BAB I

PENDAHULUAN

1.1 Latar Belakang

Dengan semakin berkembangnya protokol HTTP pada saat ini telah membangkitkan minat para pengembang aplikasi untuk membangun aplikasi mereka berbasis pada teknologi *Web* atau biasa disebut *Web-based Application*. Oleh karena itu penggunaan aplikasi berbasis *Web* sudah menjadi suatu yang umum dalam suatu komunitas, seperti pada perusahaan ataupun lembaga pendidikan. Aplikasi berbasis *Web* biasanya selalu menyertakan otentikasi untuk melakukan validasi terhadap penggunanya sehingga terdapat banyak proses otentikasi yang terjadi.

Salah satu solusi yang biasa menjadi pilihan dalam mengatasi masalah di atas adalah dengan mengintegrasikan *Single Sign On* atau disingkat SSO pada jaringan dimana apliksi-aplikasi itu akan dipergunakan oleh pengguna. SSO adalah sebuah konsep jaringan yang memungkinkan pengguna untuk melakukan otentikasi melalui satu aplikasi untuk mendapat akses ke beberapa aplikasi yang tergabung dalam sistem ini.

Dalam mengintegrasikan SSO terdapat banyak cara yang dapat ditempuh antara lain melalui penggunaan *central authentication service* atau CAS yang pertama kali dikembangkan oleh Universitas Yale dan dikembangkan lebih lanjut oleh *Java in Administration Special Interest Group* atau di singkat **JASIG** sehingga lebih dikenal

dengan JASIG-CAS, CAS banyak dipilih oleh *network adminisitrator* karena merupakan produk *open-sources* sehingga dapat dikonfigurasikan sesuai dengan kebutuhan atau dapat disesuaikan dengan kondisi yang sudah ada pada tempat dimana sistem akan diimplementasikan.

JASIG-CAS yang merupakan *Framework* SSO secara *default* tidaklah menyertakan *datastore* guna menampung *credential*/ID pengguna dan hanya menyertakan *simpletext authentication handler* yang sudah *build-in* di dalam JASIG-CAS sebagai demo saja sehingga *network administrator* yang membangun sistem SSO dengan menggunakan JASIG-CAS dapat menentukan sendiri *datastore* dan jenis *authetication handler* yang diinginkan.

Salah satu protokol penyimpanan data atau *datastore* yang sering digunakan pada JASIG-CAS adalah *Lightweight Directory Accesss Protocol* (LDAP) yang merupakan salah satu alternatif dalam menyimpan *credential/ID user* selain dari menggunakan *database*, LDAP banyak digunakan adalah karena keunggulannya dalam menjalankan fungsi sebagai *datastore* karena kecepatannya dalam proses membaca *reading entry-entry* yang berada di dalam *directory*-nya. LDAP cocok digunakan dalam sistem yang menyimpan data statik atau data yang tidak dipergunakan dalam proses transaksi seperti data *username* dan *password*.

JASIG-CAS sebagai penyedia layanan otentikasi pada sistem SSO telah mendukung berbagai jenis *Authenticator* sebagai *backend*-nya salah satunya adalah *Remote*

Accesss Dial In User (RADIUS) yang merupakan penyedia layanan otentikasi yang telah banyak didukung oleh berbagai *platform* aplikasi sehingga mempermudah proses integrasi sistem yang akan dibangun. Selain itu RADIUS juga dapat dikombinasikan dengan LDAP dalam melakukan proses otentikasi pengguna agar dapat meningkatkan keamanan data yang tersimpan dari tindakan *hacking* seperti network *sniffing* yang bertujuan mendapatkan *credential* pengguna.

Dengan menggunakan LDAP dan RADIUS dalam JASIG-CAS maka sistem SSO yang utuh dapat diwujudkan sehingga otentikasi aplikasi-aplikasi berbasis *Web* yang ada akan ditangani oleh CAS sehingga proses otentikasi akan lebih mudah karena pengguna hanya perlu mengingat *credential/ID*-nya yang terdaftar pada CAS.

1.2 Rumusan masalah

Berdasarkan uraian pada subbab di atas, rumusan masalah pada penelitian ini adalah:

1. Bagaimana membangun LDAP *datastore* guna menampung dan memusatkan *credential* pengguna.
2. Bagaimana membangun RADIUS *server* yang dapat melakukan otentikasi dengan menggunakan *credential* yang terdapat pada LDAP *datastore*.
3. Bagaimana mengintegrasikan LDAP dan RADIUS *server* sebagai otentikator pada JASIG-CAS dalam memberikan layanan SSO.
4. Bagaimana cara meningkatkan keamanan sistem SSO dari serangan *sniffing*.

1.3 Batasan masalah

Masalah yang akan dibahas dibatasi pada pembahasan mengenai analisis penggunaan *Lightweight Directory Accesss Protocol* (LDAP) bersamaan dengan *Remote Accesss Dial In User* (RADIUS) yang diimplemetasikan ke dalam *Central Authentication Service* (CAS) dalam mewujudkan layanan SSO.

Batasan pada pengembangan dan analisis sistem ini adalah sebagai berikut ini:

1. Pembuatan *datastore* pada penelitian ini adalah dengan menggunakan *Lightweight Directory Accesss Protocol* (LDAP)
2. *Authenticator* yang digunakan adalah RADIUS yang telah dikonfigurasi untuk menggunakan LDAP sebagai *datastore*-nya.
3. Sistem yang akan dibangun merupakan integrasi dari LDAP, RADIUS dan JASIG CAS dalam mewujudkan layanan SSO.
4. Peningkatan keamanan sistem melalui penggunaan SSL /HTTPS.

1.4 Tujuan Penelitian

Adapun tujuan penelitian ini adalah melakukan analisis penggunaan LDAP dan RADIUS dalam SSO pada *Central Authentication Service* yang dapat menjadi solusi terhadap masalah yang disebutkan pada rumusan masalah.

1. Membangun LDAP *datastore* guna menampung dan memusatkan *credential* pengguna.

2. Membangun RADIUS *server* yang dapat melakukan otentikasi dengan menggunakan *credential* yang terdapat pada LDAP *datastore*.
3. Mengintegrasikan LDAP dan RADIUS *server* sebagai *authenticator* pada JASIG CAS dalam memberikan layanan SSO.
4. Menambahkan fitur keamanan pada sistem SSO terhadap serangan *sniffing*.

1.5 Sistematika Penulisan

Penulisan skripsi ini tersusun dalam 5 (lima) bab dengan sistematika penulisan sebagai berikut:

BAB I Pendahuluan

Bab pendahuluan berisi latar belakang masalah, rumusan masalah, tujuan penyusunan skripsi, metodologi, dan sistematika penyusunan skripsi.

BAB II Dasar Teori

Dasar teori berisi beberapa teori yang menjadi dasar implementasi sistem SSO.

BAB III Design Sistem

Pada bab ini diuraikan deskripsi dan *design* sistem yang akan dibangun.

BAB IV Implementasi dan Pembahasan

Berisi implementasi dan evaluasi terhadap sistem SSO berbasis LDAP .

BAB V Penutup

Bab penutup berisi kesimpulan dan saran yang berkaitan dengan hasil penelitian.