JSiI | Jurnal Sistem Informasi
Vol.10 No.1 Maret 2023, Hal.41-49

DOI: 10.30656/jsii.v10i1.6186
p-ISSN: 2406-7768
e-ISSN: 2581-2181

# EVALUASI PENERAPAN SINGLE SIGN-ON SAML DAN OAUTH 2.0: STUDI PADA PERGURUAN TINGGI YOGYAKARTA

**Salmuasih[1], Mukhammad Andri Setiawan[2]**

*[1,2] Jurusan Teknik Informatika Fakultas Teknik Industri Universitas Islam Indonesia*
*Jl. Kaliurang No.Km. 14,5, Sleman, Yogyakarta 55584*

[1]18917127 @students.uii.ac.id

[2]andri@uii.ac.id

**Abstrak**

Dalam memutuskan strategi *Single Sign-On* (SSO) yang efektif, perguruan tinggi perlu memahami manfaat SSO, mengidentifikasi kebutuhan spesifik organisasi, dan memilih protokol yang akan memenuhi kebutuhan tersebut. Kontribusi penelitian ini adalah menganalisis efektifitas penerapan SSO protokol SAML dan OAuth 2.0 pada perguruan tinggi Yogyakarta. Langkah penelitian meliputi pengumpulan data, kemudian melakukan analisis penerapan protokol SAML dan OAuth 2.0 terhadap referensi yang relevan. Pengumpulan data dilakukan melalui literatur review, observasi pada domain-domain website resmi perguruan tinggi, survei, dan wawancara kepada 22 responden dari 17 Pusat IT perguruan tinggi. Dari hasil survei dan wawancara ditemukan ketidaksesuaian penerapan protokol pada 7 perguruan tinggi yang mengintegrasikan aplikasi *native* (*desktop-based*/*mobile-based*) dan IoT menggunakan SAML dan juga ditemukan ketidaksesuaian penerapan protokol yaitu OAuth 2.0 pada 2 perguruan tinggi. Hasil analisis menunjukkan bahwa beberapa perguruan tinggi belum menerapkan SSO secara efektif. Meskipun 60% perguruan tinggi mengklaim telah melakukan riset dalam pemilihan protokol SSO yang digunakan, namun pada praktiknya masih dijumpai penerapan SSO yang justru menambah kompleksitas permasalahan sebelumnya.

**Kata kunci***:* evaluasi, oauth 2.0, perguruan tinggi, saml, single sign-on

## I. PENDAHULUAN

Menurut *press release* Gartner pada April 2021, selama pandemi Covid-19 migrasi dari *on-premises* ke *cloud* mengalami pertumbuhan yang signifikan. Kebutuhan industri dan akademik terhadap layanan cloud terus meningkat, terutama pada model layanan *Software-as-a-Service* (SaaS) yang menjadi segmen pasar terbesar, disusul *Platform-as-a-Service* (PaaS) dan *Infrastructure-as-a-Service* (IaaS). Sebagai contoh di perguruan tinggi, proses belajar mengajar yang semula tatap muka beralih ke *platform online*, memanfaatkan berbagai aplikasi *Learning Management System* (LMS) dan *online meeting* seperti Zoom, Google Meet, Microsoft Teams, dan Cisco Webex Meeting [1]. Selain SaaS, perguruan tinggi juga masih menggunakan aplikasi pada infrastruktur *on-premises*, dimana sebagian besar *monolith* dan menggunakan *role-based access control* (RBAC) [2]. Dengan semakin banyaknya aplikasi dan sumber daya yang tersedia untuk pengajar, staf, dan mahasiswa, penyediaan akses yang *seamless* menjadi semakin penting. *Single Sign-On* (SSO) dapat menjadi salah satu solusi untuk mengintegrasikan sistem yang dimiliki perguruan tinggi [3].

SSO menyediakan tempat terpusat untuk mengakses semua aplikasi dan sumber daya dengan satu *username* dan *password*. Manajemen identitas yang terpusat pada SSO meminimalisir kesalahan dan kelalaian pemberian/pencabutan hak akses pengguna pada sistem tertentu. SSO mengizinkan Penyedia Identitas (*Identity Provider* - IdP) untuk berbagi informasi autentikasi dan otorisasi dengan Penyedia Layanan (*Service Provider* - SP). Autentikasi digunakan untuk membuktikan bahwa pengguna yang hendak *login* benar-benar pemilik akun yang sah. Metode autentikasi diantaranya menggunakan *login* kredensial, autentikasi multifaktor, autentikasi pihak ketiga, *password* teks sederhana, objek *password* 3D, *password* grafis, autentikasi biometrik, dan autentikasi perangkat digital. Proses otorisasi memutuskan aplikasi apa yang diizinkan untuk tampil pada sistem identitas sesuai hak akses pengguna yang diautentikasi [4]. *Security Assertion Markup Language* (SAML) dan *Open Authentication* (OAuth) 2.0 merupakan protokol SSO yang populer digunakan [4]. Kedua protokol tersebut memiliki standar spesifikasi tersendiri. SAML dengan standar XML dapat digunakan untuk autentikasi dan otorisasi pengguna,


Received: February 6th, 2023 | Published: March 22nd, 2023

DOI: 10.30656/jsii.v10i1.6186
p-ISSN: 2406-7768
e-ISSN: 2581-2181

sementara OAuth 2.0 digunakan untuk memberikan otorisasi dari satu layanan ke layanan lainnya [5].

Untuk memutuskan strategi SSO yang efektif, perguruan tinggi perlu memahami manfaat SSO, mengidentifikasi kebutuhan spesifik organisasi, dan memilih protokol/layanan yang akan memenuhi kebutuhan tersebut. Pemanfaatan SAML dan OAuth 2.0 masing-masing menyesuaikan kasus yang terjadi [6]. SAML memungkinkan domain web bertukar data dengan aman [7]. Universitas Kyushu memanfaatkan SSO Shibboleth yang berbasis SAML untuk tujuan *security* dan *usability*. Kategori *security* berlaku untuk *service* terkait data penelitian dan nilai mahasiswa, sedangkan kategori *usability* berlaku untuk layanan email dan *wireless* LAN [8]. SAML juga digunakan untuk berbagi akses antarinstitusi (kolaborasi) terhadap data, instrumen penelitian, kluster komputasi [9], mengintegrasikan layanan *online meeting* seperti Zoom, layanan LMS seperti Moodle [10], dan teknologi pendukung pengajaran lainnya [11]. Integrasi menggunakan SSO SAML memungkinkan *user login* sekali menggunakan akun resmi perguruan tinggi untuk mengakses semua teknologi yang tersedia dan diizinkan.

OAuth 2.0 mengandalkan format data JSON, yang lebih menyederhanakan integrasi dengan aplikasi modern. Salah satu ekstensi penting OAuth 2.0 adalah fleksibilitasnya terhadap lingkungan *runtime*. Hal ini memungkinkan integrasi OAuth 2.0 dengan aplikasi *native* pada perangkat *mobile* dan IoT [7]. Pada beberapa perguruan tinggi akses ke LMS dilakukan menggunakan OAuth 2.0, yaitu dengan mengotorisasi via jejaring sosial seperti Twitter, Facebook, dan Yahoo. Hal ini memudahkan dosen, administrator, dan mahasiswa untuk berkolaborasi tanpa perlu membuat akun baru pada LMS [12] [13]. OAuth 2.0 juga dimanfaatkan untuk mengintegrasikan perangkat IoT pada perguruan tinggi [14], seperti IoT-*based Smart classroom*, IoT-*based Smart lab*, dan IoT-*based Smart campus* [15].

Dari contoh penggunaan diatas, tidak semua solusi SSO cocok untuk diimplementasikan pada sebuah perguruan tinggi. Pemilihan solusinya perlu mempertimbangkan kondisi infrastruktur, kebutuhan aplikasi, dan seberapa banyak upaya yang diperlukan. Pada penerapannya, memungkinan adanya gap antara kebutuhan organisasi dengan protokol SSO yang dipilih. Penelitian ini akan mengevaluasi penerapan SSO SAML dan OAuth 2.0 terhadap kebutuhan perguruan tinggi. Hal ini dimaksudkan untuk melihat efektifitas dan kesesuaian protokol SSO yang dipilih/diterapkan, sehingga setiap fitur dari kedua protokol SAML dan OAuth 2.0 dapat dimanfaatkan dengan optimal.

## II. METODOLOGI PENELITIAN

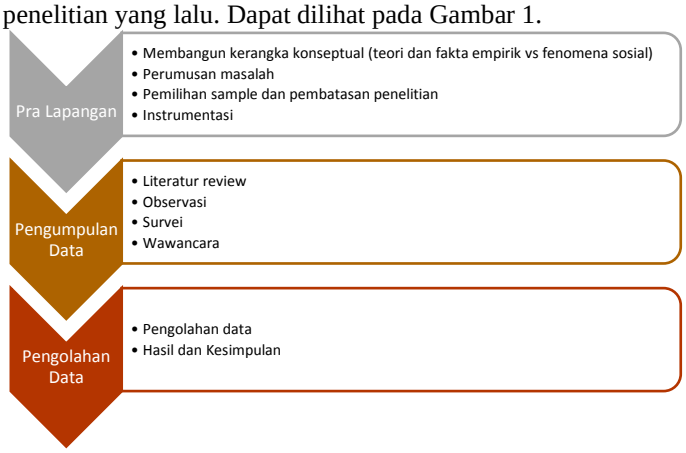
### A. *Pendekatan Penelitian*

Untuk memahami tantangan yang dihadapi oleh perguruan tinggi saat mengimplementasikan solusi SSO, penting untuk berinteraksi, memahami, dan menganalisis wawasan orang yang bekerja di platform tersebut. Berdasarkan penelitian sebelumnya terkait SSO, memberikan wawasan tentang metode dan analisis pengumpulan data. Penelitian ini akan menggunakan metode kualitatif untuk pengumpulan data. Metode pengumpulan data kualitatif melibatkan wawancara individu, survei, observasi, dan literatur *review*. Survei dan wawancara dengan narasumber personil Pusat IT perguruan tinggi di Yogyakarta akan dilakukan secara *online*.

Sebelum melakukan survei dan wawancara, penulis telah melakukan observasi pada domain website resmi beberapa perguruan tinggi di Yogyakarta untuk melihat domain-domain aplikasi yang telah diintegrasikan dengan SSO. Selain itu, penulis juga meninjau berbagai penelitian yang telah dilakukan sebelum penelitian ini dan menganalisis hasil dan keluaran dari penelitian tersebut. Survei dan wawancara akan dilakukan pada perguruan tinggi yang sudah mengimplementasikan solusi SSO, maupun yang belum atau berencana menerapkan beberapa bentuk solusi SSO. Hal ini dimaksudkan untuk memberikan lebih banyak wawasan tentang tantangan yang harus dilalui perguruan tinggi dalam memilih solusi yang tepat.

Survei dan wawancara adalah sumber data utama untuk penelitian yang diusulkan. Selain untuk membandingkan implementasi protokol SAML dan OAuth 2.0, survei dan wawancara dapat menjadi pedoman yang dapat dipertimbangkan saat menerapkan SSO. Pertanyaan survei dan wawancara lebih difokuskan pada kebutuhan organisasi, penerapan SSO yang telah dilakukan, dan tantangan yang dihadapi dengan solusi tersebut. Pertanyaan-pertanyaan ini dimaksudkan untuk menganalisis keadaan yang berbeda di dalam perguruan tinggi sebelum membuat kesimpulan.

Survei dan wawancara yang akan dilakukan juga akan memiliki pertanyaan yang terkait infrastruktur organisasi serta keefektifan solusi SSO untuk menjawab permasalahan organisasi. Tanggapan yang diperoleh dari survei dan wawancara dibandingkan dengan spesifikasi dan *business case* SSO SAML dan OAuth 2.0 di perguruan tinggi pada penelitian yang lalu. Dapat dilihat pada Gambar 1.




**Gambar 1.** Kerangka Penelitian


Received: February 6th, 2023 | Published: March 22nd, 2023

DOI: 10.30656/jsii.v10i1.6186
p-ISSN: 2406-7768
e-ISSN: 2581-2181

Kerangka metodologi tinjauan pustaka dimotivasi dan diadaptasi dari karya Vom Brocke et al. [16]. Kerangka kerja ini dilakukan dalam rangkaian 5 fase yang bersifat siklik. Tahapannya adalah sebagai berikut: definisi ruang lingkup review, konseptualisasi topik penelitian, pencarian literatur, analisis literatur yang diperoleh dan penentuan agenda penelitian. Penjelasan rinci tentang bagaimana tinjauan literatur dilakukan pada setiap fase dijelaskan pada sub-bagian berikut

*B. Definisi Ruang Lingkup Review*

Ruang lingkup kajian pustaka adalah:

1. Untuk mempelajari protokol yang populer digunakan dalam sistem manajemen identitas (SAML dan OAuth 2.0) dan membuat analisis komparatif untuk menjelaskan perbedaan fiturnya.
2. Untuk mempelajari *business case* SAML dan OAuth 2.0 pada perguruan tinggi.

*C. Konseptualisasi Topik Penelitian*

Untuk memulai topik penelitian, dilakukan pencarian literatur untuk menemukan artikel dengan menggunakan istilah-istilah kunci yang relevan. Istilah kunci awal yang digunakan untuk pencarian adalah sebagai berikut: SAML, OAuth2, *Identity and Access Management, Single Sign-On, Authentication, Authorization*, perguruan tinggi. Studi pendahuluan dari artikel ini digunakan untuk membantu menurunkan istilah kunci yang lebih luas seperti *business case* SAML pada perguruan tinggi, *business case* OAuth2 pada perguruan tinggi, IMS, *on-premises*, lingkungan multi/hibrid, autentikasi SAML

*D. Pencarian Literatur*

Kata kunci di atas dicari pada *database* yang diterbitkan, menggunakan kriteria pencarian khusus untuk menemukan artikel yang relevan, ditunjukkan pada Tabel 1.

**Tabel 1.** Kriteria pencarian dan database yang digunakan

| Kriteria Pencarian | Database |
|---|---|
| Artikel yang diterbitkan pada: | Google Scholar |
| - Jurnal, Conference, website dan buku | ACM digital library |
| - Rentang waktu antara 2016-2022 | Science Direct |

Artikel hasil pencarian kemudian dipelajari berdasarkan judul, abstrak dan kesimpulan. Jika artikel cukup sesuai, maka dilakukan pencarian lebih lanjut berdasarkan kutipan dan referensi yang digunakan dalam artikel tersebut. Penelitian terkait implementasi protokol SSO SAML dan OAuth 2.0 pada perguruan tinggi terdiri dari: (1) kolaborasi dan federasi, (2) integrasi dengan sistem berbasis web pada perguruan tinggi, (3) integrasi dengan perangkat IoT dan aplikasi *native*, (4) perbandingan fitur. Tabel 2 menunjukkan jumlah artikel yang dicari dan digunakan dalam penelitian.

**Tabel 2**. Topik dan jumlah artikel yang digunakan

| Topik | Jumlah artikel |
|---|---|
| Perbandingan fitur SAML dan OAuth 2.0 | 6 |
| Implementasi SAML pada perguruan tinggi | 6 |
| Implementasi OAuth 2.0 pada perguruan tinggi | 7 |

*E. Analisis Literatur yang Diperoleh*

1. Perbandingan fitur SAML dan OAuth 2.0

Integrasi pada lingkungan domain yang berbeda memerlukan protokol autentikasi standar untuk membangun komunikasi yang aman antara pihak yang terlibat. Bagian ini menyajikan analisis komparasi fitur protokol SSO yaitu SAML dan OAuth 2.0 [17] seperti yang ditunjukkan pada Tabel 3. Dari analisis ini disimpulkan bahwa SAML memiliki keterbatasan pada perangkat mobile dan IoT. OAuth 2.0 merupakan protokol otorisasi yang mengizinkan delegasi akses, tidak untuk kebutuhan autentikasi. OAuth 2.0 dapat digunakan untuk autentikasi dengan beberapa fitur tambahan (seperti analogi lemari es dengan *freezer* tambahan). OIDC adalah spesifikasi dari fitur ini. OIDC telah dikembangkan untuk memberikan layanan untuk web, *cloud*, perangkat *mobile*, dan IoT.

**Tabel 3.** Perbandingan fitur SAML dan OAuth 2.0

| Fitur | SAML | OAuth 2.0 | Sumber |
|---|---|---|---|
| ***Authentication*** | ✓ | | [6] [17] [4] [18] [3] |
| ***Authorization*** | ✓ | ✓ | |
| ***Access Delegation*** | | ✓ | |
| ***Support Web App*** | ✓ | ✓ | |
| ***Support Native Mobile App*** | | ✓ | |
| ***Mobile Standard (IoT)*** | | ✓ | |
| ***Flexibility (ease of use)*** | | ✓ | |


Received: February 6th, 2023 | Published: March 22nd, 2023

DOI: 10.30656/jsii.v10i1.6186
p-ISSN: 2406-7768
e-ISSN: 2581-2181

| | | | |
|---|---|---|---|
| ***Interoperability*** | ✓ | ✓ | |
| ***Single Sign-On*** | ✓ | | |
| ***Single Logout*** | ✓ | ✓ | |
| ***Attribute/ Claims*** | ✓ | | |
| ***Federation*** | ✓ | | |
| ***Extensibility*** | ✓ | ✓ | |
| ***Open Standard*** | ✓ | ✓ | |

2. Implementasi SAML pada perguruan tinggi

Dalam pengaturan paling dasar (dan paling populer), SAML memungkinkan pertukaran informasi tentang pengguna antara IdP dan SP melalui *browser* pengguna (User Agent). Hal ini tidak memerlukan koneksi langsung antara IdP dan SP – semuanya terjadi melalui *redirect browser*. Pengguna meminta dokumen yang ditandatangani yang mengonfirmasi identitas mereka dari IdP, diautentikasi, dan kemudian mengirimkan dokumen yang ditandatangani ke SP untuk *login*. Dokumen yang ditandatangani juga dapat menyertakan informasi tentang *privileges* pengguna, grup, dll [17].

SAML digunakan untuk menyediakan pusat manajemen identitas dan mengintegrasikan *resource* pada perguruan tinggi, terutama yang berbasis web. Universitas Aristotle sudah menggunakan SSO berbasis SAML untuk mengautentikasi *user* pada berbagai aplikasi web, seperti Moodle dan Zoom [10]. West University of Timişoara juga mengintegrasikan teknologi SaaS yang terdiri dari Google Workspace, Office 365, h5p, Cisco Webex, *anti-plagiarism platform* Turnitin, dan Moodle untuk mendukung kurikulum digital [11].

Kolaborasi ilmiah menyatukan peneliti dan infrastruktur lintas institusi akademik, penyedia layanan *cloud*, dan batas internasional. Meski demikian, pada prakteknya sering terbatas pada mekanisme autentikasi dan otorisasi. Ketersediaan federasi identitas, memungkinkan peneliti mengakses infrastruktur siber menggunakan kredensial yang telah dimiliki, tanpa harus membuat kredensial baru [9]. SAML banyak digunakan pada perguruan tinggi untuk berkolaborasi antarinstitusi di berbagai negara. Universitas Kyushu menggunakan Shibboleth untuk berkolaborasi dalam federasi akademik GakuNin[8]. CILogon dibangun di atas perangkat lunak Shibboleth dan COmanage *open source* menyediakan platform IAM terintegrasi untuk sains, yang digabungkan ke seluruh dunia melalui eduGAIN. CILogon melayani kebutuhan unik kolaborasi penelitian, yaitu untuk secara dinamis membentuk grup kolaborasi lintas organisasi dan negara [9].

3. Implementasi OAuth 2.0 pada perguruan tinggi

OAuth biasanya digunakan untuk mendelegasikan akses ke sesuatu. Kita dapat memperbolehkan seseorang untuk "bertindak" sebagai kita. Pada kasus otorisasi antaraplikasi, OAuth digunakan untuk memberikan akses ke API yang dapat melakukan sesuatu sebagai akun kita [17]. Manajemen identitas adalah salah satu masalah IoT karena praktik keamanan yang buruk sering diterapkan. Sebagai contoh, penggunaan *clean textual content*/Base64 *encoded* IDs/*passwords with gadgets* dan *machine-to-machine* (M2M) adalah kesalahan umum yang harus diganti dengan *controlled token* seperti JSON Web Tokens (JWT) [14].

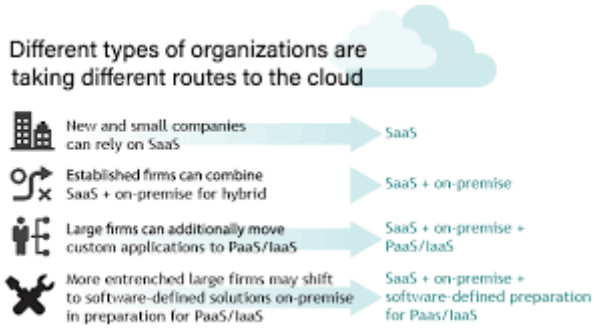
Perguruan tinggi memiliki berbagai macam *resource* yang sebagian ataupun keseluruhannya diintegrasikan menggunakan OAuth 2.0 [19] [7] [13], karena dinilai lebih fleksibel [17] dan mendukung integrasi aplikasi *native* [7] serta perangkat IoT [19] [15] [20]. Perangkat IoT yang digunakan pada perguruan tinggi terus bertambah, karena mobilitas, skalabilitas, dan kemudahan penggunaan. IoT pada sektor akademik diantaranya IoT-*based Smart classroom*, IoT-*based Smart lab*, dan IoT-*based Smart Campus* [15]. Studi kasus kampus digital di Jepang memiliki platform yang terdiri dari tablet PC untuk setiap mahasiswa, akses ke jaringan Wi-Fi, LMS, groupware, SNS, data *opensource* terbaru, berbagai kursus *online* gratis yang tersedia secara global, jam tangan, dan kacamata pintar. Akses ke semua platform pendidikan dan kesehatan tersebut dilakukan menggunakan otorisasi OAuth 2.0 [19].

4. Implementasi *Identity Access Management* (IAM) dan SSO pada organisasi secara umum

Menurut IDC OPINION, semakin besar organisasi dan semakin teregulasi industrinya, semakin besar kemungkinan perusahaan memiliki sistem IAM *on-premises*. Singkatnya, pengguna organisasi berada pada tahap adopsi *cloud* dan implementasi IAM yang berbeda, seperti pada Gambar 2. Banyak yang memiliki sistem dan *software on-premises*, dalam waktu yang bersamaan juga menggunakan SaaS, PaaS atau IaaS. Beberapa terhubung dengan mitra dan pelanggan dalam skenario B2B dan B2C. Organisasi lainnya memiliki lingkungan SaaS murni, namun ingin menambahkan autentikasi yang kuat, SSO, dan perlindungan data, termasuk perluasan bisnis ke *social identity* [21].

 Received: February 6th, 2023 | Published: March 22nd, 2023

DOI: 10.30656/jsii.v10i1.6186
p-ISSN: 2406-7768
e-ISSN: 2581-2181




**Gambar 2**. Pemanfaatan cloud pada berbagai level organisasi [21]

### *F. Penetapan Agenda Penelitian*

Berdasarkan analisis tinjauan pustaka, dapat dirangkum beberapa poin penting dalam implementasi SAML dan OAuth 2.0 di lingkungan *on-premises* dan *cloud*. Penelitian-penelitian tersebut mencakup analisis komparasi fitur protokol SSO yaitu SAML dan OAuth 2.0, serta teknis integrasi dengan aplikasi *on-premises* dan integrasi dengan aplikasi SaaS. Terkait implementasinya pada perguruan tinggi, SAML dan OAuth 2.0 banyak digunakan untuk mengintegrasikan berbagai *resource* yang dimiliki perguruan tinggi agar aksesnya *seamless*, meskipun digunakan pada perangkat yang beragam. Fokus utamanya ada pada *usability*, baru kemudian *security*.

Penelitian ini akan mengevaluasi implementasi SSO protokol SAML dan OAuth 2.0 pada perguruan tinggi di Yogyakarta dan mengidentifikasi keterbatasan yang dimiliki oleh perguruan tinggi yang belum memanfaatkan SSO.

## III. HASIL DAN PEMBAHASAN

### *A. Klasifikasi Perguruan Tinggi*

Klasifikasi perguruan tinggi ditentukan berdasarkan infrastruktur organisasi. Praktik yang direkomendasikan untuk diikuti dapat bervariasi berdasarkan klasifikasi dan kebutuhan perguruan tinggi. Klasifikasi perguruan tinggi dikelompokkan menjadi kecil, sedang, dan besar berdasarkan jumlah aplikasi yang dimiliki [22]:

a. Kecil, jumlah aplikasi kurang dari 50
b. Sedang, jumlah aplikasi kurang dari 150 dan lebih dari 50
c. Besar, jumlah aplikasi lebih dari 150

Arsitektur dalam suatu organisasi dapat dikategorikan berdasarkan:

a. *On-premises*
b. *Cloud*
c. Hibrid

Arsitektur tersebut meningkatkan kompleksitas pengelolaan pengguna karena meningkatnya risiko privasi dan keamanan. Kompleksitasnya dikelompokkan berdasarkan variasi *resource* yang dikelola, termasuk jika terdapat aplikasi *legacy* dan SaaS yang dikelola akan menambah kompleksitas arsitektur perguruan tinggi. Kompleksitas pengelolaan *resource* perguruan tinggi pada penelitian ini terbagi menjadi:

a. Sederhana, jika mengelola minimal 1 sampai 2 jenis *resource*
b. Sedang, jika mengelola 3 sampai 4 jenis *resource*
c. Kompleks, jika mengelola lebih dari 4 jenis *resource*

### *B. Proses Analisis Data*

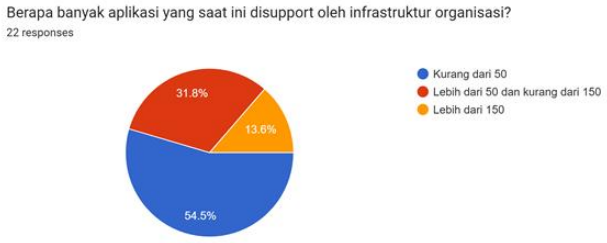
Kuesioner terdiri dari 37 pertanyaan yang dibagi menjadi 3 (tiga) kategori, yaitu (1) Identifikasi Infrastruktur dan Kebutuhan Organisasi; (2) Implementasi SSO Eksisting; (3) *Roadmap*/ Rencana Implementasi SSO. Proses analisis data seperti yang dijelaskan di bawah ini:

- Memahami klasifikasi dan kebutuhan perguruan tinggi yang disurvei saat ini
- Menganalisis kondisi eksisting dan isu-isu yang dihadapi oleh perguruan tinggi yang telah menerapkan solusi IAM dan SSO
- Menganalisis kemungkinan kendala isu yang dihadapi oleh perguruan tinggi saat hendak merealisasikan solusi IAM dan SSO
- Membandingkan umpan balik dari survei dengan *business case* penelitian terdahulu

### *C. Hasil Penelitian*

Hasil penelitian didasarkan pada survei yang dilakukan terhadap 22 personil Pusat IT dari 17 perguruan tinggi Yogyakarta. Proses survei tidak membatasi jumlah responden per perguruan tinggi, sehingga memungkinkan terdapat lebih dari satu responden dalam satu perguruan tinggi. Hal ini memungkinkan adanya perbedaan jawaban pada beberapa pertanyaan, dikarenakan perbedaan pemahaman/ persepsi responden. Hasil penelitian yang disajikan di bawah ini telah dianalisis dan dibandingkan dengan penelitian sebelumnya.

1. Infrastruktur dan kebutuhan organisasi




**Gambar 3.** Jumlah aplikasi yang dikelola

Berdasarkan survei yang dilakukan dapat disimpulkan bahwa sebagian besar perguruan tinggi masuk dalam klasifikasi kecil dengan mengelola kurang dari 50 aplikasi, yaitu sebesar 54.5% (Gambar 3). Hanya 13.6% responden dari 2 perguruan tinggi yang masuk dalam klasifikasi besar dengan mengelola lebih dari 150 aplikasi.

Aplikasi diatas merupakan bagian dari *resource* yang dikelola oleh perguruan tinggi. Penelitian ini


Received: February 6th, 2023 | Published: March 22nd, 2023

DOI: 10.30656/jsii.v10i1.6186
p-ISSN: 2406-7768
e-ISSN: 2581-2181

mengelompokkan *resource* menjadi lima jenis, yaitu jaringan/Wifi, email, IoT, aplikasi *web-based*, dan aplikasi *native*. Gambar 4 menunjukkan *resource* yang saat ini dikelola oleh perguruan tinggi yang disurvei. Berdasarkan kompleksitasnya, 81.8% perguruan tinggi memiliki kompleksitas sedang dengan mengelola 3 sampai dengan 4 jenis *resource*, selebihnya yaitu 18.2% termasuk klasifikasi kompleks dengan mengelola lebih dari 4 *resource*. Perguruan tinggi dengan klasifikasi kompleks tersebut juga mengelola aplikasi *legacy* dan SaaS yang diintegrasikan dengan SSO SAML.


**Gambar 4.** Jenis resource yang dikelola

Menurut respon survei, berbagai *resource* yang dimiliki perguruan tinggi di Yogyakarta keseluruhannya dikelola secara terpusat pada arsitektur *on-premises* (50%), hibrid (45.5%), dan *cloud* (4.5%). Terkait kebutuhan fitur SSO, 45.5% responden memerlukan pendefinisian atribut disisi pengguna. Ini merupakan salah satu fitur SAML untuk memudahkan admin IT disaat terdapat perubahan atribut pengguna. Admin IT hanya perlu menyesuaikan atribut pengguna, karena akses ke aplikasi akan mengikuti atribut yang melekat pada pengguna. Namun hal ini tidak sejalan dengan kebutuhan kolaborasi, dimana terdapat 13 responden (59.1%) yang memiliki rencana untuk berkolaborasi dengan perguruan tinggi lain. Saat perguruan tinggi berkolaborasi dengan perguruan tinggi lain, akan ada *resource* atau data yang dipertukarkan. Penggunaan protokol yang mendukung prinsip federasi sangat disarankan.

2. Implementasi SSO


**Gambar 5.** Perguruan tinggi sudah menerapkan SSO

Penelitian ini menganalisa implementasi SSO pada 10 dari 22 responden (Gambar 5) berdasarkan umpan balik survei dan wawancara dari 20 pertanyaan. Hasilnya dapat disimpulkan sebagai berikut:

a. Tujuh (7) perguruan tinggi memiliki rencana untuk berkolaborasi dengan perguruan tinggi lain. Dari ketujuh perguruan tinggi tersebut, dua diantaranya masih menggunakan OAuth 2.0 dan sudah memiliki rencana untuk melakukan evaluasi. Satu dari dua perguruan tinggi tersebut sudah melakukan riset dan sudah menentukan akan menggunakan kombinasi SAML dan OAuth 2.0 sesuai kasus yang ada.
b. Dilihat dari protokol yang diterapkan, 6 perguruan tinggi melakukan riset terlebih dahulu untuk menentukan yang paling sesuai dengan kebutuhan organisasi; 3 perguruan tinggi menerapkan protokol yang dianggap populer dilingkungan perguruan tinggi; dan 1 perguruan tinggi sisanya mendapatkan rekomendasi dari pihak ketiga. Terlepas dari motivasi dan upaya penerapannya, berdasarkan hasil observasi kesepuluh perguruan tinggi ini memiliki tim IT yang memadai untuk mengelola, memelihara, dan terus mengembangkan *tools* yang telah diterapkan.
c. Dari sisi pengembangan, semua perguruan tinggi yang melakukan riset sebelum memilih protokol yang hendak digunakan, membangun layanan SSO nya secara mandiri karena menilai bahwa implementasinya cukup mudah. Meskipun masih terdapat 4 perguruan tinggi yang belum sepenuhnya mengintegrasikan semua *resource* dengan SSO.
d. Diantara domain aplikasi yang diintegrasikan ke SSO, domain Layanan Kemahasiswaan menjadi prioritas perguruan tinggi. Disusul oleh Layanan Administrasi perguruan tinggi, dan Layanan Pembelajaran.
e. Perguruan tinggi klasifikasi besar selalu memiliki arsitektur yang kompleks, memiliki infrastruktur *on-premises*, dan menggunakan protokol SAML untuk mengintegrasikan *resource*-nya. Berdasarkan hasil survei, perguruan tinggi ini memiliki *resource* yang beragam, masih memiliki aplikasi *legacy* dan juga memanfaatkan layanan SaaS.
f. Pada perguruan tinggi klasifikasi sedang dan kecil, terdapat 2 responden yang menggunakan layanan SaaS


Received: February 6th, 2023 | Published: March 22nd, 2023

DOI: 10.30656/jsii.v10i1.6186
p-ISSN: 2406-7768
e-ISSN: 2581-2181

mengintegrasikannya dengan OAuth 2.0. Berdasarkan penelitian sebelumnya, baik SAML maupun OAuth 2.0 sangat memungkinan untuk mengintegrasikan aplikasi *legacy* dan aplikasi SaaS.

g. Terdapat 7 perguruan tinggi yang mengintegrasikan aplikasi *native* (*desktop-based/mobile-based*) dan IoT menggunakan SAML, hal ini tidak sejalan dengan *business case* SAML.

Teknis implementasi SSO di lapangan sangat bervariasi, disamping manfaat yang dirasakan, beberapa perguruan tinggi masih memiliki kendala (Gambar 6**Error! Reference source not found.**), diantaranya:

a. Masih banyak permintaan *reset password* dikarenakan lupa *password* akun aplikasi maupun akun SSO
b. Pengguna masih cenderung menggunakan fitur *login* masing-masing aplikasi, karena masih terdapat pilihan *login* menggunakan SSO dan *login* bawaan aplikasi
c. Pengelolaan hak akses belum dilakukan secara terpusat, masih dilakukan pada masing-masing aplikasi
d. Manajemen data pengguna belum terpusat (*Provisioning* akun pengguna memakan waktu lama karena harus memberikan/menghapus akses pada masing-masing aplikasi terkait sesuai *role*-nya.) [22]
e. Masih rentan terjadi kebocoran data
f. Kesulitan saat mengintegrasikan dengan aplikasi *on-premises* (aplikasi *legacy*)
g. Implementasinya cukup kompleks
h. Tidak dapat berkolaborasi/ sharing *resource* dengan perguruan tinggi lain [4]
i. Tidak dapat diintegrasikan dengan aplikasi *Native* (*mobile-based*/*desktop-based*) dan IoT, kalaupun bisa akan membutuhkan banyak kustomisasi yang tidak sesuai *best practice* [22][23]
j. Tidak mendukung *Single Logout* [22]
k. Tidak ada kendala berarti


**Gambar 6.** Kendala SSO eksisting

Dari kendala-kendala yang masih dialami pada pemanfaatan SSO eksisting, 70% perguruan tinggi memiliki rencana untuk mengevaluasi dan menyesuaikan protokol SSO yang digunakan. Namun hanya 40% saja yang telah menentukan hendak menggunakan protokol apa, selebihnya masih akan melakukan riset kembali. Gambar 7 menunjukkan prosentase tersebut.


**Gambar 7.** Rencana penggunaan protokol

3. Rencana pengembangan SSO (*Roadmap*)

Pada perguruan tinggi yang belum menerapkan SSO, terdapat 12 responden yang 58.3% diantaranya telah memiliki *roadmap* implementasi SSO, namun belum menentukan protokol apa yang hendak digunakan. Perguruan tinggi belum mengimplementasikan SSO karena berbagai kendala. Kendala terbesar adalah keterbatasan SDM, baik karena minim SDM yang *capable* untuk mengimplementasikan SSO (75%) maupun keterbatasan *update* pengetahuan (66.7%).

4. Tantangan Implementasi IAM dan SSO

Berikut merupakan tantangan yang dihadapi terkait implementasi solusi IAM dan SSO berdasarkan survei yang dilakukan dan penelitian sebelumnya:

a. Kurangnya penelitian yang dilakukan untuk mempelajari apakah solusi yang hendak digunakan dapat memenuhi kebutuhan/ kriteria organisasi [22]
b. Kompleksitas arsitektur dan aplikasi yang perlu diintegrasikan dengan solusi IAM dan SSO [4]
c. Memahami kelemahan masing-masing solusi IAM dan SSO, untuk mengetahui pengaruhnya terhadap infrastruktur organisasi [4]
**d.** SDM yang berwawasan dan *resource* yang memadai untuk mendukung implementasi *tools* [22]

## IV. KESIMPULAN

Berdasarkan hasil survei dan wawancara, perguruan tinggi Yogyakarta menggunakan SAML dan OAuth 2.0 untuk mengintegrasikan berbagai *resource* perguruan tinggi, termasuk aplikasi SaaS dan aplikasi *legacy*. Protokol SSO yang digunakan pun beragam, ada yang menerapkan SAML, OAuth 2.0, dan kombinasi keduanya. Pada praktiknya, masih terdapat ketidaksesuaian penerapan SAML dan OAuth 2.0. Terdapat pula keterbatasan penerapan lain yang menyebabkan masih munculnya kendala-kendala yang seharusnya dapat teratasi dengan adanya penerapan SSO.

Penelitian tidak hanya dibatasi pada perguruan tinggi yang telah menerapkan SSO, namun juga melibatkan perguruan tinggi yang belum menerapkannya. Tujuannya untuk mengidentifikasi infrastruktur, kebutuhan, langkah yang telah dilakukan untuk menuju penerapan SSO, dan kendala yang


Received: February 6th, 2023 | Published: March 22nd, 2023

DOI: 10.30656/jsii.v10i1.6186
p-ISSN: 2406-7768
e-ISSN: 2581-2181

dialami dalam prosesnya. Berdasarkan hasil survei dan wawancara, terlihat bahwa lebih banyak perguruan tinggi yang belum menerapkan SSO (10:12) karena berbagai kendala, termasuk 3 responden yang mengklaim belum adanya kebutuhan SSO. Terlepas dari kendala yang ada, 9 responden lainnya telah menyadari permasalahan yang dihadapi dan mengusahakan solusi dengan menyusun *roadmap* terkait rencana penerapan SSO.

## V. SARAN

Penelitian ini memiliki keterbatasan dikarenakan metode survei dan wawancara dilakukan secara *online*. Oleh karena itu, pada penelitian selanjutnya dapat dilakukan dengan metode yang lebih intensif, sehingga dapat menggali informasi yang lebih lengkap dan tanggapan yang dirasa kurang sesuai dapat terkonfirmasi dengan baik. Selain itu, dengan metode semacam ini, penulis dapat memberikan pertanyaan lain yang mendukung diluar pertanyaan yang telah disusun.

Pengembangan penelitian juga dapat dilakukan dari sisi responden, karena pada penelitian ini masih terbatas pada 22 responden dari 17 perguruan tinggi, sehingga masih terdapat 97 perguruan tinggi lainnya di Yogyakarta yang dapat dijangkau pada penelitian yang akan datang.

## REFERENSI

[1] K. Costello and M. Rimol, "Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021," *https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021*, Apr. 21, 2021.

[2] Z. Triartono and R. M. Negara, "Implementation of Role-Based Access Control on OAuth 2.0 as Authentication and Authorization System," *2019 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2019, doi: https://doi.org/10.23919/EECSI48112.2019.8977061.

[3] M. Aldosary and N. Alqahtani, "A Survey on Federated Identity Management Systems Limitation and Solutions," *International Journal of Network Security & Its Applications*, vol. 13, no. 03, pp. 43–59, May 2021, doi: 10.5121/ijnsa.2021.13304.

[4] I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. 574–588, 2018, doi: 10.1016/j.jestch.2018.05.010.

[5] J. Basney, P. Cao, and T. Fleury, "Investigating Root Causes of Authentication Failures Using a SAML and OIDC Observatory," in *Proceedings - 2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application, DependSys 2020*, Dec. 2020, pp. 119–126. doi: 10.1109/DependSys51298.2020.00026.

[6] N. Naik and P. Jenkins, "An Analysis of Open Standard Identity Protocols in Cloud Computing Security Paradigm", doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.85.

[7] C. Glahn and R. Mazza, "Integrating Native Mobile Apps into Institutional Educational-technology Ecosystems," *17th World Conference on Mobile and Contextual Learning*, pp. 77–83, 2018.

[8] E. Ito, Y. Kasahara, and N. Fujimura, "Implementation and operation of the kyushu university authentication system," in *Proceedings ACM SIGUCCS User Services Conference*, 2013, pp. 137–142. doi: 10.1145/2504776.2504788.

[9] J. Basney *et al.*, "CILogon: Enabling Federated Identity and Access Management for Scientific Collaborations," 2019. [Online]. Available: https://www.shibboleth.net/

[10] V. Kalfa, G. Roussos, D. Charidimou, and A. Agorogianni, "Coping with the COVID-19 challenges in a comprehensive university: learning tools and procedures adopted by Aristotle University of Thessaloniki," *Proceedings of the European University Information Systems Conference 2021*, 2021, doi: https://doi.org/10.29007/hhvq.

[11] M. Iordan, G. Bîzoi, A.-C. Bîzoi, and C. Herman, "MOODLE PLATFORM' SUPPORT IN DIGITIZING THE ACADEMIC PROCESS. CASE STUDY WEST UNIVERSITY OF TIMIȘOARA," 2021, [Online]. Available: https://www.researchgate.net/publication/361440775

[12] V. Kumar and D. Sharma, "Creating Collaborative and Convenient Learning Environment Using Cloud-Based Moodle LMS: An Instructor and Administrator Perspective," *International Journal of Web-Based Learning and Teaching Technologies*, vol. 11, no. 1, pp. 35–50, Jan. 2016, doi: 10.4018/IJWLTT.2016010103.

[13] A. Juma, J. Rodríguez, J. Caraguay, M. Naranjo, A. Quiña-Mera, and I. García-Santillán, "Integration and evaluation of social networks in virtual learning environments: A case study," in *Communications in Computer and Information Science*, 2019, vol. 895, pp. 245–258. doi: 10.1007/978-3-030-05532-5_18.

[14] A. A. Mawgoud, M. H. N. Taha, and N. E. M. Khalifa, "Security Threats of Social Internet of Things in the Higher Education Environment," in *Studies in Computational Intelligence*, vol. 846, Springer Verlag, 2020, pp. 151–171. doi: 10.1007/978-3-030-24513-9_9.

 Received: February 6th, 2023 | Published: March 22nd, 2023

DOI: 10.30656/jsii.v10i1.6186
p-ISSN: 2406-7768
e-ISSN: 2581-2181

[15] A. Arina, "Analysis of IoT security issues used in Higher Education Institutions," *International Journal of Mathematics and Computer Research*, vol. 09, no. 05, May 2021, doi: 10.47191/ijmcr/v9i5.01.

[16] J. vom Brocke, A. Simons, B. Niehaves, B. Niehaves, and K. Reimer, "Reconstructing the Giant- On the Importance of Rigour in Documenting the Literature Search Process," *European Conference on Information Systems*, p. 2009, 2009, [Online]. Available: https://aisel.aisnet.org/ecis2009/161

[17] N. Naik and P. Jenkins, "Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect," *2017 11th International Conference on Research Challenges in Information Science (RCIS)*, 2017, doi: 10.1109/RCIS.2017.7956534.

[18] J. Carretero, G. Izquierdo-Moreno, M. Vasile-Cabezas, and J. Garcia-Blas, "Federated identity architecture of the European eID System," *IEEE Access*, vol. 6, pp. 75302–75326, 2018, doi: 10.1109/ACCESS.2018.2882870.

[19] T. Ueda and Y. Ikeda, "Socio-economics and educational case study with cost-effective IOT campus by the use of wearable, tablet, cloud and open E-learning services," *Japan Society for the Promotion of Science KAKENHI*, 2017.

[20] S. Hammann, R. Sasse, and D. Basin, "Privacy-Preserving OpenID Connect," *ASIA CCS '20: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 2020, doi: https://doi.org/10.1145/3320269.3384724.

[21] C. A. Christiansen and L. Stuart, "Identity as a Service on the Journey to the Cloud IDC OPINION," 2016.

[22] U. Joshi, S. Cha, and S. Esmaili-Sardari, "Towards adoption of authentication and authorization in identity management and single sign on," *Advances in Science, Technology and Engineering Systems*, vol. 3, no. 5, pp. 492–500, 2018, doi: 10.25046/aj030556.

[23] OASIS, "Security Assertion Markup Language (SAML) V2.0 Technical Overview," 2008. [Online]. Available: http://docs. oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

 Received: February 6th, 2023 | Published: March 22nd, 2023