Pemanfaatan dan Implementasi Library XMLSEC Untuk Keamanan Data Pada XML Encryption

Ari Muzakir
Universitas Bina Darma
Jalan A. Yani No 12 Palembang, Indonesia
ariemuzakir@gmail.com

Abstrak
Keamanan menjadi hal yang sangat penting dalam dunia teknologi informasi. Apalagi dalam hal pertukaran data menggunakan jalur internet. XML (eXtensible Markup Language) adalah sebuah standar untuk mendefinisikan data dalam format yang sederhana dan fleksibel. Dimana web service mendukung komunikasi antar aplikasi dan integrasi aplikasi dengan menggunakan XML dan Web. Bentuk pengamanan yang diterapkan adalah dengan penggunaan teknik kriptografi kunci-publik. Implementasi yang telah dilakukan dengan menggunakan library keamanan akan memberikan kemudahan dalam membangun keamanan sistem. XML Encryption yang memanfaatkan algoritma kriptografi RSA dengan panjang kunci 1024 bit mampu memberikan perlindungan terhadap transmisi data antara client dan server web service sampai pada database. Hasil yang diperoleh yaitu pesan SOAP request terenkripsi dan mampu didekripsi dengan baik serta keamanan data tetap terjaga dengan menggunakan library XMLSEC.

***Kata Kunci** : Keamanan Data, XML Encryption, Library XMLSEC,Web Service*

1. PENDAHULUAN

Keamanan data menjadi hal yang sangat penting dalam dunia teknologi informasi. Apalagi dalam hal pertukaran data menggunakan jalur internet. Web service menggunakan teknologi XML dalam melakukan pertukaran data. *Web service*s menjadi sangat populer di *enterprise* karena kemampuannya dalam mengintegrasikan aplikasi-aplikasi yang berbeda *platform* dengan menggunakan dokumen XML. XML (*eXtensible Markup Language*) adalah sebuah standar untuk mendefinisikan data dalam format yang sederhana dan fleksibel. Dimana *web service* mendukung komunikasi antar aplikasi dan integrasi aplikasi dengan menggunakan XML dan *Web*. Faktor keamanan pada jalur komunikasi antara *client* ke *server web service* itu belum sepenuhnya terjamin. Hal ini dibuktikan dengan banyaknya faktor yang menimbulkan celah-celah ancaman terhadap *web service* tersebut seperti yang telah dilakukan oleh penelitian terdahulu.

Selain itu, pada kerahasiaan pesan yang dikirimkan melalui *web service* masih berupa data XML. Sehingga hal ini menyebabkan terjadinya data yang tidak asli ketika sampai di sisi penerima. Walaupun pesan telah di enkripsi menggunakan suatu algoritma maka bukan berarti bahwa pesan yang di terima oleh penerima benar-benar masih asli, karena bisa saja bahwa struktur pesan telah berubah ketika pesan dikirimkan atau ketika diterima.

Kemudian masalah keamanan *web service* pada kasus-kasus sebelumnya kebanyakan penelitian dilakukan pada satu model keamanan atau standar keamanan untuk *web service*. Sehingga dengan adanya sistem keamanan yang seperti ini dirasakan masih kurang memberi suatu perlindungan yang maksimal terhadap ancaman keamanan *web service* antara *client* ke *server service* sendiri walaupun secara umum sudah mampu mencukupi. Masih adanya kendala mengenai *web service* yaitu beberapa pihak yang masih merasa ragu untuk menerapkan *web service*, khususnya mereka yang menggunakan jaringan internet pada transaksinya. Keraguan ini dilihat dari tingkat keamanan dari teknologi *web service*. Aspek keamanan menjadi sangat penting untuk menjaga data atau informasi agar tidak disalahgunakan ataupun diakses secara sembarangan (Rakhim, 2010). Sehingga pada penelitian ini akan menghadirkan sebuah model dari *prototype* keamanan dalam pertukaran data pada khusunya pada dokumen XML dengan memanfaatkan *library* XMLSEC untuk *generate* sepasang kunci pada saat pengiriman data. Cara pengamanan ini dilakukan dengan cara mengenkripsi serta menyisipkan *security token* pada pesan SOAP *request* dan *response* dengan memanfaatkan XML *Encryption*.

2. TINJAUAN PUSTAKA

Beberapa penelitian yang telah dilakukan berkenaan dengan keamanan ini yaitu analisa mengenai bagaimana mengatasi tantangan pada keamanan *web service* dengan menyajikan keamanan kerangka atau *framework* terpadu yang didasarkan pada penggunaan otentikasi, otorisasi, kerahasiaan, dan mekanisme integritas pada *web service* serta untuk mengintegrasikan dan menerapkan mekanisme keamanan tersebut untuk membuat *web service* kuat terhadap serangan (Adriansyah dkk, 2005).

Selain itu penelitian terhadap keamanan *web service* juga pernah dilakukan pada integrasi data laporan kejadian perkara satuan reserse kriminal (satreskrim) yang dilengkapi dengan mekanisme keamanan internal, dimana yang dilakukan pada implementasi mekanisme keamanannya adalah menambahkan fungsi-fungsi

keamanan pada *tool* NuSOAP yang mana digunakan sebagai otentikasi serta untuk kerahasiaan pesan SOAP menggunakan kriptografi AES 128 (Kenali, 2010).

Kemudian untuk mengimplementasikan algoritma RSA untuk pembuatan pasangan kunci public dan kunci privat guna proses enkripsi dan dekripsi. Selain itu RSA juga berperan menunjukan jangkauan data yang dapat diproses. Selanjutnya mengimplementasikan *message digest* untuk fungsi hash SHA-1 yang digunakan untuk proses penandatanganan dokumen XML (Supriyanto, 2007). Penelitian lainya yaitu mengenai data XML yang dienkripsi menggunakan kunci publik dengan algoritma RSA dengan hasil implementasinya berupa dua buah program komputer yaitu findkey.exe dan crypto.exe yang dibuat menggunakan bahasa pemrograman C (Hartono, 2005).

3. METODE PENELITIAN

A. Analisa Sistem

Secara umum sistem yang akan dibangun dalam penelitian ini adalah keamanan data nilai yang akan diimplementasikan menggunkan *web service* dengan memanfaatkan XML *Encryption* dan kriptografi RSA. Pada kriptografi RSA memanfaatkan *library* XMLSEC untuk pembuatan sepasang kunci publik. Selanjutnya untuk *generate username token* juga memanfaatkan algoritma RSA-SHA1.

Pada penelitian ini dilakukan dengan melakukan analisa kebutuhan sistem yang akan diterapkan, yaitu menggunakan kebutuhan fungsional. Dalam implementasinya, web service akan dibagi menjadi dua, yaitu:

a. Client menghasilkan web service request

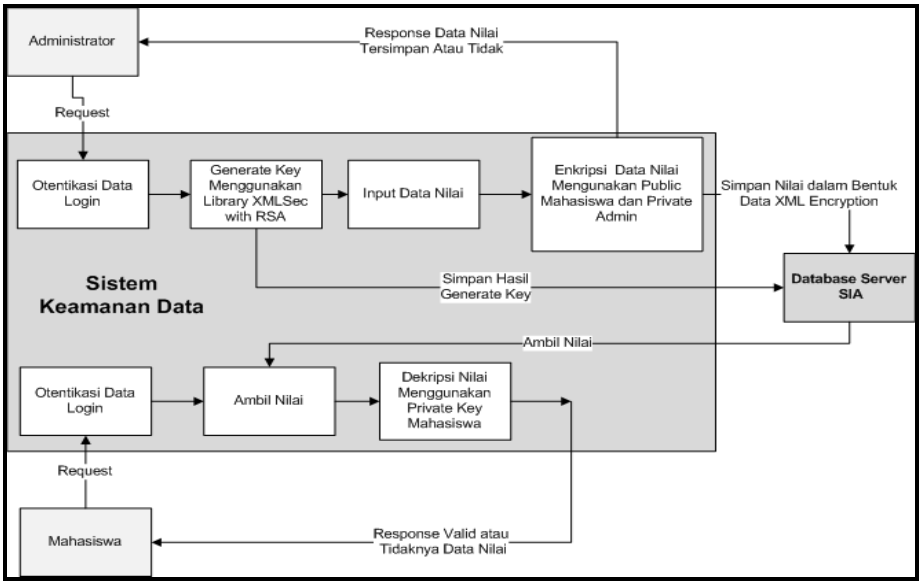
Tahap ini berkaintan dengan proses-proses yang dilakukan oleh *client* untuk melakukan request kepada *web service.*

b. Server mengotentikasi client dan mengembalikan response

Tahap ini menjelaskan beberapa proses yang dilakukan oleh *web service* setelah menerima SOAP *Request* dari *client*. Proses yang terjadi antara lain memastkan integritas pesan, mengotentikasi pengguna menggunakan username token, mengenkripsi data XML serta mendekripsi data XML menggunakan XML Encryption.

B. *Perancangan Sistem*

Sistem aplikasi yang akan dibangun memiliki arsitektur keamanan secara umum seperti pada Gambar 1 berikut, setiap permintaan dari *client* akan diotentikasi dan diamanakan. Otentikasi ini dilakukan ketika *client* berhasil melakukan *login* dan akan diberikan akses ke sumber daya sesuai dengan hak aksesnya, sedangkan konfidensialitas di gunakan pada proses enkripsi dan dekripsi.



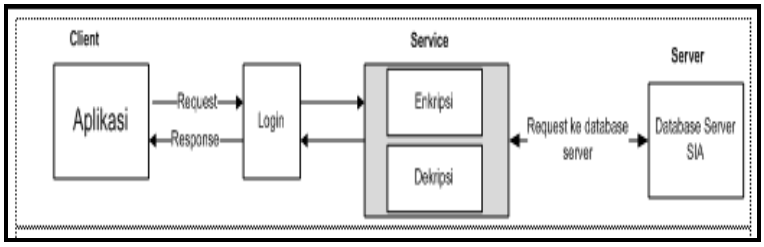
Gambar 1. Rancangan Model Keamanan Data Nilai

Pada sistem aplikasi ini, baik mahasiswa maupun petugas administrasi mengirimkan *request* (melalui jaringan internet/intranet) ke web *server* berupa pesan SOAP, jika otentikasi berhasil maka baik mahasiswa maupun petugas administrasi dapat menggunakan *service* yang telah ditentukan berdasarkan metode yang diminta ketika *login*. Perbedaan alur proses disini antara mahasiswa dan petugas administrasi adalah bahwa jika

petugas administrai bertindak sebagai pengirim nilai sekaligus memberikan keamanan terhadap isi dari dokumen tersebut namun mahasiswa bertindak sebagai pengguna dari data yang ada.

Perancangan mekanisme keamanan data ini bertujuan untuk memberikan gambaran mengenai kerahasiaan data dalam proses pembentukan sepasang kunci menggunakan *library* XMLSEC sampai proses enkripsi dan dekripsi yang melibatkan algortima kunci public RSA. Pada proses pembentukan sepasang kunci ini menggunakan panjang kunci 1024 bit. Data akan dienkripsi kemudian dikirimkan dalam format data XML yang *valid* dan disimpan di *database server*.

Secara umum, aliran proses yang dimulai dari aplikasi pengguna sampai proses penyimpanan di *database server* dapat dilihat pada Gambar 2 berikut.



Gambar 2. Rancangan Mekanisme Kerahasiaan Data *User*

Pada Gambar 2, rancanganan mekanisme kerahasiaan data nilai mahasiswa ini bertujuan untuk memberikan gambaran mengenai kerahasiaan data dalam proses enkripsi yang melibatkan kunci publik mahasiswa dan proses dekripsi yang melibatkan kunci privat mahasiswa. Enkripsi hanya digunakan oleh petugas administrasi dalam rangka menciptakan nilai yang *secure* dan rahasia. Sedangkan proses dekripsi digunakan oleh mahasiswa untuk melihat isi nilai yang hanya dapat dilihat oleh mahasiswa yang mempunyai kunci privat yang cocok dengan kunci publik yang digunakan pada saat proses enkripsi.

4. HASIL DAN PEMBAHASAN

Pengujian sistem merupakan elemen kritis dalam pengembangan sebuah perangkat lunak (*software*) karena akan merepresentasikan hasil akhir dari spesifikasi kebutuhan dari aplikasi nantinya, yaitu perancangan dan implementasi. Tujuan utama dari pengujian sistem adalah untuk memastikan bahwa hubungan antarmodul aplikasi telah memenuhi spesifikasi kebutuhan dan berjalan sesuai dengan skenario yang telah dideskripsikan sebelumnya. Pada Gambar 3 halaman utama dari sistem ini, dimana dalam halaman ini terdapat beberapa menu yang dapat dipilih. Salah satu inti dari penelitian ini yaitu pada menu data mahasiswa. Dimana pada menu data mahasiswa ini terdapat menu pilihan antara lain input nilai, *generate key* (menggunakan *library* XMLSEC), dan lihat *key* (sepasang kunci) publik dan privat

No.	NIM	Nama	Jenis Kelamin	Alamat	Kota	Telepon	Email	Password	Nilai	Generate Key	Tambah	
1	1234	Doni	L	jalan raya rawabelong raya	jakarta	02345	doni@doni.com	1234	Nilai	Generate Lihat	Hapus	Ubah
7	05142083	Usman Ependi	L	Tanjung Siapi-api	Palembang	081278965789	use_ubd@yahoo.com	usman	Nilai	Generate Lihat	Hapus	Ubah
2	2345	Didik	L	jln pandega raya	Jogjakarta	012232	Didik@didik.com	12345	Nilai	Generate Lihat	Hapus	Ubah
4	12345	muzakir	L	jogja	yogya	123	arie@mail.com	arie	Nilai	Generate Lihat	Hapus	Ubah
3	295291	Ari Muzakir	L	Sanggrahan Caturharjo	Palembang	085273221414	ariemuzakir@gmail.com	arie	Nilai	Generate Lihat	Hapus	Ubah
5	05142088	Anita Arisona	P	Pagar Alam	Pagar Alam	081368494803	anita_arisona@yahoo.com	anita	Nilai	Generate Lihat	Hapus	Ubah
6	05142086	Andri	L	Lubuk Linggau	Lubuk Linggau	085274555221	andri@gmail.com	andri	Nilai	Generate Lihat	Hapus	Ubah

Gambar 3. Halaman Utama dan Menu Sistem Keamanan

Pada tahap pengujian konfidensialitas ini, *client service* akan mengenkripsi pesan SOAP yang akan dikirimkan yaitu pada data yang akan dikirim dengan memanggil fungsi yang enkripsi yang ada di *server* dan menggunakan kunci publik dari *client*, proses enkripsi menggunakan algoritma RSA dengan panjang kunci 1024 bit. Sedangkan proses dekripsi dilakukan pada *server service* dengan menggunakan kunci privat. Selanjutnya

untuk melihat hasil pesan SOAP *request* ini yang berisi data terenkripsi dengan menggunakan metode XML Encryption. Sedangkan proses dekripsi dilakukan pada *server service* dengan menggunakan kunci privat.

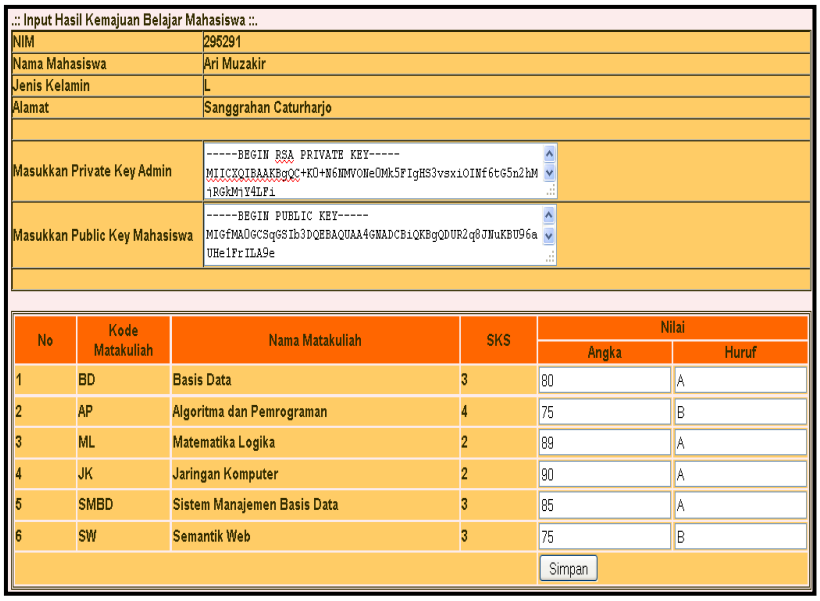
Proses pembentukkan kunci dilakukan oleh *library* dari *xmlsec* yang menghasilkan panjang kunci 1024 bit dengan menggunakan perintah berikut:

"openssl genrsa -out namafilehasil.pem 1024 "

Dengan menggunakan perintah tersebut akan menghasilkan kunci RSA seperti yang ditunjukkan pada Gambar 4.

Gambar 4. Hasil Generate Sepasang Kunci RSA dengan Panjang 1024 Bit

Hasil dari Gambar 4 diatas adalah sepasang kunci publik dan kunci privat yang akan digunakan dalam proses enkripsi dan dekripsi pesan. Kemudian untuk implementasinya, dapat dilihat pada Gambar 5 berikut, dimana ketika akan menginputkan data nilai mahasiswa diwajibkan untuk memasukkan *private key* dari pengirim dan *public key* dari penerima.



Gambar 5. Proses Input Kunci Publik dan Data Nilai Mahasiswa

Sedangkan otentikasi antara *client* dengan *server* dinyatakan dengan menggunakan *security token* pada pesan SOAP. Jika *username token* di *client* sama dengan *username token* di *server*, maka *client* dapat diizinkan untuk mengakses layanan sesuai dengan nilai parameter yang telah disisipkan pada *header*. Berikut merupakan bentuk kerangka sekaligus perintah untuk penyisipan *username token*.

```
<wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
  <wsse:UsernameToken">
   <wsse:Username>'.$user.'</wsse:Username>
   <wsse:Password Type="wsse:PasswordDigest">'.sha1($pass).'</wsse:Password>
  </wsse:UsernameToken>
</wsse:Security>
```

Gambar 6. Kerangka penggunaan *username token*

Username token sendiri akan dienkripsi menggunakan algoritma SHA1, hasilnya seperti yang ditunjukkan pada Gambar 6.

Selanjutnya setelah proses simpan dilakukan, maka data akan dilakukan enkripsi seluruh data menggunakan algoritma RSA. Hasil enkripsinya seperti seperti diperlihatkan pada Gambar 7.

```
<EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#" Type="http://www.w3.
/xmlenc#Element">
        <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripled
        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
                        <EncryptionMethod Algorithm="http://www.w3.org/2001/0
                        <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                                <KeyName/>
                        </KeyInfo>
                        <CipherData>

<CipherValue>KGPpiPVUs/MUu75cgqt7UKxmMK72N0GlJzSX36MBs4KNR7g8yF5H764yr0a053IB
KjF08slcVUrbxj4y6Z4vmdzanDEquVsFlhDljUS/0RozhvXS4jkUNTsWiDUolOSZ
l2yAjnUiPFkP8Hht0+u+QbWofad+TeyDUu7X4cEdSVk=</CipherValue>
                        </CipherData>
                </EncryptedKey>
        </KeyInfo>
        <CipherData>
                <CipherValue>/F36rJQctLGDh2R/y/gc6ZkkePUJPtjzJJaGRfFfamUL0ZeJy
cobm4l50rmMrVyER2CTo/Vw0NYc6EXTWlNIaraL+NT0Ig83058ZNF4lmFlWpRtQB
0ccQPKmVUKUjUa/u9Parvoslek1ZPf0DJRk2B/A7v6oIzSJsfBW58Y+CFJ3GQD9/
J3QHR0nHy8PxR8eyx55JLF0jFjatf6vv/2IDcZtAQjwcIBag42zrAaYpTVcDTtgF
MniaPbbftYBJtktsMDGmzEFlDDe8jCNSGMqwOB7Hl3GKgnBpwJtZCqGlcaBKCWv0
f7CcaV4+D/hTwOXT4h+Ai+GHSgp6l0tkeZi2OGfNRl0/fp2XTSqrW/hChvaSuz/y
6NDIHmA0FenrBnAbE1Zd2wXmZv5Ptq5FpG0g6fb8Rtwr5bHPc0dX0wD4frHoaVsC
7vkDvGNiLLLn/z85nlbC5w==</CipherValue>
        </CipherData>
</EncryptedData>
```

Gambar 7. Hasil Enkripsi Nilai Mahasiswa dalam Format XML

Dari Gambar tersebut dapat dilihat bahwa ketika data dikirimkan, maka *client* akan memanggil fungsi keamanan yang ada di *client service* yaitu *library* class_wss.php, selanjutnya ketika data dikirimkan dari *client service*, maka data SOAP akan disisipkan *username token* yang mana akan dicocokkan dengan *username token* milik *server service*, selain itu pesan SOAP akan ditandatangani dan dienkripsi data. Hasil enkripsi dari data XML ini dapat dilihat dari elemen <*EncryptedData*> dan </*EncryptedData*>. Kemudian pesan SOAP yang berisi data yang telah dienkripsi terlihat pada elemen <*CipherData*> dan </*CipherData*>. Elemen ini mengindikasikan bahwa data telah berhasil dienkripsi dan dipastikan data yang dikirimkan dalam keadaan aman.

5. KESIMPULAN

1. Desain dan implementasi modul yang telah dilakukan dengan menggunakan *library* keamanan serta dukungan *library* XMLSEC sebagai *library* pendukung dan *library* class_wss yang dibangun mampu mengatasi masalah keamanan pada proses pengiriman yaitu keamanan otentikasi dan konfidensialitas pesan SOAP *request* yang dihasilkan.
2. Hasil dari implementasi mengindikasikan bahwa konfidensialitas dapat terpecahkan dengan menerapkan konsep keamanan berbasis *library* keamanan yaitu XML *Encryption.* Hasil pesan SOAP *request* pada proses pengiriman dapat memenuhi standar keamanan *web service*, dimana data ketika dikirimkan dalam keadaan terenkripsi dengan menggunakan *library* class_wss yang telah dibangun.
3. Pengujian yang dilakukan pada *web service* dengan menerapkan model *library* class_wss sebagai *library* keamanan *web service* yang dibangun memberikan hasil yang baik, yaitu pesan SOAP *request* pada saat dikirimkan dalam bentuk terenkripsi dan mampu didekripsi.

DAFTAR PUSTAKA

Rakhim, R ,2010, *Keamanan Web Service Menggunakan Token*, Tesis S2 Magister Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.

Adriansyah, W. Arifandi, dan, N. Wicaksono ,2005, *Keamanan Web Service*, Teknik Informatika, Institut Teknologi Bandung, Bandung.

Kenali, Erwin ,2010, *Implementasi Web Service untuk Integrasi Data Satuan Reserse Kriminal (Studi Kasus Polda Lampung)*, Tesis S2 Magister Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.

Supriyanto, Aji, 2007, *Otentikasi Dokumen XML menggunakan Algoritma RSA dan Hash SHA-1*, Tesis S2 Magister Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.

Hartono,Budi ,2003, *Pemakaian kriptografi kunci publik dengan algoritma RSA untuk keamanan data XML*, S2 Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.