P-ISSN :2580-4316
E-ISSN :2654-8054

Pengembangan Sistem Single Sign On PT Telkom Akses Dengan Menerapkan Protokol OpenID Connect

Rian Saputra[1], Holder Simorangkir[2]

[1,2]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Esa Unggul
Jl.Arjuna Utara No.09, Duri Kepa, Kec. Kebon Jeruk, Kota Jakarta Barat,
Daerah Khusus Ibukota Jakarta 11510
E-mail : rians4042@gmail.com[1], holder@esaunggul.ac.id[2]

ABSTRAK

Perusahaan besar di dunia digital saat ini tentunya memiliki aplikasi yang membantu menyelesaikan pekerjaan atau memberi informasi terkait pekerjaan, aplikasi pun beragam antara pekerjaan satu dengan pekerjaan lainnya, PT Telkom Akses memiliki *Single Sign On* (SSO) yang bertujuan untuk menjadikan satu *username* dan *password* untuk beberapa aplikasi, namun tidak semua aplikasi yang digunakan tercakup oleh *Single Sign On* (SSO) yang berjalan saat ini, aplikasi yang tidak tercakup *Single Sign On* (SSO) PT Telkom Akses, untuk dapat digunakan karyawan bisa menggunakan akun *guest*, tetapi akun *guest* memiliki batasan pemakai sehingga karyawan meminjam akun karyawan lain untuk dapat *login* pada aplikasi, hal tersebut bisa menimbulkan celah penyalahgunaan hak akses. Dengan dibuatnya penerapan protokol OpenID Connect pada *Single Sign On* (SSO) PT Telkom Akses *username* dan *password* akan ditampung pada *Identity Provider*, kemudian *Identity Provider* akan dihubungkan dengan aplikasi sehingga ketika pengguna akan *login* aplikasi akan mengahkan pengguna untuk validasi *username* dan *password* pada *Identity Provider* dengan satu *username* dan *password*. Dengan diterapkannya metode ini diharapkan dapat membantu karyawan lebih mudah dalam mengakses aplikasi yang digunakan tanpa kendala.

Kata kunci : Single Sign On (SSO), OpenId Connect, Identity Provider

ABSTRACT

Large companies in the digital world today certainly have applications that help complete work or provide information related to work, applications vary from one job to another, PT Telkom Access has Single Sign On (SSO) which aims to make one username and password for several applications, but not all applications used are covered by Single Sign On (SSO) currently running, applications that are not covered by PT Telkom Access Single Sign On (SSO), employees can use guest accounts, but guest accounts have user restrictions. so that employees borrow other employees' accounts to be able to log in to the application, this can create a loophole for abuse of access rights. With the implementation of the OpenID Connect protocol on the Single Sign On (SSO) PT Telkom Access username and password will be accommodated in the Identity Provider, then the Identity Provider will be connected to the application so that when the user logs in the application will direct the user to validate the username and password on the Identity Provider by one username and password. With the implementation of this method is expected to help employees more easily access the applications used without any problems.

Keyword : Single Sign On (SSO), OpenId Connect, Identity Provider

1. PENDAHULUAN

PT Telkom Akses ialah anak industri dari PT Telkom Indonesia. Usaha utama dari perusahaan Telkom Akses adalah penyedia infrastruktur dan pemeliharaan jaringan telekomunikasi milik PT Telkom Indonesia dan juga mempunyai kantor di kota-kota besar di Indonesia. PT Telkom Akses terdiri dari beberapa divisi dan diantaranya merupakan divisi SDI (*Survey Design Inventory*), setiap area PT Telkom akses terdapat divisi SDI yang bertanggung jawab untuk membuat desain jaringan dan mencatat semua hasil pembangunan jaringan. Setiap staff karyawan pada Divisi SDI (*Survey Design Inventory*) mengharuskan mengakses aplikasi-aplikasi kantor yang berhubungan dengan tugas pekerjaan.

Pada Divisi SDI (*Survey Design Inventory*) area Jakarta Selatan untuk proses yang berjalanan saat ini dalam melakukan pekerjaan bukan hanya mengakses aplikasi milik PT Telkom Akses saja namun terdapat aplikasi yang mengharuskan mengakses aplikasi milik PT Telkom Indonesia dikarenakan pekerjaan yang masih berkaitan. Saat ini masih terdapat beberapa kendala pada staff karyawan dalam mengakses aplikasi-aplikasi untuk pekerjaan, yaitu ketika akses ke aplikasi-aplikasi yang dimiliki oleh PT Telkom Indonesia karyawan PT Telkom Akses harus menggunakan akun *guest user* untuk dapat mengaksesnya dan akses sebagai *guest user* yang disediakan memiliki keterbatasan pengguna, tentunya hal tersebut bisa menghambat dalam aktivitas pekerjaan. Ketika keterbatasan pengguna terkadang karyawan PT Telkom akses menggunakan akun dari karyawan PT Telkom Indonesia dan hal tersebut dikhawatirkan terdapat penyalahgunaan akun kedepannya.

PT Telkom Akses saat ini sudah menerapkan *Single Sign On* (SSO) untuk akses ke aplikasi milik PT Telkom Akses namun masih belum efektif dikarenakan masih terdapat akun yang berbeda-beda jika akses ke aplikasi-aplikasi yang dibutuhkan. Hal tersebut cenderung membuat setiap karyawan harus selalu mengingat *username* serta *password* pada tiap aplikasi.

Single Sign On (SSO) bisa disebut sebuah sistem yang menjadikan satu *username* serta *password* cukup diingat oleh pengguna yang autentik untuk mengakses layanan berbeda sekaligus (Fathurrahmani et al., 2021). Salah satu penelitian yang membahas tentang *Single Sign On* (SSO) yaitu (Suhardi et al., 2017) Penelitian tersebut menerapkan protocol OAuth 2.0 dengan hasil memisah server identitas pengguna dengan data pengguna, dengan demikian pengguna dapat melakukan login dengan akun yang sama pada server yang berbeda. Penelitian lainnya yang dilakukan di Bandung oleh (Rahayu et al., 2021) penelitian ini menguji *Single Sign On* (SSO) dengan beberapa teknologi protokol untuk penggunaannya seperti SAML dan OpenID dan hasil dari penelitian tersebut menunjukkan hasil yang sama walaupun berbeda protokol.

Dari hasil beberapa uraian penjelasan di atas sebelumnya dibuat lah sebuah tujuan dari penelitian ini ialah membuat sebuah solusi, yaitu "Pengembangan Sistem Single Sign On PT Telkom Akses dengan Menerapkan Protokol Openid Connect". Cara kerja dari protokol Openid Connect dengan menjadikan pihak ketiga sebagai penyedia identitas, yang kemudian diintegrasikan dengan aplikasi yang sudah ada. Diharapkan dari penelitian ini dapat mempermudah karyawan untuk mengakses aplikasi yang digunakan karyawan.

P-ISSN :2580-4316
E-ISSN :2654-8054

2. LANDASAN TEORI

Single Sign On (SSO)

Single Sign On (SSO) ialah sesuatu sistem yang membolehkan satu nama pengguna serta kata sandi supaya digunakan pada website yang berbeda aplikasi. Untuk pengguna, sistem *Single Sign On* (SSO) menghasilkan apa yang diucap bukti diri federasi. Dengan demikian aplikasi berbasis *Single Sign On* (SSO) dapat melaksanakan manajemen bukti diri yang hendak mengingat satu nama pengguna dan satu kata sandi, pengguna tidak perlu melakukan proses pendaftaran ulang yang berlebihan pada aplikasi yang berbeda (Suhardi et al., 2017). Keuntungan menggunakan *Single Sign On* (SSO) yaitu tidak diharuskannya pengguna untuk mengingat semua kredensial aplikasi secara terpisah, namun kekurangannya jika ada pihak yang tidak bertanggung jawab dapat mengakses kredensial maka seluruh sistem menjadi tidak aman.

OpenID Connect

Pola *OpenID Connect* adalah lapisan identitas sederhana di atas protokol OAuth 2.0. Hal ini memungkinkan pengguna untuk memverifikasi identitas pengguna berdasarkan otentikasi yang dilakukan oleh Server Otorisasi, serta untuk memperoleh informasi profil dasar tentang pengguna dengan cara yang dapat dioperasikan dan seperti REST. Rangkaian spesifikasi dapat diperluas, memungkinkan peserta untuk menggunakan fitur opsional seperti enkripsi data identitas, penemuan Penyedia OpenID, dan manajemen sesi (Fett et al., 2017).

JSON

JSON(JavaScript Object Notation) merupakan format pertukaran informasi yang sangat ringan dan lebih gampang dibaca serta ditulis oleh manusia, sehingga gampang buat diterjemahkan serta terbuat (*generate*) oleh mesin. Pada biasanya, seluruh bahasa pemprograman modern menunjang buat struktur informasi ini dalam wujud yang sama ataupun komponen yang berlainan. Perihal ini pantas diucap demikian sebab format informasi gampang dipertukarkan dengan bahasa-bahasa pemprograman yang pula bersumber pada pada struktur informasi ini (Warsito et al., 2017).

JSON Web Token (JWT)

JWT ialah sebuah token berbentuk string JSON yang sangat padat ukurannya (Rahmatulloh et al., 2018). JWT digunakan untuk berbagi informasi keamanan antara dua pihak klien dan server juga merupakan standar terbuka. JWT ditandatangani menggunakan algoritma kriptografi untuk memastikan bahwa klaim tidak dapat diubah setelah token dikeluarkan.

Keycloak

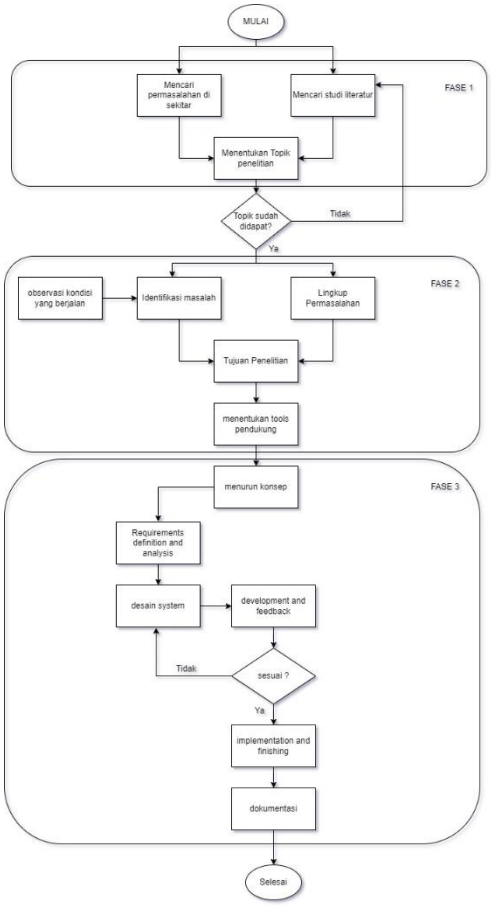
Keycloak merupakan sumber terbuka solusi *Identity and Access Management* yang disediakan untuk modern layanan dan aplikasi (Divyabharathi D. N. & Cholli, 2020). IAM terdiri dari sistem dan proses yang memungkinkan admin untuk menetapkan satu identitas digital ke setiap entitas, mengautentikasinya saat mereka masuk, memberi otorisasi kepada mereka untuk mengakses sumber daya tertentu, dan memantau serta mengelola identitas tersebut sepanjang siklus hidupnya.

Docker

Docker adalah platform sumber terbuka yang memungkinkan pengembang untuk membangun, menyebarkan, menjalankan, memperbarui, dan mengelola wadah komponen standar yang dapat dieksekusi yang menggabungkan kode sumber aplikasi dengan pustaka sistem operasi (OS) dan dependensi yang diperlukan untuk menjalankan kode itu di lingkungan apa pun.

3. METODOLOGI

Untuk berjalannya penelitian ini tahapan penelitian digambarkan dalam kerangka penelitian di bawah:



Gambar 1. Kerangka penelitian

Metode RAD akan diterakpan untuk pengembangan terkait penelitian seperti pada Gambar 1. *Rapid Aplication Development* (RAD) ialah siklus yang menekankan pengembangan pendek, singkat, dan cepat(Widiyanto, 2018). Untuk mengetahui kekurangan terhadap sistem yang sudah ada digunakanlah analisis *PIECES.*

4. HASIL DAN PEMBAHASAN

Teknik Pengumpulan Data

Untuk pengumpulan data, data Kualitatif yang akan digunakan di tahapan penelitian ini. Data didapatkan dengan melakukan wawancara kepada karyawan PT Telkom Akses divisi SDI (*Survei, Design, Inventory*) area Jakarta Selatan untuk mendapatkan informasi pengalaman dan permasalahan yang dirasa oleh karyawan. Berdasarkan hasil wawancara 6 karyawan menyatakan untuk *Single Sign On (SSO*) yang saat ini dirasa masih belum optimal dan perlu untuk dilakukan pengembangan.

Selain dengan melakukan wawancara, penelitian ini juga melakukan perbandingan dengan jurnal yang berkaitan sebagai pendukung topik penelitian.

Analisis Sistem

Pada penelitian ini dilakukan alaisis *PIECES* untuk mengidentifikasi masalah terhadap system yang berjalan saat ini. Berikut ini hasil analisis *PIECES*:

Tabel 1. Analisa *PIECES*

No	*Faktor*	*Hasil Analisa*
1	*Peformance* (Kinerja)	Kurang efektifnya sistem saat ini karena untuk aplikasi selain milik Telkom Akses, drafter harus mengingat *username* dan *password* aplikasi lain yang mereka gunakan.
2	*Information* (Informasi)	Ketika karyawan menggunakan akun guest dan terjadi kesalahan, tidak ada informasi yang detail siapa yang melakukan kesalahan tersebut.

P-ISSN :2580-4316
E-ISSN :2654-8054

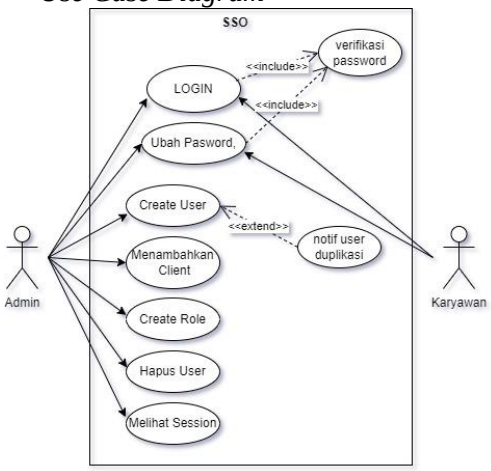
Tabel 1. Lanjutan

No	*Faktor*	*Hasil Analisa*
3	*Economy* (Ekonomi)	Ketika karyawan tidak memiliki akses ke aplikasi, maka akan berperngaruh juga terhadap project yang sedang berjalan, dan semakin lama project itu berjalan akan bertambah juga biayanya.
4	*Control (*Kendali)	Penggunaan akun guest dan meminjam *username* dan *password* orang lain untuk mengakses aplikasi kerja, memberikan celah untuk penyalah gunaan hak akses.
5	*Eficiency* (Efisiensi)	Ketika karyawan menggunakan *username* dan *password* hasil meminjam namun tidak bisa digunakan karena update *password*, dan *guest user* sudah penuh, hal ini membuat waktu kerja tersita untuk mencari cara agar bisa mengakses aplikasi.
6	*Service* (Pelayanan)	Aplikasi yang digunakan saling berkaitan, maka ketika satu aplikasi terkendala akan menghambat pekerjaan lain yang menggunakan aplikasi lainnya.

Gambaran Sistem Usulan

Untuk gambaran sistem usulan akan digambarkan dengan beberapa diagram. *Unified Modelling Language (UML)* ialah diagram gambaran yang dibuat untuk acuan umum pada industri yang digunakan untuk penggambaran, rancangan dan arsipan terhadap system perangkat lunak(Malabay, 2018).

1. Use Case Diagram

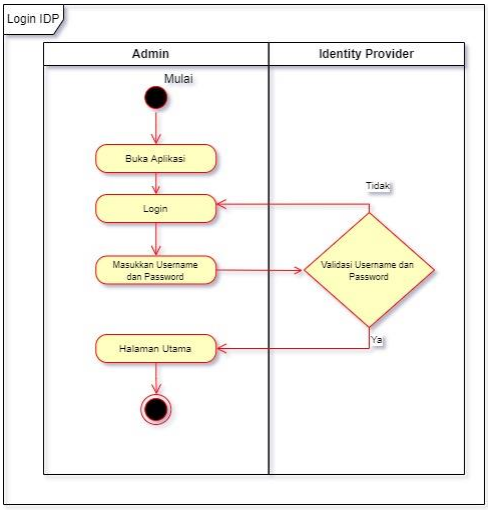


Gambar 2. *Use case diagram*

Perhatikan Gambar 2. Proses dimana user hanya bisa *login* dan mengubah *password* pada *Identity Provider* untuk akses aplikasi. Sedangkan admin dapat membuat *user* untuk penambahan karywan baru, menambahkan *client* untuk mengintegrasi aplikasi baru, menambahkan *role* untuk mengelompokkan *user*, menghapus *user* untuk memutus akses bagi karyawan yang *resign*, dan melihat *session* yang bejalan pada *Identity Provider.*

2. Activity Diagram

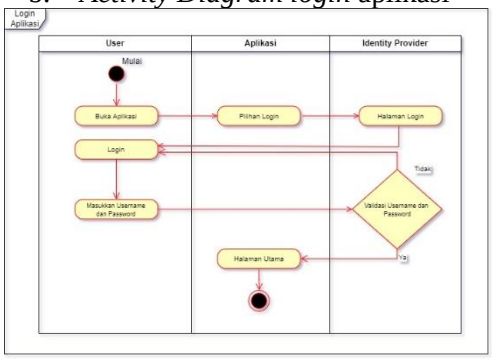
a. Activity Diagram login Identity Provider



Gambar 3. *Activity diagram* login

Gambar 3. untuk admin bisa melakukan tugasnya di *Identity Provider*, terlebih dulu melakukan *login* agar tidak sembarangan orang mengakses *Identity Provider* dengan memasukkan *username* dan *password*

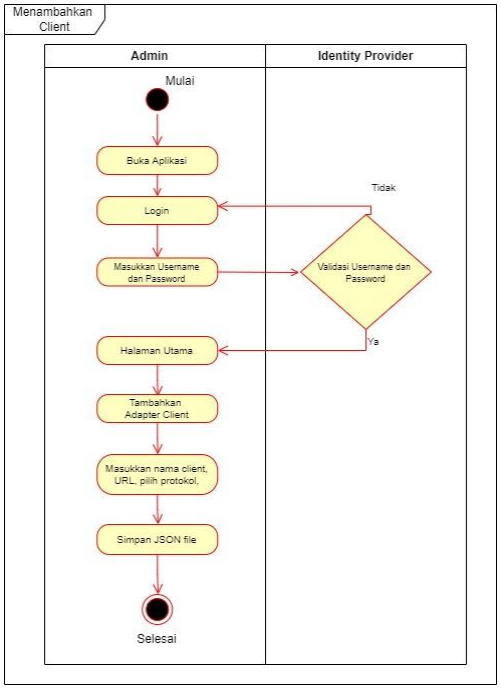
b. *Activity Diagram login* aplikasi



Gambar 4. *Activity diagram login* aplikasi

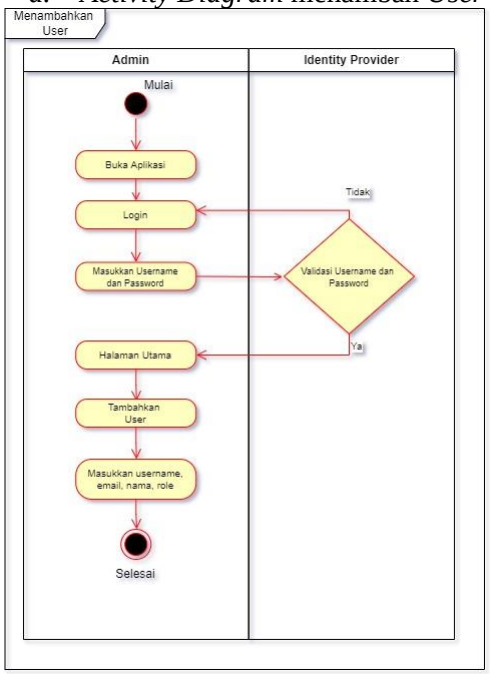
Ketika pengguna akan mengakses aplikasi dan diarahkan ke halaman login, di halaman *login* akan ada menu pilihan untuk *login* menggunakan *Identity Provider*. Ketika memilih *Identity Provider* kemudian akan diarahkan ke halaman login pada *Identity Provider* dan pengguna diminta memasukkan *username* dan *password*, lalu *username* dan *password* akan dicocokkan oleh *Identity Provider*, jika sesuai kemudian akan lanjut ke halaman utama aplikasi.

c. *Activity Diagram* menambahkan *Client*



Gambar 5. *Activity diagram* menambahkan *client*

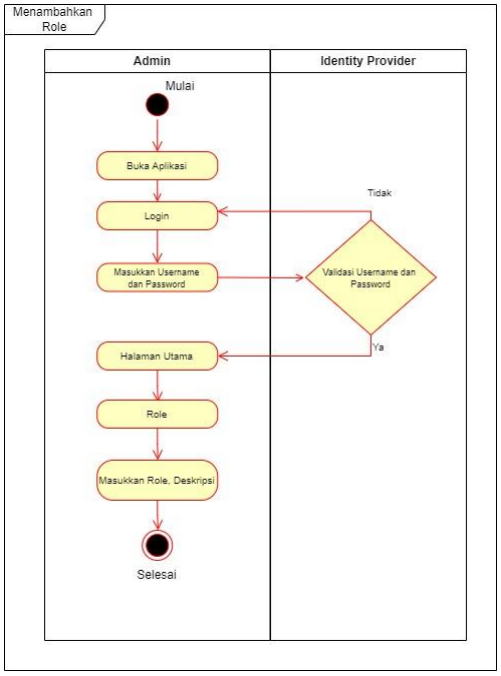
d. *Activity Diagram* menambah *User*



Gambar 6. *Activity diagram* menambah *user*

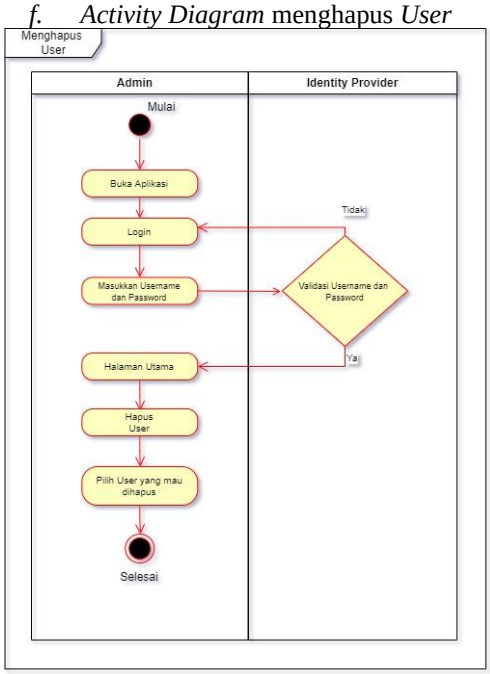
P-ISSN :2580-4316
E-ISSN :2654-8054

e. Activity Diagram menambahkan *role*



Gambar 7. *Activity diagram* menambah *role*

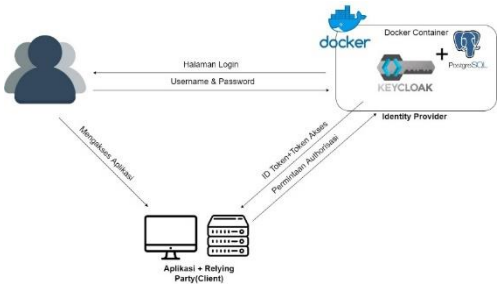
f. Activity Diagram menghapus *User*



Gambar 8. *Activity diagram* menghapus *role*

Implementasi

Untuk implementasinya penelitian ini akan membuat arsitekrur dengan menerapkan protokol *OpenID Connect* seperti gambar di bawah.



Gambar 9. Arsitektur sistem usulan

Untuk sistem yang diusulkan ini terdapat dua komponen, yaitu *Idendity Provider* dan *Client.*

a. Identity Provider

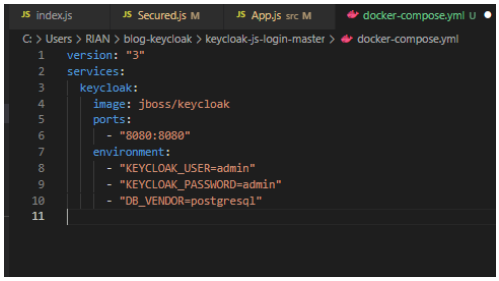
Identity Provider bertugas sebagai penyimpan dan pengelola *user*, selain itu juga bertugas mengauthentikasi *request* dari *client* yang terhubung dan mengembalikan *request* tersebut dengan token yang berisi informasi *user* ke *client.*

b. Client

Client merupakan aplikasi yang akan meminta dan menerima *token* berisi informasi *user* yang dikirimkan dari *Identiy Provider*, token yang diterima akan di enkrip menjadi informasi yang diperlukan oleh aplikasi seperti nama dan *role*.

Implementasi Identity Provider

Tahapan awal dari implementasi *Identity Provider* yaitu dengan menyediakan *Identity Provider* yaitu keycloak dan PostgreSQL sebagai database yang akan dijalankan di dalam container docker.



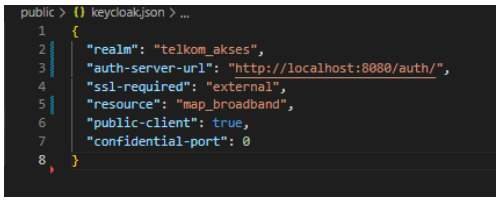
Gambar 10. Mendefinisikan PostgreSQL sebagai Database Keycloak

Pada saat sebelum menjalankan Keycloak dan PostgreSQL, database yang akan digunakan harus didefinisikan diawal karena penelitian ini tikda menggunakan database bawaan dari keycloak, kalua tidak didefinisikan diawal instalasi maka akan menggunakan database bawaan keycloak yaitu H2.

Gambar 11. Keycloak dan PostgreSQL dalam Docker

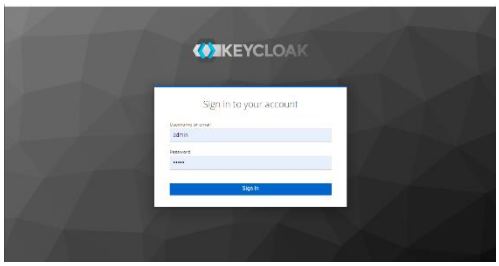
Implementasi Client

Tahap selanjutnya setelah *Identity Provider* yaitu menyiapkan *Client*, dimana *client* merupakan aplikasi yang akan dihubungkan dengan *Identity Provider*.

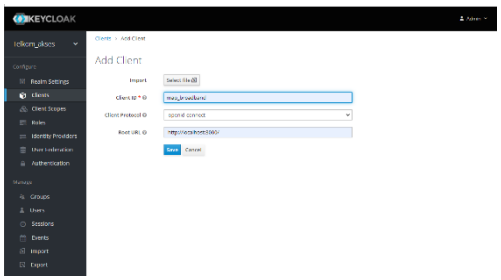


Gambar 12. Keycloak dan PostgreSQL dalam Docker

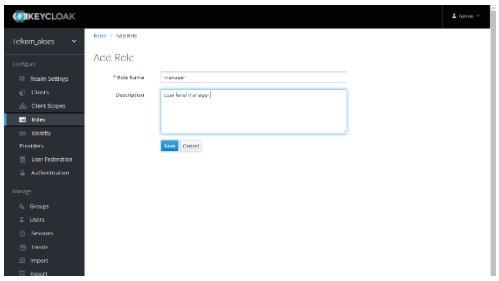
Gambar 12. menampilkan isi dari file JSON yang menghubungkan antara Keycloak sebagai *Identity Provider* dan juga *Client*. Pada file tersebut berisi alamat beserta *port* dari *Identity Provider*, nama *Realm*, dan informasi *client*.



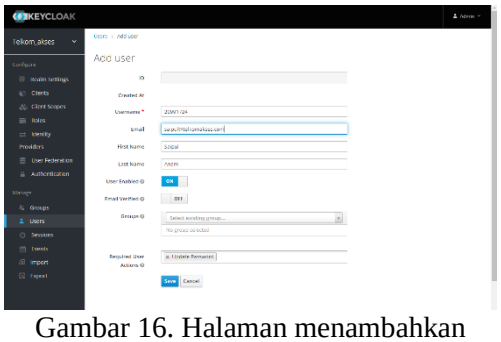
Gambar 13. Halaman login *Identity Provider*



Gambar 14. Halaman menambahkan *Client*



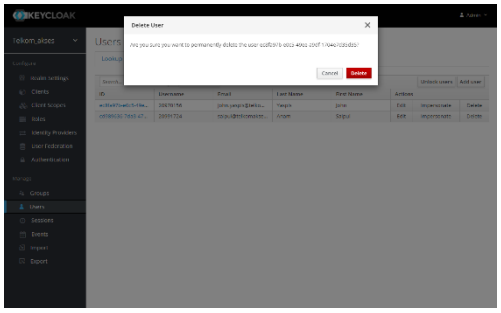
Gambar 15. Halaman menambahkan *Role*



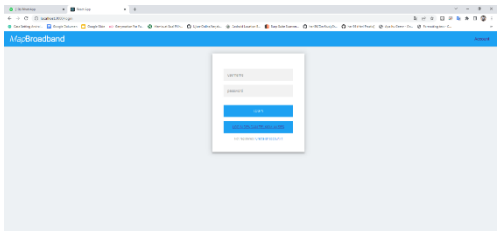
Gambar 16. Halaman menambahkan *User*

Gambar 16. berisi halaman untuk menambahkan *user* baru.

P-ISSN :2580-4316
E-ISSN :2654-8054

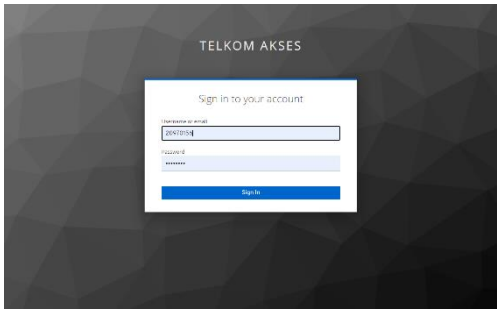


Gambar 17. Halaman menghapus *User*

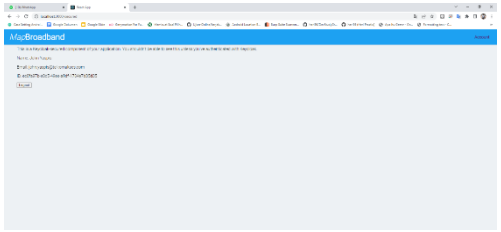


Gambar 18. Halaman login dari aplikasi

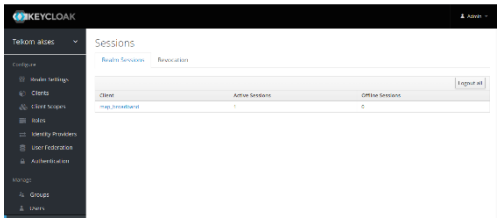
Untuk halaman *login* untuk karyawan mengakses aplikas seperti Gambar 18. di atas, lalu ada menu *login* yang akan mengarahkan ke *Identity Provider*.



Gambar 19. *Login* aplikasi melalui *Identity Provider* Telkom Akses



Gambar 20. Halaman berhasil *login*



Gambar 14. Halaman melihat *session* yang aktif

5. KESIMPULAN

Dengan hasil penelitian yang diselesaikan, Kesimpulan yang dapat diambil dari penelitian ini adalah sebagai berikut

1. Dalam penelitian ini sistem yang sudah ada bisa mengintegrasikan dan dapat menjawab permasalahan PT. Telkom Akses
2. Pengelolaan *user* menjadi terpusat dalam sebuah *Identity Provider*, pengguna tidak perlu login dengan akun yang berbeda-beda, cukup dengan satu akun *login*.
3. Dengan memisahkan antara aplikasi dengan *Identity Provider*, maka ketika ada aplikasi baru cukup menambahkan *client* baru dan menghubungkannya dengan *Identity Provider*.

Tidak hanya kesimpulan ada pula saran yang bisa diambil dari riset ini untuk riset berikutnya merupakan selaku berikut:

1. Untuk *Identity Provider* bisa menggunakan *Identity Provider* lain seperti *Google Cloud Identity*.
2. Melakukan pengembangan dengan menggunakan protokol lain seperti SAML atau LDAP.
3. Melakukan penyesuaian tampilan halaman *login* aplikasi dengan *Identity Provider*.

DAFTAR PUSTAKA

Divyabharathi D. N., & Cholli, N. G. (2020). A Review on Identity and Access Management Server (KeyCloak). *International Journal of Security and Privacy in Pervasive*

Computing, *12*(3), 46–53. https://doi.org/10.4018/ijsppc.2020070104

Fathurrahmani, Herpendi, & Hafizd, K. A. (2021). Perancangan Single Sign on(Sso)Pada Aplikasi Web Menggunakan Cloud Identity(Studi Kasus:Politeknik Negeri Tanah Laut). *ANTIVIRUS: Jurnal Ilmiah Teknik Informatika*, *15*(2), 242–251.

Fett, D., Kusters, R., & Schmitz, G. (2017). The Web SSO Standard OpenID Connect: In-depth Formal Security Analysis and Security Guidelines. *Proceedings - IEEE Computer Security Foundations Symposium*, 189–202. https://doi.org/10.1109/CSF.2017.20

Malabay. (2018). Model Rancangan Pembelajaran Aktif, Kreatif Dan Inovatif Dengan Pendekatan Unified Modeling Language. *Jurnal Ilmu Komputer Vol 15 No 1*, *15*, 81–82.

Rahayu, A., Hermawaty, Mujib, M. A., & DZ, R. (2021). *Dengan Menggunakan Wso2 Is Di Stmik " Amikbandung ." 03*, 7–13.

Rahmatulloh, A., Sulastri, H., & Nugroho, R. (2018). Keamanan RESTful Web Service Menggunakan JSON Web Token (JWT) HMAC SHA-512. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi (JNTETI)*, *7*(2). https://doi.org/10.22146/jnteti.v7i2.417

Suhardi, A., Fatkhiyah, E., & Sholeh, M. (2017). Perancangan Dan Implementasi SSO (Single Sign On) Menggunakan Protokol OAuth 2.0. *JARKOM*.

Warsito, A. B., Ananda, A., & Triyanjaya, D. (2017). Penerapan Data JSON Untuk Mendukung Pengembangan Aplikasi Pada Perguruan Tinggi Dengan Teknik Restfull Dan Web Service. *Technomedia Journal*, *2*(1), 26–36. https://doi.org/10.33050/tmj.v2i1.313

Widiyanto, W. W. (2018). Analisa Metodologi Pengembangan Sistem Dengan Perbandingan Model Perangkat Lunak Sistem Informasi Kepegawaian Menggunakan Waterfall Development Model, Model Prototype, Dan Model Rapid Application Development (Rad). *Jurnal Informa Politeknik Indonusa Surakarta ISSN*, *4*(1), 34–40. http://www.informa.poltekindonusa.ac.id/index.php/informa/article/view/34