

ABSTRAK

Identifikasi yang sering ditemui adalah dalam bentuk *login* yang menggunakan *username* dan *password*. Dari sini akan timbul kesulitan untuk mengelola *login* tersebut jika seorang pengguna memiliki *login* yang berbeda-beda untuk setiap sistem aplikasi, dengan demikian seseorang harus menghafalkan banyak *username* dan *password*.

Single Sign-On (SSO) merupakan fasilitas yang memberikan kemudahan untuk *user* yang melakukan *login* ketika menjelajah di *internet*. Dengan menggunakan metode SSO ini, setiap *user* hanya perlu memiliki satu *username*, satu *password*. *User* hanya perlu *login* satu kali saja agar bisa dapat menggunakan semua fasilitas yang ada di *web* utama. *User* tidak perlu menghafal banyak *account*, dan tidak perlu berulang kali *login*. Hal ini juga dapat mempermudah dalam pengorganisasian data *user* yang ada, karena menggunakan tempat penyimpanan data *user* yang terpusat. CAS digunakan untuk menangani masalah komunikasi antara *web*. LDAP digunakan sebagai sebuah protokol direktori servis, dimana semua data *user* disimpan di dalam LDAP.

Dari hasil analisa performansi *single sign on* pada *web*. Nilai *response time server* adalah sebesar 0.90 *second*, dan dalam 1 detik *server* mampu melayani 110 *request* dari *user*. Fasilitas ini dapat melayani hingga 500 *user* yang melakukan *request* secara bersamaan dalam satu waktu kepada *server single sign on*. Hal ini dikarenakan respon *error server* ketika melayani 500 *user* bernilai nol. Sedangkan waktu tercepat *server* dalam melayani *user* adalah 191ms dan waktu terlama dalam melayani *user* adalah 11864ms.

Kata Kunci : autentikasi, single sign-on, web, LDAP