

## Penerapan *Single Sign On* (SSO) Pada Keamanan Jaringan Dengan Metode *Lightweight Directory Access Protocol* (LDAP) di PT. Unichem

Agung Kurnianto, Danang Haryo Sulaksono, dan Andy Rachman

Jurusan Teknik Informatika, Institut Teknologi Adhi Tama Surabaya

### ABSTRACT

Unichem Ltd is one of national companies in the field of food manufacturing such as consumed salt, pepper, rice, and others. As an advanced company, Unichem Ltd has adopted the uses of computer and local network as a communication medium among client computers. The LAN also has become the access of application installed in the server computer. In addition to application access, the server has local directory divided in several folders based on the job division in the company. The local directory is used to save the data of occupational documents so that the employees working in one division can use it simultaneously. To optimize the user performance, the information security system, and the IT productivity, an authentication implementing SSO in LDAP (Lightweight Directory Access Protocol) is necessary. LDAP can ease the user in employing only one password for numerous applications. Therefore, the user must keep inputting the name and password during the authentication process of each application. By SSO system, the administrator is expected to be able to manage every account of user conveniently and safely. SSO will ease not only the administrator in managing the user's account, but also the user in remembering his account and password. Some networks integrated with SSO have applied LDAP as the protocol for authentication and MySQL server as the database. Thus, the implementation of SSO in LDAP is expected to assist the company particularly IT Division to organize the network use and maintain the company's data.

### Article History

Received 23 – 8 – 2021  
Revised 21 – 1 – 2022  
Accepted 12 – 9 – 2022

### Key words

SSO  
LDAP  
LAN

### ABSTRAK

PT. Unichem merupakan salah satu perusahaan nasional yang bergerak di bidang manufaktur makanan seperti garam konsumsi, lada, beras, minyak dan lain sebagainya. PT. Unichem telah mengadopsi penggunaan komputer dan jaringan lokal sebagai jalur komunikasi antar komputer *client*. Penggunaan jaringan LAN juga menjadi akses aplikasi yang terinstal pada komputer *server*. Selain untuk mengakses aplikasi, pada server juga terdapat *local directory* yang terbagi menjadi beberapa folder berdasarkan divisi kerja di perusahaan. Penggunaan *local directory* untuk menyimpan data-data dokumen kerja, sehingga dapat saling dipergunakan oleh rekan sesama divisi perusahaan. Dalam mengoptimalkan kinerja pengguna, keamanan sistem informasi, dan produktifitas IT, hingga perlu dilaksanakan otentikasi dengan SSO memakai LDAP (*Light Weight Directory Access Protocol*). Penerapan LDAP dapat mempermudah pengguna dalam pemakaian kata sandi, dimana pengguna hanya mengingat satu kata sandi saja untuk banyak aplikasi. Untuk itu pengguna tetap harus menginput nama dan kata sandi saat akan melakukan otentikasi pada masing-masing aplikasi. Dengan diterapkannya SSO ini diharapkan admin bisa mengelola setiap *user account* dengan mudah dan aman. Selain dari itu, setiap *user* tidak perlu susah payah dalam mengingat *user account* dan *password* yang akan dipakai. Beberapa jaringan yang terintegrasi dengan SSO, sudah menerapkan LDAP sebagai protokol untuk otentikasi dan menggunakan Database Server MySQL sebagai database-nya. Penerapan SSO dengan menggunakan LDAP ini diharapkan dapat membantu perusahaan khususnya bagian IT untuk melakukan manajemen pengguna jaringan dan menjaga keamanan data perusahaan.

### PENDAHULUAN

PT. Unichem adalah perusahaan yang menghasilkan berbagai makanan seperti garam, lada, beras, dan lainnya. Perusahaan ini telah menerapkan komputer dan jaringan lokal seperti Local Area Network (LAN) untuk mendukung komunikasi antar pegawai dalam perusahaan. Selain itu, dalam jaringan LAN tersebut terdapat sebuah computer server untuk mengakses berbagai aplikasi. Untuk mengakses aplikasi-aplikasi tersebut dibutuhkan berbagai akun untuk dapat masuk ke dalam aplikasi. Hal ini menyebabkan pengguna harus mengingat banyak akun untuk berbagai aplikasi

sehingga menyulitkan jika aplikasi bertambah banyak nantinya. Untuk mengatasi hal tersebut, beberapa penelitian lain menggunakan SSO dan Lightweight Directory Access Protocol (LDAP) seperti penelitian [1]–[3].

Pada penelitian ini digunakan Single Sign On (SSO) dan Lightweight Directory Access Protocol (LDAP) untuk memaksimalkan kinerja pengguna dan efisiensi akun pengguna dalam akses berbagai aplikasi perusahaan. Single Sign On (SSO) yaitu sebuah mekanisme dimana masing-masing user hanya memiliki satu akun yang berfungsi sebagai identitas user satu-satunya [4]. Akun yang satu ini bisa digunakan untuk mendapatkan hak akses dari sistem agar pengguna dapat mengakses berbagai aplikasi dengan username dan password yang sama pada sesi tertentu. SSO mengurangi jumlah human error yang merupakan alasan kegagalan utama dari sebuah sistem. Teknologi *Single Sign On* begitu penting bagi portal, singkatnya portal membutuhkannya guna mengkoordinasikan beberapa *website* dan penyimpanan data, *XML*, serta sistem transaksi lainnya.

Lightweight Directory Access Protocol (LDAP) merupakan protokol yang mendefinisikan bagaimana data direktori dapat diakses melalui jaringan [5]. *LDAP* biasanya dipakai menyimpan banyak informasi terpusat yang bisa dijangkau oleh banyak macam mesin atau aplikasi dari jaringan. Penggunaan *LDAP* pada sistem akan membuat pencarian informasi menjadi terintegrasi dan sangat mudah. *LDAP* seringkali digunakan menyimpan data yang ada di dalam sistem secara terpusat.

## TINJAUAN PUSTAKA

### Single Sign On (SSO)

Pada penelitian ini, studi kasus yang diambil berada pada PT. Unichem. Perusahaan ini telah menggunakan aplikasi untuk kebutuhan operasional perusahaan dan tentu saja aplikasi yang tersedia tidak hanya 1 saja. Sehingga ketika semakin banyak aplikasi maka semakin banyak proses login dan autentikasi yang dibutuhkan. Hal ini dapat diselesaikan dengan Single Sign On (SSO) yaitu sebuah sistem autentikasi untuk para pengguna. Dengan adanya SSO maka para pengguna hanya perlu melakukan login untuk dapat masuk atau mengakses beberapa aplikasi sekaligus. Hal ini dapat meningkatkan efisiensi kinerja pengguna dengan tidak perlu login pada setiap aplikasi. SSO dapat diartikan sebagai 2 hal yaitu Single Sign On yaitu pengguna dapat masuk ke dalam berbagai aplikasi dalam sekali login atau Single Sign Out yaitu ketika logout dari 1 aplikasi maka semua aplikasi yang telah diatur juga akan ikut logout pula.

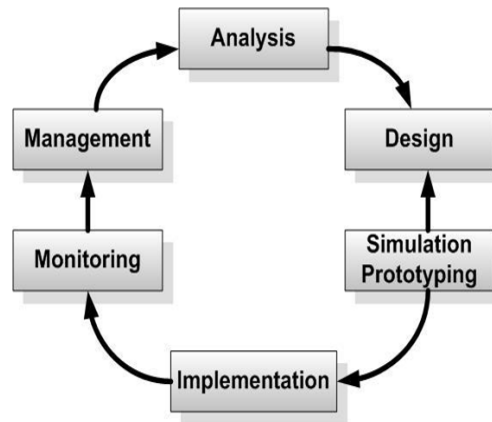
Dengan cara kerja SSO yang telah dijelaskan di atas, maka SSO memiliki setidaknya 3 manfaat. Pertama, pengguna tidak perlu menyimpan atau mengingat banyak akun dengan username dan password yang berbeda. Yang dibutuhkan hanya 1 akun yang penting untuk sekali proses autentikasi. Selanjutnya, para pengguna dapat mengakses semua aplikasi yang tersedia dalam jaringan. Kedua, manajemen pengguna dapat dilakukan dengan mudah dimana ketika terdapat pengurangan atau penambahan pengguna hanya perlu dilakukan sekali pada server database backend, bukan apada setiap aplikasinya. Sehingga meningkatkan efisiensi waktu dalam manajemen pengguna dan kepraktisan dalam proses data. Terakhir, tidak diperlukan membuat akun di setiap aplikasi karena hanya perlu memasukkan data pengguna sekali saja ke dalam server database backend.

### Lightweight Directory Access Protocol (LDAP)

Merupakan sebuah protokol untuk mengakses direktori secara ringan dimana definisi ringan ini adalah penggunaan jaringan internet yang besaran paketnya sangat kecil sehingga bisa dikatakan ringan. LDAP digunakan untuk mengakses suatu direktori suatu perusahaan dan sebagainya dan juga bisa untuk menambah informasi serta memperbarui informasi yang terdapat pada jaringan tersebut. Dalam LDAP juga dilengkapi SASL (Simple Authentication and Security Layer) untuk memastikan izin pengguna untuk akses direktori. Hal inilah yang menjadikan LDAP banyak digunakan bersamaan dengan Single Sign On.

## METODE

Metode pengembangan yang digunakan pada penelitian ini yaitu *Network Development Life Cycle* yang memiliki skema dan tahapan kegiatan berikut ini.



Gambar 1. Kerangka Kerja *Network Development Life Cycle*

### 1. Analisis

Di fase ini akan dilakukan analisa permasalahan yang sedang terjadi di PT. Unichem. Penggalan informasi dilakukan dengan observasi ke lokasi kantor PT. Unichem dan melakukan wawancara kepada manager IT. Kegiatan observasi berfokus terhadap inti permasalahany, penyebab permasalahan dan solusi yang dibutuhkan. Pada tahap ini juga dilakukan analisa perancangan dan topologi jaringan di PT. Unichem.

### 2. Desain

Berdasarkan data-data dari tahap analisis, dilakukan desain atau perancangan untuk solusi yang akan diberikan. Desain dapat berupa topologi jaringan yang diusulkan dan prosedur setting jaringan yang diusulkan. Pada penelitian ini juga dilakukan perancangan sistem web portal sebagai media SSO.

### 3. Simulasi Prototype

Berdasarkan desain topologi jaringan dan setting yang telah dibuat, langkah selanjutnya adalah melakukan simulasi prototipe atau desain tersebut dengan menggunakan *software cisco packet tracer* atau *mikrotik packet tracer*. Simulasi dilakukan untuk tujuan memudahkan dan meminimalisir kesalahan setting saat implementasi secara langsung di PT. Unichem.

### 4. Implementation

Pada tahap ini dilakukan pengaturan topologin jaringan dan setting pada perangkat jaringan sesuai dengan desain dan hasil simulasi yang telah dilakukan.

### 5. Monitoring

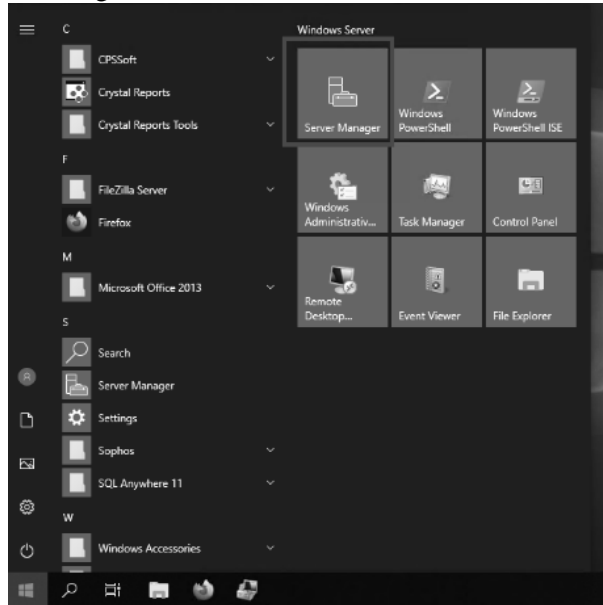
Jaringan yang telah diimplementasi perlu dilakukan monitoring dengan tujuan menjaga performa dan kestabilan jaringan, sehingga hasil implementasi dapat dipertanggungjawabkan.

## HASIL DAN PEMBAHASAN

Pada point ini akan dibahas mengenai hasil penerapan SSO dengan metode *LDAP* di PT.UNICHEM

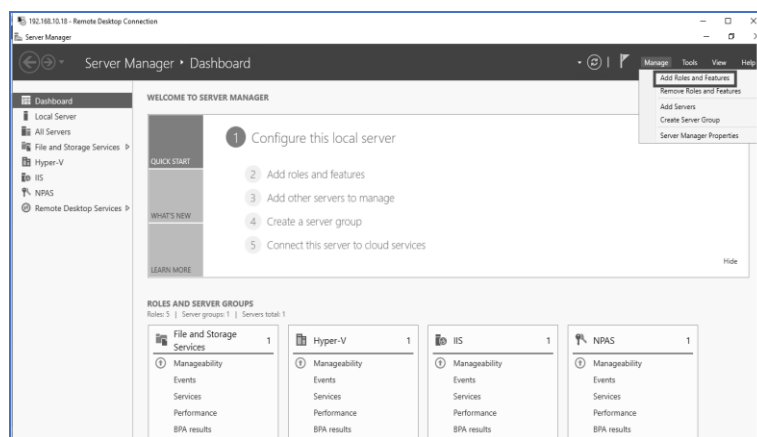
a. Instalasi dan Setting *LDAP*

Tahap pertama untuk implementasi *LDAP* adalah melakukan Instalasi active directory di windows server. Instalasi active directory di windows server dapat dilakukan melalui server manager. Server manager dapat diakses melalui menu start windows. **Gambar 2** merupakan tampilan menu untuk membuka dashboard server manager.



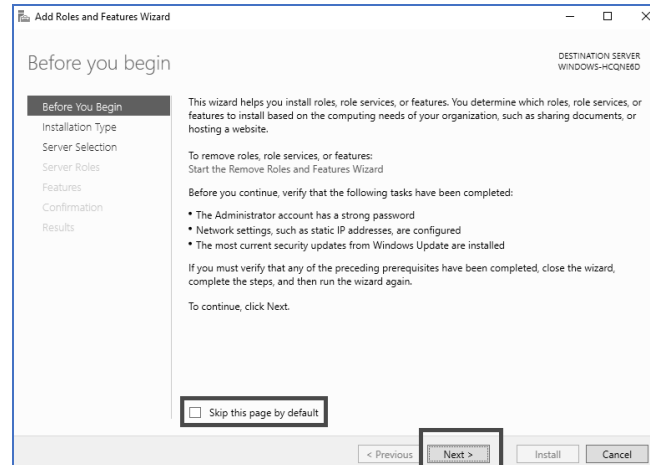
Gambar 2. Halaman Menu Akses Server Manager

Pada tampilan server manager, tekan menu manage kemudian pilih *add roles and features*. Gambar 3 menunjukkan visualisasi pemilihan menu *add roles and features*.



Gambar 3. Halaman Dashboard Server Manager untuk akses Menu *Add Roles and Features*

Windows server menampilkan halaman penjelasan *before you begin* yang memberikan informasi fungsi dari menu *add roles and features*. Pada halaman ini dapat centang *skip this page by default* dan tekan tombol *next*. Berikut ini visualisasi petunjuk di halaman *before you begin*.



Gambar 4. Halaman *before you begin*

Setelah itu dilanjutkan dengan konfigurasi yang ada didalam windows server.

#### b. Implementasi *LDAP*

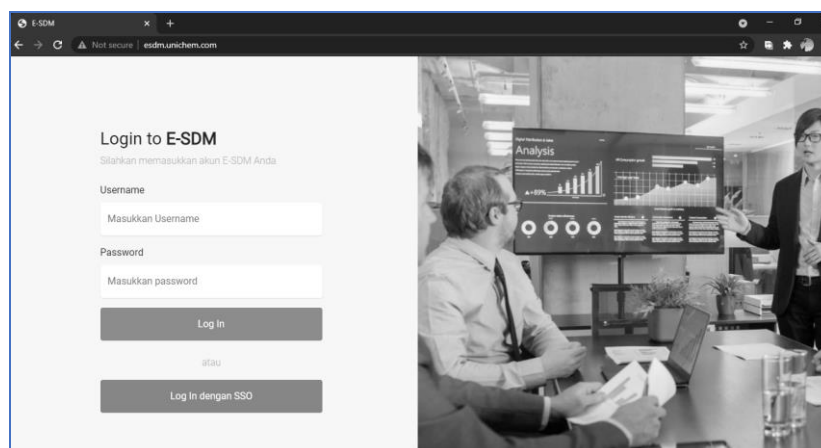
Akses data *LDAP* pada penelitian ini menggunakan bahasa pemrograman PHP. Berikut ini script login PHP yang digunakan untuk melakukan proses validasi data active directory. Berikut ini potongan kode program untuk proses *LDAP* Connect.

```
<?php
// LDAP variables
$LDAPuri = "LDAP:192.168.10.1:389"; // your LDAP-uri
// Connecting to LDAP
$LDAPconn = LDAP_connect($LDAPuri)
or die("That LDAP-URI was not parseable");
?>
```

Pada potongan kode program diatas dapat diketahui akses data ke *server LDAP* yang mempunyai alamat *IP* di 192.168.10.1 dengan port *default LDAP* adalah 389.

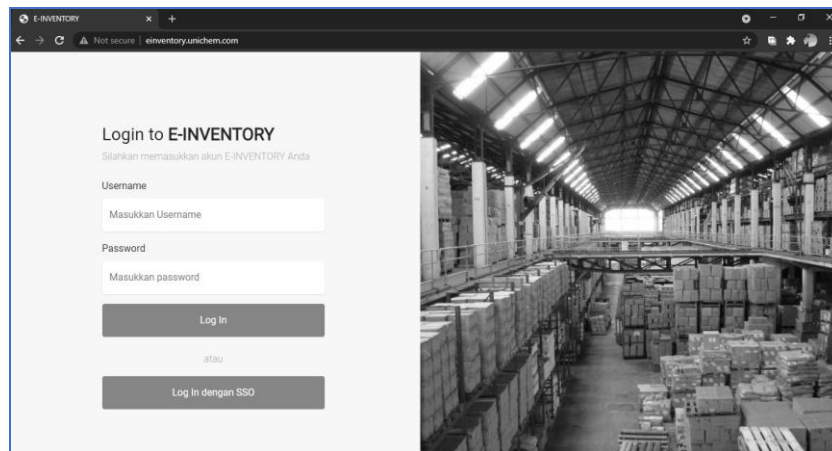
#### c. Implementasi Website Perusahaan Dengan *LDAP*

Website yang diimplementasikan dengan *LDAP Connect* adalah *E-SDM* milik perusahaan yang berfungsi untuk manajemen data karyawan. Berikut ini tampilan halaman *login* dari sistem *E-SDM*.



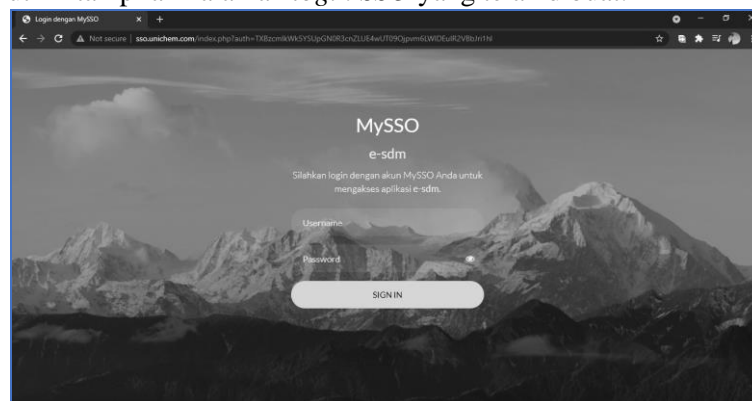
Gambar 5. Halaman Login E-SDM

Selain E-SDM, perusahaan juga memiliki E-Inventory yang digunakan untuk melakukan pengolahan data stok produk Berikut ini tampilan halaman *login E-Inventory*.



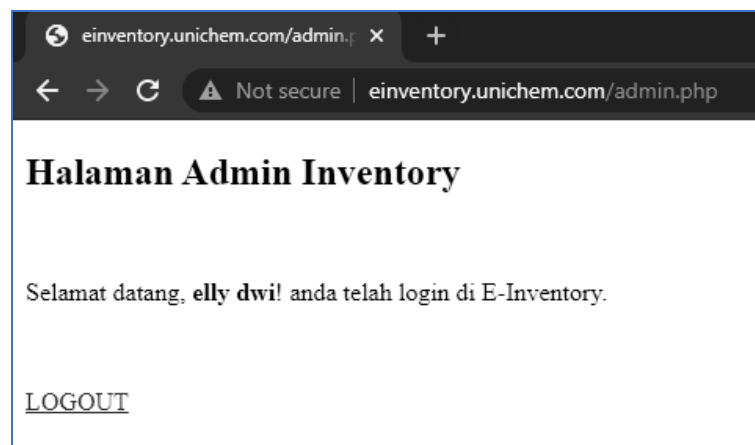
Gambar 6. Halaman Login E-Inventory

Dengan menggunakan *LDAP Connect*, maka dibuat satu halaman login dengan konsep *Single Sign ON* agar karyawan tidak perlu melakukan login berulang pada masing-masing sistem. Berikut ini tampilan halaman *login SSO* yang telah dibuat.



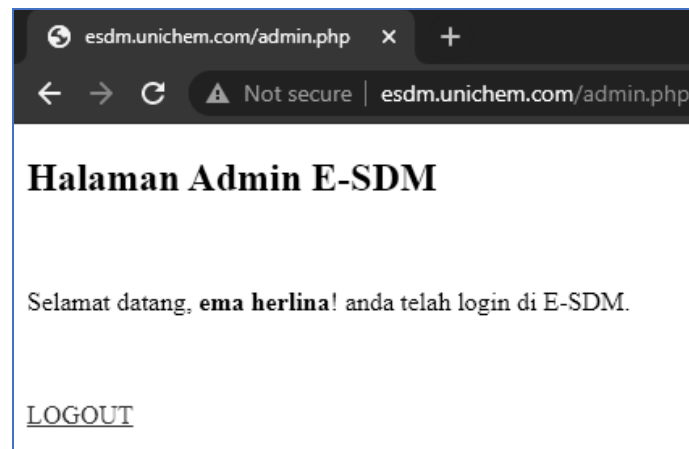
Gambar 7. Halaman Login Single Sign ON

Karyawan yang berhasil *login* dapat melakukan akses diseluruh sistem milik perusahaan. Berikut ini visualisasi karyawan dapat melakukan akses di sistem E-Inventory.



Gambar 8. Halaman E-Inventory Dapat Diakses Tanpa Melakukan Login

Begitu juga untuk sistem E-SDM, karyawan dapat langsung membuka sistem E-SDM tanpa perlu lagi melakukan *login*. Berikut ini visualisasi dari sistem E-SDM yang dapat diakses.



Gambar 9. Halaman E-SDM Dapat Diakses Tanpa Melakukan Login

## KESIMPULAN

Berdasarkan hasil penelitian serta pembahasan yang telah dilakukan pada penelitian ini, maka dapat diambil kesimpulan bahwa penelitian ini berhasil menerapkan otentikasi SSO dengan menggunakan menggunakan LDAP (*Light Weight Directory Access Protocol*) pada jaringan lokal di perusahaan. Hasil pengujian *blackbox testing* telah memastikan otentikasi SSO dengan menggunakan menggunakan LDAP (*Light Weight Directory Access Protocol*) telah berjalan di sistem milik perusahaan. Hasil *User Accepted Test* membuktikan 100 % pengguna sistem Sangat Setuju Terhadap Penerapan SSO di sistem milik perusahaan.

## DAFTAR PUSTAKA

- [1] A. Amarudin, W. Widyawan, and W. Najib, "ANALISIS KEAMANAN JARINGAN SINGLE SIGN ON (SSO) DENGAN LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP) MENGGUNAKAN METODE MITMA," *SEMNASTEKNOMEDIA ONLINE*, vol. 2, 2014.
- [2] R. G. Jatsuma, "Penerapan Sistem Single Sign On ( SSO ) Pada Kampus XYZ Berbasis Lightweight Directory Access Protocol ( LDAP )," vol. 2, no. 6, pp. 1–12, 2022.
- [3] A. R. Ruli and A. Hidayati, "Implementasi dan Analisa Single Sign On Firewall Checkpoint Menggunakan Active Directory Pada Akita Jaya Mobilindo," 2017.
- [4] I. Putu, A. Eka, and D. Udayana, "Implementasi Dan Analisis Single Sign on Pada Sistem Informasi Universitas Udayana," *Semnasteknomedia Online*, vol. 4, no. 1, pp. 1-4–67, 2016, [Online]. Available: <https://ojs.amikom.ac.id/index.php/semnasteknomedia/article/view/1153>.
- [5] H. A. Saputra, "Pengembangan Teknologi Single Account Menggunakan Web Service Dan Lightweight Directory Access Protocol (Ldap) (Studi Kasus : Moodle Dan Wordpress)," p. 128, 2017.