Sistem Keamanan SSO Berbasis SAML pada Jalur Komunikasi dengan Menggunakan XML Encryption

Dwi Rita Sari[1], Yesi Novaria Kunang[2], Ari Muzakir[3]
[1,3] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Bina Darma
[2] Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Bina Darma
Palembang, Indonesia
[1] dwiritasari@yahoo.co.id, [2] yesi_kunang@mail.binadarma.ac.id

Abstract. Seiring dengan meningkatnya penggunaan aplikasi berbasis teknologi web, menyebabkan user harus mengingat sejumlah username dan password yang berbeda untuk login pada setiap aplikasi. Teknologi Sigle Sign On (SSO) merupakan authentifikasi terhadap user, dengan sekali login seorang user bisa mengakses beberapa aplikasi tanpa harus login dimasing aplikasi. Dengan menggunakan SSO pengguna hanya menggunakan satu username dan password untuk melakukan proses authentikasi terhadap aplikasi-aplikasi web yang telah terintegrasi. SSO menyediakan fasilitas Security Assertion Markup Language (SAML) yang merupakan tempat proses authentikasi dilakukan. Untuk mengatasi jalur komunikasi dari ancaman kehilangan atau kebocoran data digunakanlah XML Encryption. XML Encryption dapat menyembunyikan informasi ke bentuk yang tidak terbaca oleh manusia.

Keywords: Sistem keamanan, SSO, SAML, XML Encryption.

1 Pendahuluan

Peningkatan pengguna *internet* mendorong semakin banyaknya penggunaan aplikasi berbasis *web*. Aplikasi berbasis *web* membutuhkan autentikasi atau *login*. Sehingga, semakin banyak aplikasi *web* yang tersedia, membuat *user* harus mengingat sejumlah *usename* dan *password*. Untuk membuat proses *login* menjadi sederhana, maka diperlukan sistem yang disebut dengan *Single Sign On* (SSO).

SSO adalah sebuah sistem yang memfasilitasi penanganan *user account* untuk beberapa *server* dengan menggunakan satu *username* dan *password* saja [1]. Dengan SSO, *authentication* cukup sekali *login*, seorang *user* bisa mengakses beberapa aplikasi tanpa harus *login* di masing-masing aplikasi. Salah satu produk SSO ini adalah *Security Assertion Markup Language* (SAML) yang digunakan sebagai portal penghubung antara pengguna dengan aplikasi *web*. SAML merupakan tempat proses *authentication* dilakukan. Menurut Ragouzis, et al. [2] SAML merupakan standar yang mendefinisikan kerangka berbasis XML untuk menggambarkan dan bertukar informasi keamanan antar mitra bisnis *online*. SAML mendefinisikan standar untuk menentukan sintaks dan aturan untuk meminta, menciptakan dan berkomunikasi serta menggunakan pernyataan SAML. Pada penelitian yang telah dilakukan oleh Lewis [3]

menyebutkan bahwa otentifikasi SSO dengan menggunakan SAML akan memberikan keamanan pada proses pertukaran dan identifikasi data berbasis XML.

Masing-masing jalur komunikasi memiliki kekurangan dalam hal keamanan yang menimbulkan ancaman berupa kehilangan atau kebocoran data. Sehingga, dibutuhkan sistem keamanan pada jalur komunikasi untuk menjamin kerahasian data. Salah satunya dengan algoritma kriptografi kunci publik *(public key)* menggunakan *XML Encryption*. *XML Encryption* adalah [4] dalah elemen <*EncryptedData*> yang didalamnya memuat seluruh informasi mengenai parameter-parameter yang digunakan dalam proses enkripsi. Dalam penggunanya, elemen tersebut akan menggantikan simpul yang di enkripsi beserta seluruh simpul anak yang dimilikinya.

Pada penelitian yang telah dilakukan oleh Santoso [5] yang menyebutkan bahwa *XML Encryption,* merupakan cara mengimplemtasikan teknologi kriptografi kedalam sebuah dokumen *XML* tanpa merusak struktur dokumen tersebut.

Pada penelitian ini penulis akan mengimplementasikan pada aplikasi *web* berupa *wordpress* dan *moodle*. *Wordpress* merupakan *weblog (blog)* terpopuler yang dapat membantu sebagai media untuk menyebarluaskan pengetahuan melalui internet [6]. Sedangkan *moodle* adalah sebuah aplikasi web gratis yang pendidik dapat digunakan untuk membuat situs pembelajaran *online* yang efektif [7]. Serta membuat sistem keamanan pada jalur komunikasi menggunkan *XML Encryption.*

2 Metode Penelitian

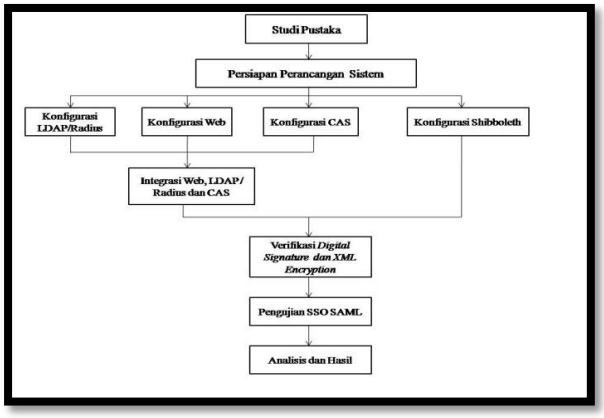
Metode penelitian yang digunakan adalah penelitian tindakan (*action research*), adapun tahapan-tahapan nya [8]: 1) Mendiagnosa (*diagnosing*), yaitu merupakan tahap awal dari penelitian, pada tahap ini akan melakukan identifikasi masalah-masalah pokok yang ada serta membuat hipotesa awal, 2) Melakukan perencanaan tindakan (*action planning*), pada tahap ini akan memahami pokok masalah yang ada, serta menyusun rencanya dan tindakan yang tepat untuk menyelesaikan permasalahan yang ada, 3) Menjalankan perencanaan tindakan (*action taking*), 4) Melakukan evaluasi (*evaluating*) terhadap tindakan yang sudah diterapkan, dan 5) Menentukan pembelajaran dari hasil penelitian (*learning*).

3 Hasil dan Pembahasan

Berdasarkan langkah-langkah penelitianyang penulis lakukan seperti yang tertera pada bagian metode penelitian, makan didapat hasil seperti yang akan penulis uraikan sebagai berikut:

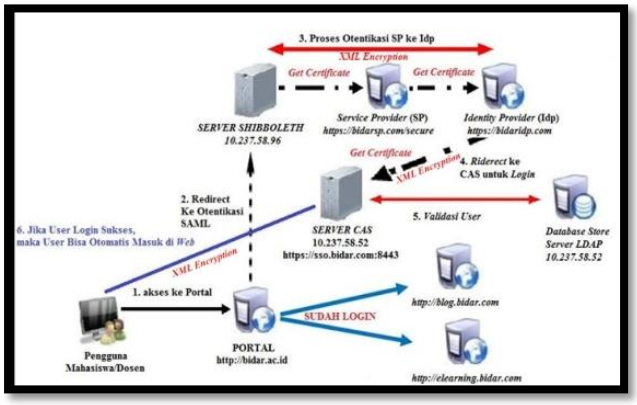
3.1 Perancangan

Pada tahap perancangan, perlu dilakukan observasi terhadap beberapa *server* dan aplikasi *web* yang digunakan sebagai *client*. Pada penelitian ini, akan dibangun beberapa *server* yang menyediakan otentikasi dan layanan akses kepada pengguna melalui protokol komunikasi. Aplikasi web yang digunakan yaitu *moodle* dan *wordpress*. Alur perancangan sistem yang akan dibangun tertera pada gambar 1.



Gambar 1. Alur Rancangan Penelitian Sistem

Pada gambar 1 menjelaskan bahwa masing-masing *server* dan *client* tersebut akan dikonfigurasi dan diintegrasikan untuk membentuk sistem otentikasi SSO berbasis SAML. Selanjutnya sistem tersebut diverifikasi dengan *Digital Signature* dan *XML Encryption*. Pengujian dilakukan untuk mengetahui sistem kemaanan SSO berbasis SAML dengan menggunakan XML Encryption pada jalur komunikasi.



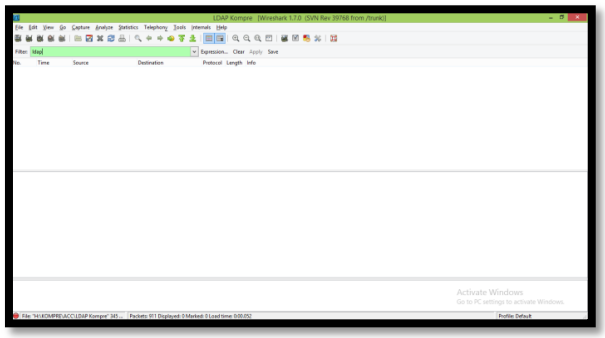
Gambar 2. Arsitektur Sistem

3.2 Hasil Rancang Bangun Sistem

Hasil dari rancang bangun sistem otentikasi SSO berbasis SAML menggunakan *XML Encryption* adalah *server* otentikasi yang terintegrasi dengan aplikasi *web blog* dan *e-learning* menggunakan mekanisme otentikasi. Arsitektur sistem lihat pada gambar 2.

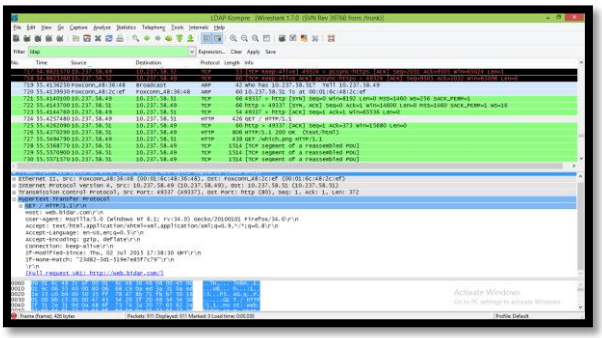
3.3 Pengujian SSO SAML Menggunakan *Backend* LDAP

Pengujian SSO SAML menggunakan *backend* LDAP ini dilakukan pada komputer *client*. Berikut ini merupakan hasil *sniffing* pada SSO SAML dengan *backend* LDAP menggunakan aplikasi *web blog* dan *e-learning*:



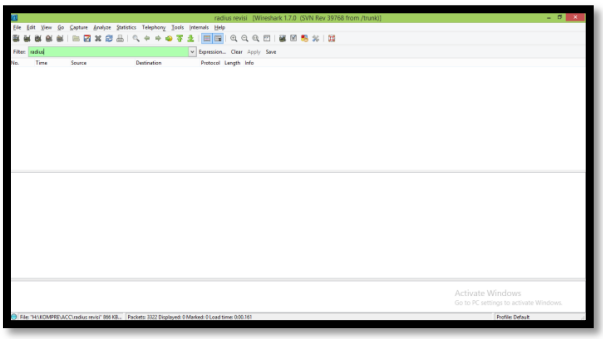
Gambar 3. Hasil *Sniffing Backend* LDAP

Gambar 3 menjelaskan pengujian yang dilakukan dengan menggunakan *backend* LDAP pada saat *login* menggunakan *server* SSO SAML dan *server* cas terenkripsi. Hal ini ditunjukkan bahwa protokol LDAP tidak terbaca ketika dilakukan *sniffing*.



Gambar 4. Paket *Login Web Blog* dan *Elearning*

Setelah LDAP berhasil login maka pengguna bisa langsung masuk kehalaman aplikasi web blog dan elearning tanpa melakukan login lagi (gambar 4). Dari hasil *sniffing* yang dilakukan proses enkripsi hanya dilakukan pada bagian content dari aplikasi web tersebut sedangkan pada bagian header web blog dan elearning tidak terenkripsi. Jadi, mekanisme login menggunakan SSO berbasis SAML dengan menggunakan backend LDAP pada aplikasi web blog dan elearning ini aman karena komunikasi menggunakan protokol yang terenkripsi.

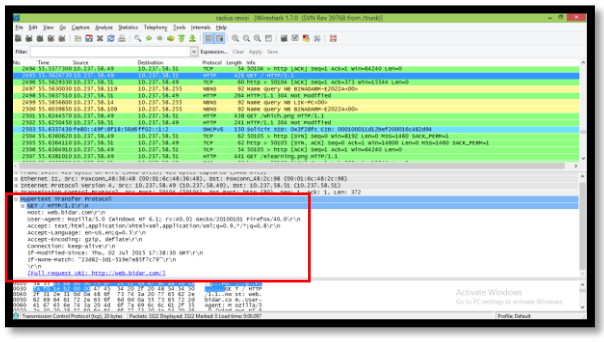


Gambar 5. Paket *Login Web Blog* dan *Elearning*

3.3 Pengujian SSO SAML Menggunakan *Backend* Radius

Pengujian SSO SAML menggunakan backend Radius ini dilakukan pada komputer client. Hasil sniffing pengguna pada SSO SAML dengan backend Radius menggunakan aplikasi web blog dan elearning dapat dilihat pada gambar 5 dan 6.

Gambar 5 menjelaskan pengujian yang dilakukan dengan menggunakan backend Radius pada saat login menggunakan server SSO SAML dan server cas terenkripsi. Hal ini ditunjukkan bahwa protokol Radius tidak terbaca ketika dilakukan sniffing.



Gambar 6. Paket *Login Web Blog* dan *Elearning*

Gambar 6 menjelaskan bahwa setelah Radius berhasil *login*, maka pengguna bisa langsung masuk ke halaman aplikasi *web blog* dan *e-learning*. Dari hasil *sniffing* yang dilakukan proses enkripsi hanya pada *content* aplikasi web, sedangkan bagian *header web blog* dan *elearning* tidak terenkripsi. Jadi, mekanisme login menggunakan SSO berbasis SAML dengan menggunakan backend Radius pada aplikasi *web blog* dan *elearning* ini aman, sehingga *username* dan *password* tidak bisa dibaca *sniffer*.

4 Kesimpulan

Kesimpulan dari penelitian mengenai *sigle sign on* berbasis SAML menggunakan sistem keamanan *XML Encryption* yaitu:

1. Sistem *sigle sign on* berbasis SAML ini dapat mengintegrasikan aplikasi web blog dan elearning, sehingga memberikan kemudahan terhadap pengguna.
2. *XML Encryption* hanya melakukan enkripsi pada *header digital signature* X509.
3. SAML 1.0 pada penelitian ini hanya membentuk kerangka kerja XML untuk memungkinkan otentikasi dan otorisasi dari SSO.
4. Enkripsi hanya pada jalur komunikasi antara *portal* SAML sampai *login* CAS. Untuk aplikasi *web*, proses enkripsi dilakukan pada bagian *content*.

Daftar Pustaka

1. W. Suseno. (2009). *Penggunaan Sistem Single Sign On dengan LDAP*. Available: http://purpalacious.arieflatu.net/2009/08/penggunaansistem-single-sign-on-dengan-ldap/
2. N. Ragouzis, *et al.* (2007). *Security Assertion Markup Language (SAM) V2.0 Technical Overview*. Available: https://www.oasis-open.org/committees/download.php/22553/sstc-saml-tech-overview.pdf
3. K. D. Lewis and J. E. Lewis, "Web single sign-on authentication using SAML," *International Journal of Computer Science Issues (IJCSI),* vol. 2, 2009.
4. T. Wahyuningrum, "Implementasi XML Encryption (XML Enc) Menggunakan Java," *Jurnal INFOTEL,* vol. 4, 2012.
5. B. Susanto. (2007). *Pemrograman XML Security*. Available: https://budsus.files.wordpress.com/2007/08/xmlsecurity.pdf
6. 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.
7. 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.
8. S. Madya, *Teori dan Praktik Penelitian Tindakan*. Bandung, 2006.