Pengembangan Sistem Otentikasi SSO dengan SAML Berbasis LDAP

Indah Pratiwi[1], Yesi Novaria Kunang[2], Ari Muzakir[3]
[1,3] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitasa Bina Darma
[2] Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitasa Bina Darma
Palembang, Indonesia
[1] f.indahpratiwi@gmail.com, [2] yesi_kunang@mail.binadarma.ac.id

Abstract. Setiap universitas menggunakan banyak aplikasi web yang digunakan untuk proses belajar mengajar antara dosen dan mahasiswa. Setiap aplikasi web memiliki user account (username dan password) yang berbeda. Hal ini menimbulkan masalah bagi pengguna yang harus menghafal user account dalam jumlah banyak untuk banyaknya aplikasi web yang digunakan. Single Sign On (SSO) adalah sistem yang menggunakan satu user account yang digunakan di berbagai aplikasi web lainnya. Tetapi, sistem SSO ini kurang aman, jika ada hacker memperoleh user account SSO, maka akan terbuka semua aplikasi web tersebut. SSO dengan Security Assertion Markup Language (SAML) berbasis Lightweight Directory Access Protocol (LDAP) adalah pengembangan dari SSO yang menggunakan sistem keamanan dengan SAML dan database store LDAP.

Keywords: User Account, Single Sign On (SSO), Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP)

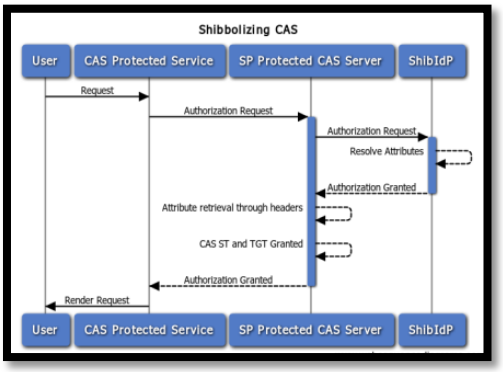
1 Pendahuluan

Setiap universitas menggunakan banyak aplikasi yang dimanfaatkan sebagai media belajar mengajar. Aplikasi-aplikasi itu menggunakan *user account* yang berbeda, sehingga menyulitkan pengguna dalam mengakses banyak aplikasi secara bersamaan. Sistem *Single Sign On* (SSO) merupakan sistem untuk otentikasi terhadap *user* dengan satu kali login akan bisa mngakses ke beberapa aplikasi tanpa harus login di masing-masing web. SSO merupakan suatu teknik dimana *user* melakukan otentikasi hanya sekali dan otomatis login ke *Service Provider* (SP) dan meningkatkan kegunaan jaringan secara keseluruhan serta memusatkan pengelolaan dari parameter sistem yang relevan. Otentikasi SSO digunakan dalam sistem atau kelompok sistem yang terpecaya [1]. SSO dengan *Security Assertion Markup Language* (SAML) berbasis *Lightweight Directory Access Protocol* (LDAP) adalah sistem pengembangan SSO dengan menggunakan sistem keamanan SAML dan *database store* LDAP sehingga memudahkan pengguna dalam mengakses beberapa aplikasi secara bersamaan dengan *satu user account* dengan aman.

Menurut Carter [2] LDAP terdiri dari : 1) *Lightweight* diartikan ringan karena menggunakan sedikit pesan diatas udara yang dipetakan secara langsung pada TCP layer, 2) *Directory* karena LDAP server dapat digunakan sebagai *backend storage* untuk *web server*, 3) *Access Protocol* karena LDAP merupakan *message-based*, *client-server protocol* yang dapat menimbulkan banyaknya *request* dan *response* mungkin datang dalam urutan yang berbeda ketika pertanyaan dimunculkan.

Tujuan penelitian ini untuk mempelajari dan menganalisis layanan *web* (*blog* dan *elearning*) serta menerapkan sistem SSO dengan SAML berbasis LDAP di Universitas Bina Darma (UBD) untuk mengintegrasikan seluruh layanan.

Batasan masalah dalam penelitian ini, adalah : 1) Sistem Operasi centOS sebagai server SAML (*Shibboleth*), Windows XP SP3 sebagai server CAS dan Ubuntu 12.04 LTS sebagai web dan server LDAP, 2) Aplikasi *web blog* (*wordpress*) dan *elearning* (*moodle*), 3) *Shibboleth* hanya dilakukan pada aplikasi *web* berbasis LDAP, dan 4) Hanya membahas otentikasi *shibboleth* [3] pada saat *login* di SSO yang berintegrasi dengan LDAP. Cara kerja s*hibboleth* dapat dilihat apada gambar 1.

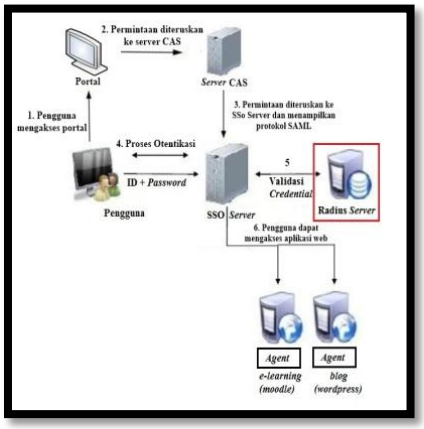


Gambar 1. Cara Kerja *Shibboleth*

E-learning adalah skema pembelajaran yang menawarkan konsep belajar menjadi *placeless*, *boarderless* dan *timeless* [4]. *Moodle* adalah sebuah aplikasi *web* gratis yang pendidik dapat digunakan untuk membuat situs pembelajaran *online* yang efektif. Sedangkan *Weblog (blog)* membantu sebagai media untuk menyebarluaskan pengetahuan melalui *internet* [5].

2 Metode Penelitian

Metode penelitian yang digunakan adalah metode penelitian tindakan (*action research*) [6], adapun tahapan-tahapannya sebagai berikut: 1) Mendiagnosa (*diagnosing*), 2) Melakukan perencanaan tindakan (*action planning*), 3) Melakukan evaluasi (*evaluating*), dan 4) Menentukan pembelajaran dari hasil penelitian (*learning*).



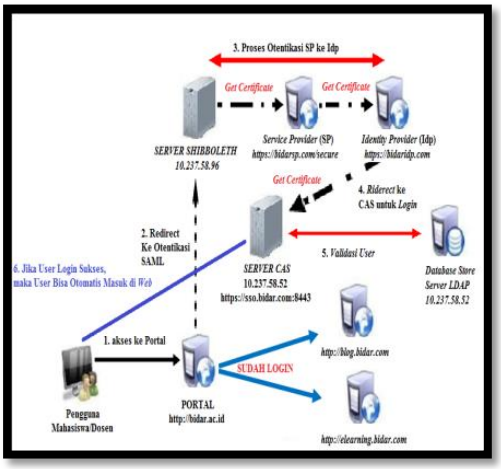
Gambar 2. Model Arsitektur Sistem

Rancangan sistem yang akan dibangun dapat dilihat pada gambar 2. Pada gambar 2 tersebut, menjelaskan pengguna mengakses portal, kemudian permintaaan diteruskan ke server CAS. Permintaan diterima di server CAS dan kemudian diteruskan ke SSO SAML. Pada form login pengguna akan mengisi sesuai dengan user account dan terjadi proses otentikasi bersamaan dengan validasi credential yang melakukan pengecekan di LDAP. Pengguna berhasi login, maka secara otomatis sudah login disemua aplikasi web.

3 Hasil dan Pembahasan

3.1 Arsitektur SSO SAML Berbasis LDAP

Hasil dari model arsitektur sistem dalam membangun *server* dan *client*, dapat dilihat pada gambar 3. Pengguna mengakses *portal* http://bidar.com akan *redirect* ke *Server Shibboleth* (SAML) dan mengalami otentikasi dengan mengkonfirmasi sertifikat yang diberikan di *Service Provider* (SP) (https://bidarsp.com) setelah itu akan di teruskan ke *Identity Provider* (Idp) dan mengkonfirmasi sertifikat Idp, setelah itu diteruskan ke login CAS. Sebelum masuk ke login CAS, pengguna harus mengkonfirmasi sertifikat. Pengguna akan login dengan menggunakan *user account* yang telah terdaftar di *Database store* LDAP. Jika sesuai maka pengguna akan mendapatkan keterangan jika sudah bisa terotentikasi dan secara otomatis sudah login di *web* (*elearning* dan *blog*) tanpa harus *login* di masing-masing *web*.

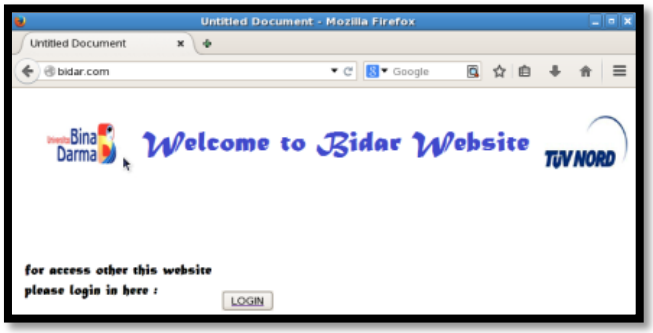


Gambar 3. Arsitektur SSO SAML Berbasis LDAP

Awalnya pengguna mengakses portal dan akan di *redirect* otentikasi ke *server* SAML menggunakan *server shibboleth*. Pada proses ini terjadi otentikasi *shibboleth-sp* dan *shibboleth* idp untuk menuju ke *server* CAS. Selanjutnya, pengguna *username* dan *password* untuk validasi *user* pada *server radius*. Setelah berhasil login, maka secara otomatis aplikasi web dapat diakses tanpa perlu melakukan login kembali.

3.2 Pengujian

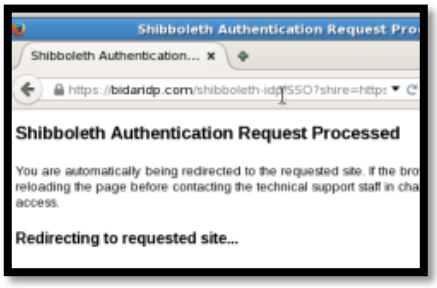
Pengujian bisa dilakukan dengan cara pengguna bisa mengakses di *browser* ke portal UBD http://bidar.com, seperti gambar 4.



Gambar 4. Portal Bidar

Setelah klik login akan redirect ke https://bidarsp.com/securere direct ke https://bidaridp.com kemudian redirect ke https://sso.bidar.com:8443/cas, setelah login di CAS maka akan mengalami otentikasi, dapat dilihat pada gambar 5. Setelah

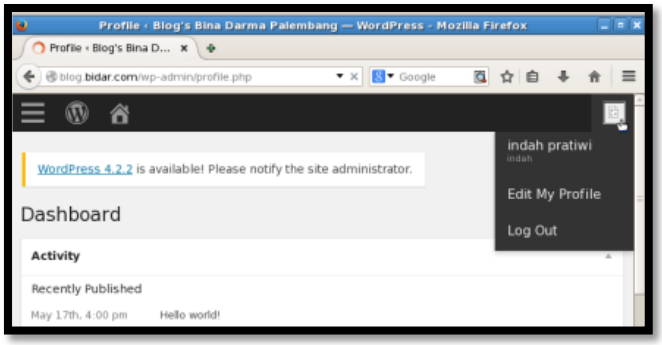
proses otentikasi selesai, maka akan muncul tampil halaman pilihan aplikasi web yang akan digunakan (*moodle* dan *wordpress*) seperti pada gambar 6.



Gambar 5. Proses Otentikasi *Shibboleth*

Gambar 6. *Access* Aplikasi *Web*

Jika pengguna ingin memilih *blog*, maka tinggal klik dan pengguna akan masuk halaman *dashboard wordpress* tanpa perlu melakukan login kembali, dapat dilihat pada gambar 7.



Gambar 7. Halaman *Dashboard Wordpress*

Jika pengguna ingin memilih *e-learning*, maka tinggal klik dan seperti *blog*, juga langsung masuk ke halaman *e-learning*, tanpa harus melakukan *login* ulang, dapat dilihat pada gambar 8.

Gambar 8. Halaman *E-Learning*

Berdasarkan gambar 7 dan 8, pengguna hanya perlu melakukan satu kali login di portal yang sebelumnya mengalami beberapa kali otentikasi di SP dan Idp dan kemudian masuk ke login CAS, sedangkan untuk mengakses dua aplikasi webtidak memerlukan login kembali. Hal ini membuktikan bahwa sistem sudah berhasil mengembangkan sistem otentikasi SSO dengan SAML berbasis LDAP.

4 Kesimpulan

Kesimpulan dari penelitian pengembangan sistem otentikasi SSO dengan SAML berbasis LDAP, yaitu:

1. Sistem mengalami otentikasi SSO pada bidarsp sebagai *Service Provider* (SP) dan bidaridp sebagai *Identity Provider* (IdP) dan pada sisi keamanan sistem ini yaitu cukup aman terutama dengan menggunakan https pada bidarsp, bidaridp dan CAS.
2. Sistem ini sangat memungkinkan diimplementasikan pada Universitas Bina Darma (UBD) berdasarkan hasil sementara yang diujikan.
3. Sistem ini menggunakan aplikasi *web* yaitu *moodle* sebagai *e-learning* dan *wordpress* sebagai *blog* dengan menggunakan LDAP sebagai *database store* SSO dan mengintegrasikan dengan *server* CAS.

Daftar Pustaka

1. Nursyamsi, "Implementasi Sistem Single Sign-On Berbasis Java," Sarjana Teknik, Departemen Teknik Elektro, Universitas Sumatra Utara, Medan, 2009.
2. G. Carter, *LDAP system administration*: O'Reilly Media, Inc., 2003.
3. S. Cantor and T. SCAVO. (2005). *Shibboleth architecture: Protocols and Profiles*. Available: http://www.immagic.com/eLibrary/ARCHIVES/TECH/INTRNET2/I050920C.pdf
4. L. A. Abdillah, "Students learning center strategy based on e-learning and blogs," in *Seminar Nasional Sains dan Teknologi (SNST) ke-4 Tahun 2013*, Fakultas Teknik Universitas Wahid Hasyim Semarang 2013, pp. F.3.15-20.
5. L. A. Abdillah, "Managing information and knowledge sharing cultures in higher educations institutions," in *The 11th International Research Conference on Quality, Innovation, and Knowledge Management (QIK2014)*, The Trans Luxury Hotel, Bandung, Indonesia, 2014.
6. S. Madya, *Teori dan Praktik Penelitian Tindakan*. Bandung, 2006.