah mengakses semua layanan menggunakan satu identitas digital.

Proses otentikasi dapat dilihat pada Gambar 1 ketika pengguna meminta akses ke salah satu aplikasi kota pintar. Aplikasi ini mengarahkan permintaan autentikasi ke Penyedia Identitas melalui Alur Kode Otorisasi OpenID Connect. Setelah verifikasi kredensial berhasil, Penyedia Identitas menerbitkan Token ID, Token Akses, dan Token Refresh. Sesi yang telah diautentikasi kemudian dibagikan di antara semua aplikasi yang terhubung, memungkinkan akses tanpa hambatan tanpa memerlukan autentikasi berulang. Arsitektur ini mempertahankan independensi aplikasi sambil memusatkan manajemen identitas dan kontrol akses.



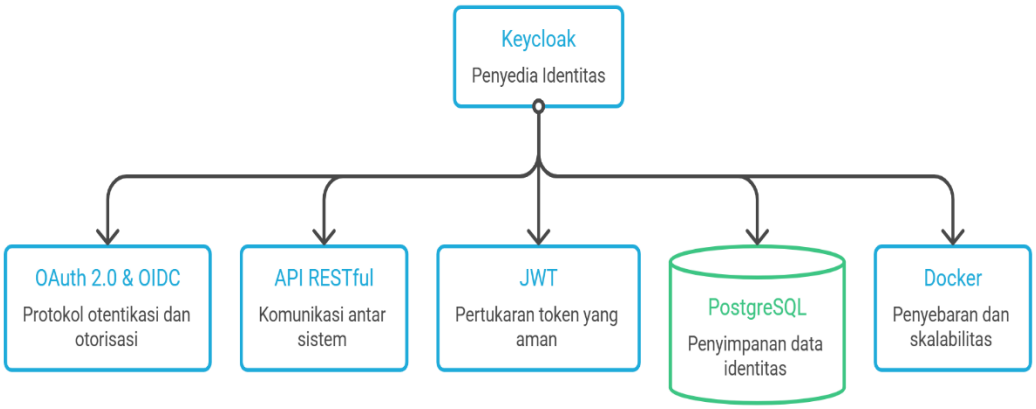
Gambar 1. Arsitektur SSO Model Manajemen Identitas

2.3. Implementasi Prototipe

Untuk memvalidasi arsitektur yang diusulkan, lingkungan prototipe dikembangkan menggunakan Keycloak sebagai Penyedia Identitas. Beberapa aplikasi kota pintar yang representatif diintegrasikan sebagai klien OpenID Connect. Setiap aplikasi mempertahankan basis data dan logika bisnisnya sendiri sambil mendelegasikan fungsi autentikasi dan otorisasi ke Penyedia Identitas terpusat.

Implementasi ini menggunakan teknologi berikut:

- Keycloak sebagai Penyedia Identitas
- OAuth 2.0 dan OpenID Connect untuk otentikasi dan otorisasi
- API RESTful untuk komunikasi antar sistem
- JSON Web Token (JWT) untuk pertukaran token yang aman
- PostgreSQL untuk penyimpanan data identitas
- Kontainer Docker untuk penyebaran dan skalabilitas



Gambar 2. Arsitektur Implementasi Sistem Identitas

Implementasi ini (Gambar 2) menunjukkan bahwa aplikasi heterogen yang dikembangkan menggunakan kerangka kerja pemrograman yang berbeda dapat beroperasi secara aman melalui protokol otentikasi standar tanpa memodifikasi fungsi bisnis intinya.

2.4. Prosedur Evaluasi

Arsitektur yang diusulkan dievaluasi dari empat perspektif.

a. Evaluasi Fungsional menilai apakah pengguna dapat melakukan otentikasi sekali dan mengakses beberapa aplikasi kota pintar tanpa login berulang.
b. Evaluasi Interoperabilitas memeriksa kemampuan aplikasi heterogen untuk berkomunikasi dengan Penyedia Identitas terpusat menggunakan protokol otentikasi standar.
c. Evaluasi Kinerja mengukur latensi otentikasi, waktu respons, waktu penerbitan token, dan throughput sistem di bawah akses pengguna bersamaan. Pengujian beban dilakukan menggunakan beberapa pengguna virtual untuk menganalisis skalabilitas dan efisiensi otentikasi.
d. Evaluasi Keamanan menganalisis kepatuhan terhadap rekomendasi keamanan OAuth 2.0 dan OpenID Connect, termasuk manajemen token yang aman, komunikasi terenkripsi menggunakan HTTPS, kontrol akses berbasis peran, manajemen sesi, dan perlindungan terhadap serangan otentikasi umum seperti duplikasi kredensial, akses tidak sah, serangan pemutaran ulang, dan pembajakan sesi.

2.5. Alur Kerja Penelitian

Alur kerja penelitian secara keseluruhan dapat diringkas sebagai berikut:

a. Menganalisis tantangan otentikasi dalam sistem kota cerdas heterogen.
b. Mendefinisikan persyaratan fungsional dan keamanan.
c. Merancang arsitektur SSO terfederasi yang diusulkan.
d. Mengimplementasikan arsitektur menggunakan Keycloak, OAuth 2.0, dan OpenID Connect.
e. Mengintegrasikan aplikasi kota cerdas yang representatif.
f. Melakukan evaluasi fungsional, interoperabilitas, kinerja, dan keamanan.
g. Menganalisis hasil evaluasi untuk menentukan efektivitas dan skalabilitas arsitektur yang diusulkan.

Metodologi yang diusulkan menyediakan kerangka kerja sistematis untuk mengembangkan infrastruktur otentikasi yang aman, interoperabel, dan skalabel yang mampu mendukung ekosistem kota cerdas terintegrasi sambil mempertahankan kompatibilitas dengan layanan publik digital yang ada.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Implementasi Arsitektur SSO

Implementasi arsitektur Single Sign-On (SSO) dilakukan dengan menggunakan Keycloak sebagai *Identity Provider* (IdP) yang terintegrasi dengan beberapa aplikasi representatif dalam ekosistem kota cerdas. Aplikasi yang digunakan dalam pengujian meliputi portal e-Government, sistem perizinan, sistem layanan kesehatan, sistem pendidikan, dan sistem transportasi. Setiap aplikasi dikonfigurasi sebagai client OpenID Connect sehingga proses autentikasi pengguna tidak lagi dilakukan secara lokal pada masing-masing aplikasi, melainkan didelegasikan ke Keycloak sebagai pusat manajemen identitas.

Hasil implementasi menunjukkan bahwa seluruh aplikasi berhasil terhubung dengan Identity Provider dan mampu menggunakan token autentikasi yang diterbitkan melalui protokol OAuth 2.0 dan OpenID Connect (Tabel 1). Pengguna hanya perlu melakukan login satu kali pada salah satu aplikasi, kemudian dapat mengakses aplikasi lain yang terintegrasi tanpa harus memasukkan ulang kredensial. Kondisi ini menunjukkan bahwa arsitektur yang diusulkan mampu mengurangi fragmentasi identitas pengguna dan menyederhanakan proses autentikasi lintas layanan.

Tabel 1. Hasil Pengujian Integrasi Fungsional SSO

No	Aplikasi Kota Cerdas	Status Integrasi OIDC	Login Tunggal	Validasi Token	Role Mapping	Hasil Pengujian
1	Portal e-Government	Berhasil	Ya	Berhasil	Berhasil	Valid
2	Sistem Perizinan	Berhasil	Ya	Berhasil	Berhasil	Valid
3	Sistem Layanan Kesehatan	Berhasil	Ya	Berhasil	Berhasil	Valid
4	Sistem Pendidikan	Berhasil	Ya	Berhasil	Berhasil	Valid
5	Sistem Transportasi	Berhasil	Ya	Berhasil	Berhasil	Valid

3.2. Hasil Pengujian Pengalaman Pengguna

Pengujian pengalaman pengguna dilakukan dengan membandingkan jumlah proses login yang diperlukan pada pendekatan autentikasi konvensional dan pendekatan SSO. Pada pendekatan konvensional, pengguna harus login secara terpisah pada setiap aplikasi. Sebaliknya, pada pendekatan SSO, pengguna cukup melakukan satu kali login untuk mengakses seluruh aplikasi yang telah terintegrasi.

Tabel 2. Perbandingan Autentikasi Konvensional dan SSO

Skenario Pengujian	Jumlah Aplikasi Diakses	Jumlah Login Konvensional	Jumlah Login dengan SSO	Penurunan Login Berulang
Akses 2 aplikasi	2	2	1	50%
Akses 3 aplikasi	3	3	1	66,7%
Akses 4 aplikasi	4	4	1	75%
Akses 5 aplikasi	5	5	1	80%

Hasil pada Tabel 2 menunjukkan bahwa penggunaan SSO mampu mengurangi proses login berulang secara signifikan. Ketika pengguna mengakses lima aplikasi kota cerdas, jumlah proses login berkurang dari lima kali menjadi satu kali, atau mengalami penurunan sebesar 80%. Temuan ini menunjukkan bahwa SSO tidak hanya meningkatkan efisiensi akses, tetapi juga memperbaiki pengalaman pengguna karena pengguna tidak perlu mengingat banyak kombinasi username dan password pada berbagai sistem layanan publik.

Dari sisi administrasi sistem, pendekatan ini juga menyederhanakan pengelolaan akun pengguna. Administrator tidak perlu lagi membuat dan mengelola akun secara terpisah pada setiap aplikasi. Seluruh proses pengelolaan identitas, perubahan kata sandi, pengaturan peran, dan pencabutan akses dapat dilakukan secara terpusat melalui *Identity Provider*.

3.3. Hasil Pengujian Kinerja Autentikasi

Pengujian kinerja dilakukan untuk mengukur kemampuan arsitektur dalam menangani akses pengguna secara bersamaan. Pengujian dilakukan dengan beberapa skenario jumlah pengguna virtual, yaitu 10, 25, 50, 75, 100, 150, dan 200 pengguna. Parameter yang diukur meliputi waktu login rata-rata, waktu penerbitan token, waktu validasi token, throughput autentikasi, dan tingkat kesalahan sistem.

Tabel 3. Hasil Pengujian Kinerja Autentikasi SSO

Jumlah Pengguna Virtual	Waktu Login Rata-Rata (ms)	Waktu Penerbitan Token (ms)	Waktu Validasi Token (ms)	Throughput (request/detik)	Error Rate (%)
10	184	42	18	54,3	0,0
25	216	50	23	115,7	0,0
50	257	61	28	194,6	0,0
75	311	73	34	241,2	0,2
100	386	88	41	259,1	0,5
150	492	112	55	304,9	1,3
200	641	146	71	312,0	2,1

Berdasarkan Tabel 3, peningkatan jumlah pengguna virtual berdampak terhadap peningkatan waktu login rata-rata. Pada skenario 10 pengguna virtual, waktu login rata-rata tercatat sebesar 184 ms, sedangkan pada skenario 200 pengguna virtual meningkat menjadi 641 ms. Meskipun terjadi peningkatan latensi, nilai tersebut masih berada dalam kategori layak untuk sistem autentikasi layanan publik digital karena waktu respons tetap berada di bawah satu detik.

Waktu penerbitan token juga mengalami peningkatan seiring bertambahnya beban pengguna, yaitu dari 42 ms pada 10 pengguna virtual menjadi 146 ms pada 200 pengguna virtual. Hal yang sama terjadi pada waktu validasi token, yang meningkat dari 18 ms menjadi 71 ms. Peningkatan ini masih dapat diterima karena proses validasi token berbasis JWT relatif ringan dan tidak selalu memerlukan komunikasi langsung dengan basis data pengguna pada setiap permintaan layanan.

Throughput system meningkat secara bertahap seiring bertambahnya jumlah pengguna virtual. Pada skenario 10 pengguna, sistem mampu menangani 54,3 request per detik, sedangkan pada 200 pengguna virtual throughput meningkat

menjadi 312,0 request per detik. Hal ini menunjukkan bahwa arsitektur yang diusulkan memiliki kemampuan skalabilitas yang baik. Namun, peningkatan error rate mulai terlihat pada skenario 75 pengguna virtual dan mencapai 2,1% pada skenario 200 pengguna virtual. Error rate tersebut masih relatif rendah, tetapi menunjukkan perlunya optimasi tambahan apabila sistem akan diterapkan pada skala kota dengan jumlah pengguna aktif yang jauh lebih besar.

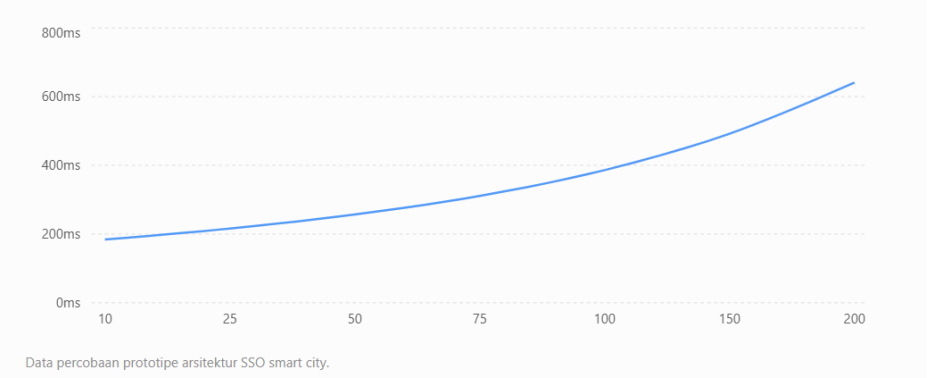
3.4. Hasil Pengujian Interoperabilitas

Pengujian interoperabilitas dilakukan untuk mengetahui kemampuan arsitektur SSO dalam mendukung aplikasi yang dikembangkan menggunakan platform teknologi berbeda. Dalam pengujian ini, aplikasi prototipe menggunakan kombinasi teknologi web dan API yang berbeda, tetapi seluruhnya menggunakan standar OpenID Connect untuk proses autentikasi.

Tabel 4. Hasil Pengujian Interoperabilitas Aplikasi

No	Aplikasi	Teknologi Aplikasi	Protokol Autentikasi	Format Token	Status Interoperabilitas
1	Portal e-Government	PHP/Laravel	OIDC	JWT	Berhasil
2	Sistem Perizinan	Node.js/Express	OIDC	JWT	Berhasil
3	Sistem Layanan Kesehatan	Java/Spring Boot	OIDC	JWT	Berhasil
4	Sistem Pendidikan	Python/Django	OIDC	JWT	Berhasil
5	Sistem Transportasi	RESTful API	OAuth 2.0	JWT	Berhasil

Hasil pengujian pada Tabel 4 menunjukkan bahwa arsitektur SSO yang diusulkan mampu mendukung integrasi lintas platform. Aplikasi yang dikembangkan menggunakan teknologi berbeda tetap dapat berkomunikasi dengan Identity Provider selama mengikuti standar protokol yang sama. Temuan ini penting dalam konteks kota cerdas karena sistem informasi pemerintahan biasanya dikembangkan oleh unit, vendor, atau instansi yang berbeda, sehingga heterogenitas teknologi hampir tidak dapat dihindari. Dengan menggunakan OAuth 2.0 dan OpenID Connect, integrasi autentikasi dapat dilakukan tanpa harus menyatukan seluruh basis data atau mengubah logika bisnis utama masing-masing aplikasi. Tren waktu login rata-rata dapat dilihat pada Gambar 3.



Gambar 3. Tren waktu login rata-rata berdasarkan jumlah pengguna virtual

3.5. Hasil Evaluasi Keamanan

Evaluasi keamanan dilakukan dengan menganalisis beberapa aspek utama, yaitu perlindungan kredensial, penggunaan token, komunikasi terenkripsi, kontrol akses berbasis peran, manajemen sesi, dan pencabutan akses. Hasil evaluasi menunjukkan bahwa arsitektur SSO mampu meningkatkan keamanan autentikasi dibandingkan pendekatan login terpisah pada setiap aplikasi.

Berdasarkan Tabel 5, arsitektur yang diusulkan memberikan peningkatan keamanan melalui pemusatan autentikasi dan pengelolaan akses. Pada pendekatan konvensional, setiap aplikasi menyimpan dan memproses kredensial pengguna secara mandiri sehingga memperbesar permukaan serangan. Dalam arsitektur SSO, kredensial pengguna hanya diproses oleh Identity Provider, sedangkan aplikasi layanan hanya menerima token yang telah divalidasi. Dengan demikian, risiko kebocoran kredensial akibat lemahnya keamanan pada salah satu aplikasi dapat dikurangi.

Tabel 5. Evaluasi Aspek Keamanan Arsitektur SSO

No	Aspek Keamanan	Mekanisme yang Digunakan	Hasil Evaluasi
1	Perlindungan kredensial	Kredensial hanya diproses oleh Keycloak	Risiko paparan kredensial berkurang
2	Komunikasi aman	HTTPS/TLS	Pertukaran data terenkripsi
3	Token akses	JWT access token	Validasi akses berjalan efisien
4	Token refresh	Refresh token dengan masa berlaku terbatas	Sesi dapat diperpanjang secara terkendali
5	Kontrol akses	Role-Based Access Control	Hak akses dapat dibedakan antarperan
6	Manajemen sesi	Centralized session management	Logout terpusat dapat diterapkan
7	Pencabutan akses	Revocation dan user disable	Akses pengguna dapat dihentikan dari pusat
8	Risiko login berulang	Satu kali autentikasi	Duplikasi kredensial berkurang

Selain itu, penggunaan role-based access control memungkinkan pembatasan akses berdasarkan peran pengguna. Misalnya, warga hanya dapat mengakses layanan publik, operator hanya dapat mengelola data layanan tertentu, sedangkan administrator memiliki hak akses yang lebih luas sesuai kewenangannya. Mekanisme ini penting untuk memastikan bahwa integrasi sistem tidak menyebabkan perluasan akses yang tidak terkendali.

3.6. Pembahasan

Hasil pengujian menunjukkan bahwa arsitektur Single Sign-On yang diusulkan mampu menjawab permasalahan utama pada sistem informasi kota cerdas, yaitu fragmentasi identitas, redundansi proses login, kompleksitas administrasi pengguna, dan keterbatasan interoperabilitas antar aplikasi. Dengan memanfaatkan Keycloak sebagai Identity Provider, proses autentikasi dapat dipusatkan tanpa menghilangkan independensi masing-masing aplikasi layanan publik.

Dari perspektif fungsional, arsitektur ini berhasil memungkinkan pengguna melakukan autentikasi satu kali dan mengakses beberapa aplikasi yang terintegrasi. Hal ini memperlihatkan bahwa model federated identity management dapat menjadi solusi praktis untuk ekosistem kota cerdas yang memiliki banyak layanan digital. Pendekatan ini juga memberikan manfaat langsung bagi pengguna karena proses akses menjadi lebih sederhana, cepat, dan konsisten.

Dari perspektif kinerja, hasil pengujian menunjukkan bahwa peningkatan jumlah pengguna virtual menyebabkan peningkatan latensi autentikasi. Namun, peningkatan tersebut masih berada dalam batas yang dapat diterima. Pada beban 200 pengguna virtual, waktu login rata-rata sebesar 641 ms masih tergolong responsif untuk sistem layanan publik digital. Selain itu, throughput yang terus meningkat menunjukkan bahwa arsitektur memiliki kemampuan menangani beban akses secara paralel. Meskipun demikian, munculnya error rate sebesar 2,1% pada beban tertinggi menunjukkan bahwa implementasi skala besar tetap memerlukan strategi optimasi, seperti load balancing, clustering Keycloak, caching token, optimasi basis data PostgreSQL, serta penggunaan reverse proxy untuk distribusi beban.

Dari perspektif interoperabilitas, penggunaan OAuth 2.0 dan OpenID Connect terbukti memudahkan integrasi aplikasi yang dibangun dengan teknologi berbeda. Hal ini sangat relevan dalam implementasi kota cerdas karena aplikasi layanan publik umumnya tidak dibangun dalam satu waktu, satu platform, atau satu vendor. Dengan standar protokol terbuka, aplikasi lama maupun baru dapat diintegrasikan secara bertahap ke dalam sistem autentikasi terpadu. Pendekatan ini lebih realistis dibandingkan membangun ulang seluruh sistem dari awal, karena pemerintah dapat mempertahankan investasi teknologi yang sudah ada.

Dari perspektif keamanan, arsitektur SSO meningkatkan pengendalian akses melalui pemusatan identitas, validasi token, enkripsi komunikasi, dan pengelolaan peran. Pengurangan penyimpanan kredensial pada masing-masing aplikasi menjadi salah satu keuntungan penting karena dapat mengurangi risiko kebocoran data autentikasi. Selain itu, mekanisme token berbasis JWT memungkinkan aplikasi melakukan validasi akses secara efisien, sementara refresh token dan session management memberikan kontrol lebih baik terhadap durasi sesi pengguna.

Dari hasil penelitian ini menunjukkan bahwa arsitektur SSO berbasis Keycloak, OAuth 2.0, dan OpenID Connect layak digunakan sebagai kerangka autentikasi untuk sistem informasi kota cerdas terintegrasi. Arsitektur ini tidak hanya meningkatkan kenyamanan pengguna, tetapi juga memperkuat tata kelola identitas digital, meningkatkan interoperabilitas layanan, serta menyediakan dasar keamanan yang lebih baik untuk pengembangan ekosistem smart city yang berkelanjutan. Beberapa dari penelitian ini masih memiliki beberapa keterbatasan. Pengujian dilakukan pada lingkungan prototipe dengan jumlah pengguna virtual yang terbatas, sehingga hasilnya belum sepenuhnya merepresentasikan kondisi produksi pada skala kota besar. Selain itu, aspek keamanan yang diuji masih berfokus pada evaluasi konfigurasi dan skenario autentikasi umum,

belum mencakup uji penetrasi mendalam terhadap seluruh komponen sistem. Penelitian selanjutnya dapat memperluas evaluasi dengan menerapkan Keycloak clustering, integrasi multi-realm antar instansi, pengujian high availability, serta evaluasi keamanan menggunakan penetration testing dan threat modeling yang lebih komprehensif.

4. KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan evaluasi yang telah dilakukan, arsitektur Single Sign-On (SSO) berbasis Keycloak, OAuth 2.0, dan OpenID Connect terbukti mampu mendukung integrasi sistem informasi kota cerdas secara aman, terpusat, dan interoperabel. Arsitektur yang diusulkan memungkinkan pengguna melakukan autentikasi satu kali untuk mengakses berbagai aplikasi layanan publik, sehingga dapat mengurangi redundansi login, menyederhanakan pengelolaan identitas, serta meningkatkan pengalaman pengguna. Hasil pengujian menunjukkan bahwa seluruh aplikasi prototipe berhasil terintegrasi dengan Identity Provider, validasi token berjalan dengan baik, dan sistem tetap menunjukkan kinerja yang stabil pada skenario akses pengguna bersamaan. Selain itu, penggunaan autentikasi berbasis token, komunikasi terenkripsi, manajemen sesi terpusat, dan kontrol akses berbasis peran memberikan peningkatan keamanan dibandingkan mekanisme autentikasi terpisah pada masing-masing aplikasi. Dengan demikian, arsitektur SSO yang diusulkan dapat menjadi kerangka referensi yang layak diterapkan dalam pengembangan ekosistem smart city yang terintegrasi, skalabel, aman, dan berorientasi pada kemudahan layanan publik.

DAFTAR PUSTAKA

[1] S. Wijayasinghe and V. Sachitra, "Smart city development and improvement of quality of life in urban cities of Sri Lanka: citizen-centric approach," *JGR*, vol. 16, no. 3, pp. 431–450, Jun. 2025, doi: 10.1108/JGR-02-2024-0027.

[2] K. Paskaleva and I. Cooper, "Have European 'smart cities' initiatives improved the quality of their citizens' lives?," *Proceedings of the Institution of Civil Engineers - Urban Design and Planning*, vol. 175, no. 3, pp. 138–151, Aug. 2022, doi: 10.1680/jurdp.22.00013.

[3] S. R. Sedita, A. Alberton, M. Pioletti, and K. Crespi Gomes, "A life cycle perspective on smart city innovation ecosystem: the case of Florianopolis," *Applied Geography*, vol. 191, p. 104015, Jun. 2026, doi: 10.1016/j.apgeog.2026.104015.

[4] P. G. Oliver, L. Mora, and J. Zhang, "Collaboration before competition: How smart city entrepreneurs co-create temporary ecosystems to build capacity for learning," *Technological Forecasting and Social Change*, vol. 214, p. 124046, May 2025, doi: 10.1016/j.techfore.2025.124046.

[5] M. Tanveer, K. Toor, A. G. Alharbi, and S. R. Hassan, "SecTwin: A secure and efficient authentication mechanism for vehicular digital twins," *Journal of Information Security and Applications*, vol. 95, p. 104292, Dec. 2025, doi: 10.1016/j.jisa.2025.104292.

[6] W. Son, S. Kwon, and J.-H. Lee, "A DID-based one-time session key authentication mechanism for secure human-AI chatbot communication," *Computers and Electrical Engineering*, vol. 127, p. 110622, Oct. 2025, doi: 10.1016/j.compeleceng.2025.110622.

[7] Y. Wang, P. Castillejo, J.-F. Martínez-Ortega, and V. Hernández Díaz, "A survey on Identity and Access Management for future IoT services," *Computer Networks*, vol. 272, p. 111718, Nov. 2025, doi: 10.1016/j.comnet.2025.111718.

[8] A. Wairagade and S. Ranjan, "AI in Identity and Access Management (IAM) for Enterprise Systems: A Comparative Analysis," *Procedia Computer Science*, vol. 263, pp. 167–174, 2025, doi: 10.1016/j.procs.2025.07.021.

[9] A. Zineddine, Y. Belfaik, A. Rehaimi, Y. Sadqi, and S. Safi, "Single Sign-On Security and Privacy: A Systematic Literature Review," *CMC*, vol. 84, no. 3, pp. 4019–4054, 2025, doi: 10.32604/cmc.2025.066139.

[10] D. Mortágua, A. Zúquete, and P. Salvador, "Enhancing 802.1X authentication with identity providers using EAP-OAUTH and OAuth 2.0," *Computer Networks*, vol. 244, p. 110337, May 2024, doi: 10.1016/j.comnet.2024.110337.

[11] G. Sassetti, A. Sharif, G. Sciarretta, R. Carbone, and S. Ranise, "Best current practices for privacy-preserving OpenID Connect: A study of their adoption in the wild," *Computers & Security*, vol. 168, p. 104934, Sep. 2026, doi: 10.1016/j.cose.2026.104934.

[12] H. Lim and S. Jin, "Are frictionless experiences always beneficial? Customer loyalty consequences of Single Sign-On (SSO) onboarding," *Journal of Retailing and Consumer Services*, vol. 92, p. 104804, Jun. 2026, doi: 10.1016/j.jretconser.2026.104804.

[13] Mauladi, T. Suratno, E. Saputra, K. Pamungkas, and R. Yahyapour, "Keycloak-SSI: A Keycloak extension for SSI-based user-controlled attribute verification in federated identity management flows," *Software Impacts*, vol. 29, p. 100846, Sep. 2026, doi: 10.1016/j.simpa.2026.100846.

[14] L. F. B. Xavier, A. P. H. G. D. A. Lima, and F. H. Taques, "Evaluation of Brazilian cities from the perspective of smart cities: An analysis of cluster and information technology initiatives," *Urban Governance*, vol. 5, no. 3, pp. 293–302, Sep. 2025, doi: 10.1016/j.ugj.2025.08.004.

[15] M. A. Fadhel *et al.*, "Comprehensive systematic review of information fusion methods in smart cities and urban environments," *Information Fusion*, vol. 107, p. 102317, Jul. 2024, doi: 10.1016/j.inffus.2024.102317.