METODE PENGAMANAN DATA DALAM *WEBSERVICE* MENGGUNAKAN METODE *XML SIGNATURE* DAN *XML ENCRYPTION*

Nazori Agani[1], Chaidir Kurnia Thoullah[2]

Program Studi Magister Ilmu Komputer, Program Pascasarjana, Universitas Budi Luhur
Jl. Ciledug Raya, Petukangan Utara, Kebayoran Lama, Jakarta Selatan, 12260
Telp. (021) 5853753, Fax (021) 5866369
[1]nazori.agani@budiluhur.ac.id, [2]chaidir.kurnia@sprintasia.net

ABSTRAK

Saat ini perkembangan teknologi di dunia sangat berkembang pesat dengan bermunculannya teknologi informasi yang semakin moderen dan canggih , semakin banyak pula permintaan dan kebutuhan komunikasi data dengan cepat dan aman melalui web , salah satu metode yang sedang berkembang saat ini adalah webservice , webservice menjadi trend dalam teknologi web karena teknologi ini dapat melakukan komunikasi multiplatform , perantara antar multiplatform ini menggunakan eXtensible Markup Language (XML) dalam berkomunikasi, karena XML mudah untuk dibaca oleh macam-macam bahasa pemograman seperti ASP.Net, PHP dll, dikarnakan komunikasi data tersebut sangat mudah dibaca , maka dengan itu semakin mudah juga XML ini dimanipulasi seperti serangan yang dilakukan berupa pengintaian, perusakan maupun pencurian data, salah satu penyelesaian terbaik adalah dengan membuat data tersebut tidak dapat dibaca orang lain dan dilakukan validasi chek apakah data tersebut sama pada saat dikirim dan diterima, Pengamanan tersebut dapat dilakukan dengan menggunakan salah satu teknik kriptografi yaitu enkripsi, dan untuk menjaga ke-absahan data yang dikirim sama dengan data yang diterima kita akan menambahkan XML Signature untuk menambah keamanan data tersebut , XML Signature digunakan untuk menyediakan kepastian terhadap integritas data (Content of message) dalam dokumen serta membuat data dan menguji tandatangan elektronik tersebut (digital signature), dengan Prototipe aplikasi ini akan dikembangkan menggunakan UML (Unified Modeling Language) dan metode Prototyping, Protoyping ini akan diuji dengan Fungsional test dan User Accepted, dan penelitian ini diharapkan akan menjaga kerahasiaan data dalam webservice khususnya untuk menjaga kevalidan data dan kerahasiaan data pada saat pengiriman data.

Kata Kunci : *Prototyping, Web Service , XML Signature , Kriptografi, XML Encription*

I. PENDAHULUAN

1.1. Latar Belakang

Saat ini perkembangan technologi di dunia sangat berkembang pesat dengan bermunculannya technologi informasi yang semakin modern dan canggih, semakin banyak pula permintaan dan kebutuhan akan komunikasi data dengan cepat dan aman melalui web, *webservice*sedang menjadi *trend* di dalam teknologi web karena teknologi ini dapat melakukan komunikasi multiplatfrom, jadi *Webservice* ini sangat banyak digunakan dalam perusahaan – perusahaan yang memerlukan komunikasi data dengan berbeda platform namun berbasis web, multiplatfrom merupakan salah satu kelebihan dari *Webservice* ini, ada beberapa kelebihan – kelebihan *Webservice* seperti mudah dibaca baik, untuk berinteraksi dengan platfrom lain *Webservice* menggunakan *eXtensible Markup Language* (XML) dalam berkomunikasi , karena XML mudah dibaca menggunakan komputer maupun dengan mata telanjang membuat banyaknya celah – celah ancaman terhadap data XML pada *Webservice* karena mudahnya untuk membaca format XML[1].

1.2. Masalah Penelitian

Didalam masalah penelitian ini penulis akan menjelaskan identifikasi masalah yang ada sehingga dapat diketahui permasalahan yang terjadi pada keamanan komunikasi dalam menggunakan XML dan ancaman – ancaman yang bisa mengancam keamanan komunikasi data menggunakan XML format tersebut, pembatasan masalah pada penelitian dibuat agar penelitian tetap focus pada materi dan tujuan awal penelitian, peneliti juga hatus membuat rumusan masalah sehingga yang diajukan semakin jelas dan terarah dalam menjelaskan suatu penelitian.

1.3. Identifikasi Masalah

Setelah menganalisis berdasarkan pengalaman yang ada mengenai perkembangan teknologi informasi khususnya diteknologi komputerisasi, maka penulis mengidentifikasi teknologi yang diterapkan serta adanya hal – hal melatarbelakangi penulisan.

1.4. Pembatasan Masalah

Dalam pembatasan masalah penulis melakukan pembatasan dalam pembahasan tentang penulisan ini, ruang lingkup dalam pembahasan ini hanya meliputi pemberian *XML Signature* pada XML Format dan memberikan extra keamanan dengan enkripsi pada data XML yang akan dikirimkan, agar keamanan data dapat terjamin dan komunikasi *Server to Server or Client to Server* dapat terjaga dengan baik.

1.5. Tujuan Penelitian

1. Untuk menjaga keamanan data khususnya pengembangan XML dalam komunikasi data dengan metode SOA
2. Untuk menjadikan format XML tersebut salah satu alternative terbaik untuk komunikasi data yang aman dan terpercaya berbasis web.

1.6. Manfaat Penelitian

1. Memberikan Masukan dan *alternative* metode dalam menyelesaikan masalah dalam keamanan data dalam *Webservice* khususnya dengan menggunakan XML (*SOAP*atau*WSDL*)
2. Menjadikan konsep SOA dengan menggunakan XML sebagai komunikasi data adalah *alternative* terbaik, dikarnakan sudah memenuhi faktor – faktor seperti keamanan, akses cepat dan mudah digunakan dan multiplatfrom.

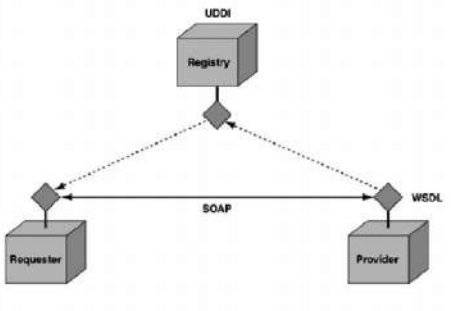
II. LANDASAN TEORI

Konsep arsitektur yang mendasari teknologi *Web service* adalah *Service Oriented Architecure* (SOA). Dalam aritektur ini, suatu aplikasi dimodelkan sebagai komposisi dari sekumpulan *service* yang disediakan oleh suatu komponen[2]. Lokasi keberadaan komponen tersebut dapat ditemukan oleh *client* secara dinamis, dalam arti tidak dinyatakan secara statis tetapi menggunakan mekanisme *discovery* untuk mencari keberadaan komponen tersebut. Demikian pula, client dapat meminta (*invoke) service* tersebut secara dinamis[3].

Dalam arsitektur ini, SOA mendefinisikan 3 peran berbeda yang menunjukkan peran dari masing-masing komponen dalam sistem, yaitu :

- *Service provider*, yaitu suatu entitas yang menyediakan interface terhadap sistem yang menjalankan suatu sekumpulan tugas tertentu. *Service provider* dapat merepresentasikan statu entitas bisnis ataupun suatu komponen software yang *reusable*.
- *Service requestor* , yaitu suatu entitas yang meminta/memperoleh (dan menemukan) *software service* dalam rangka meyelesai kan suatu tugas tertentu atau menyediakan solusi bisnis tertentu.
- *Service registry* , yaitu entitas yang bertindak sebagai penyimpan (*repository*) suatu *software service* yang dipublikasikan oleh Service provider[4].

W3C mengembangkan draft arsitektur *web service* yang terdiri dari beberapa teknologi yang saling berhubungan, seperti ditunjukkan dalam gambar 1. Berdasarkan gambar tersebut, web service tersusun dari beberapa komponen yang semuanya berbasis XML (*Extensible Markup Language*) yaitu *SOAP, WSDL dan UDDI*[5].



Gambar 1. Arsitektur *Web Service*

III.METODOLOGI DAN DESIGN PENELITIAN

3.1.MetodePenelitian

Metode yang digunakan dalam penelitian ini adalah metode penelitian deskriptif kualitatif. Selain metode deskriptif kualitatif penelitian ini juga mengguanakan metode *requeirment* untuk mengevaluasi apakah *system* yang dibuat sudah memenuhi kebutuhan *user*. Metode penelitian kualitatif menggunakan untuk meneliti pada tempat alamiah dan penelitian tidak membuat perlakuan, karena peneliti dalam mengumpulkan data berdasarkan pandangan dari sumber data atau user, bukan hanya dari pandangan peneliti, dalam penelitian kualitatif peneliti melakukan teknik pengumpulan data dengan cara observasi berperan serta dan in wawancara mendalam makan penelitan harus berinteraksi dengan sumber data, walaupun penelitian berfokus pada satu *case* atau tidak secara general dalam melakukan penelitian, bukan berarti penelitian ini hanya bisa diimplementasikan di satu tempat, tidak menutup kemungkinan hal ini bisa di terapkan di tempat lain, pada dasarnya technologi yang di dalam dapat dilakukan di semua tempat hanya berbeda dimana akan di pergunakannya. Secara konsep dan technologi akan sama.

3.2. MetodePengumpulan data

1. Pengumpulan data primer

Teknik pengumpulan data dengan cara melakukan pembagian daftar pertanyaan langsung maupun secara online sehingga data yang penulis kumpulkan menggambarkan keadaan yang sebenernya, alat penelian yang penulis gunakan adalah kuesioner, alasan yang mendasari pemakaian alat penelitian tersebut adalah kuesioner merupakan salah satu alat penelitian yang dapat digunakan untuk mekakukan pendekatan penelitan survey

2. Pengumpulan Data Sekunder

Data sekunder penulis dapat dari mengamati data, membaca mempelajari dan mengutip dari buku *literature*, *paper* jurnal serta sumber – sumber lain berhubungan erat dengan penulisan.

3.3. MetodePerancangan

Untuk memodelkan sebuah perangkat lunak, metode *prototyping* memiliki tahapan–tahapan didalam proses pengembangannya. tahapan inilah yang menentukan

keberhasilan dari sebuah aplikasi, pengembang perangkat lunak harus memeperhatikan tahapan dalam metode *prototypng* agar *software* dapat diterima oleh user, dan tahapan – tahapan dalam *prototyping.*

3.4. TahapanPengujian

Testing yang akan dilakukan ialah *Black Box* Testing. Teknik ini bertujuan untuk menunjukan fungsi sistem tentang cara beroperasinya, apakah pemasukan data keluaran telah berjalan sebagaimana yang diharapkan dan apakah informasi yang disimpan secara eksternal selalu dijaga kemutakhirannya. Pengujian *Black Box.*

IV.PEMBAHASAN HASIL PENELITIAN

4.1. Analisis dan Interprestasi

Pada bagian ini akan dibahas peroses pengolahan data dari pertanyaan-pertanyaan yang disebarkan kepada user dan tenaga ahli yang ada. Karena yang diukur adalah sikap responden terhadap pentingnya keamanan *webservice* dengan menggunakan komunikasi data dengan XML maka tipe yang akan digunakan oleh peneliti adalah *Ranting Scale.* Setelah tahap pengukuran dan validasi dilanjutkan tahap perancangan *prototype* program *XML Signature* dan *XML Signature* pada format XML.

Dari penjelasan tersebut di dapatlah klasifikasi responden penelitian untuk mengukur kinerja sistem (*system performance*) sebagai berikut.

Tabel 1. Data Responden Penelitian

Penjelasan	Klasifikasi Respon	Jumlah	Presentase
JenKel	Wanita	3	20%
	Laki-Laki	12	80%
	Jumlah	15	100%
Usia	20 – 25	4	27%
	26 – 30	7	47%
	31 - 40	3	20%
	41 - 45	1	7%
	Jumlah	15	100%
Pendi	(S1)	10	67%
	(S2)	5	33%
	(S3)	0	0%
	Jumlah	15	100%

Pada Tabel diatas dijelaskan bahwa jumlah responden yang di dapat berjumlah 15 responden terdiri dari 1) Responden dengan title *Senior Officer & Officer* sebanyak 10 orang, 2) Responden dengan tilte *Manager* sebanyak 4 Orang, 3) Responden dengan title *Head Manager*sebanyak 1 Orang, dilihat dari table tersebut terlihat mayoritas bergelar S1 (Sarjana) dikarnakan mayoritas adalah level *Officer* dengan rage usia 22 tahun - 30 tahun, dan S2 (Magister) rata-rata pada level *Manager* dengan range usia 28 tahun – 40 tahun , usia mayoritas responden adalah laki – laki karena mayoritas yang bekerja dalam IT di Rabobank adalah laki-laki.

1. Rekapitulasi data KuesionerResponden

Dari Tabel 1 dapat dijelaskan jumlah reponden adalah 15 orang dan bisa di analisa dan ditabulasikan sebagai berikut:

Jumlah skor kriteria (apabila setiap item mendapat skor tertinggi) = (skor tertinggi tiap item = 5) x (jumlah item = 5) x (jumlah responden = 15) adalah 375. Maka, jumlah skor pengumpulan data = 228. Dengan demikian yang sesuai dengan kebutuhan , menurut 15 responden , yaitu :

288/375 * 100 = 76.8%

Dan secara konitium didapatkan kategori sebagai berikut :

Tabel 2. List Kategori

0	20%	40%		60%	80%	100%
	Buruk	Kurang		Cukup	Baik	Sangat Baik

4.2. Analisis Kebutuhan

Setelah melakukan observasi secara primer dan skunder maka didapat secara kebutuhan yang diperlukan guna membangun sebuah *prototype* yang diinginkan.

Tabel 3. Analisa Kebutuhan

No	Analisa Kebutuhan (*Non Functional*)
1	Proses webservice maximal 5 detik
2	*Key Encryption* di generate 5 menit sekali secara Otomatis
3	Aplikasi *webservice* harus menggunakan windows base
4	*Key Encryption* harus di *Encryption* pada database penyimpanan
5	Proses *XML Signature* & *XML Encryption* harus dibawah 1 detik
6	*Upgrade Webservice* ke WCF
Penyusun	

Berdasarkan table diatas merupakan gambar dari Elisitasi Tahap 1, yang disusun berdasarkan hasil wawancara penulis dengan *Head corebanking platform* mengenai seluruh rancangan *prototype* Metode Keamanan *webservice* di PT.Rabobank Internasional Indonesia yang diusulkan.

1. *Requirement elicitation* tahap 2

Elistasitahap II dibentuk berdasarkan Elisitasi tahap I yang kemudian diklasifikasi melalui metode MDI, berikut penjelasan dari beberapa *requirement* yang diberiopsi *Inessential* (I) dan harus di eliminasi :

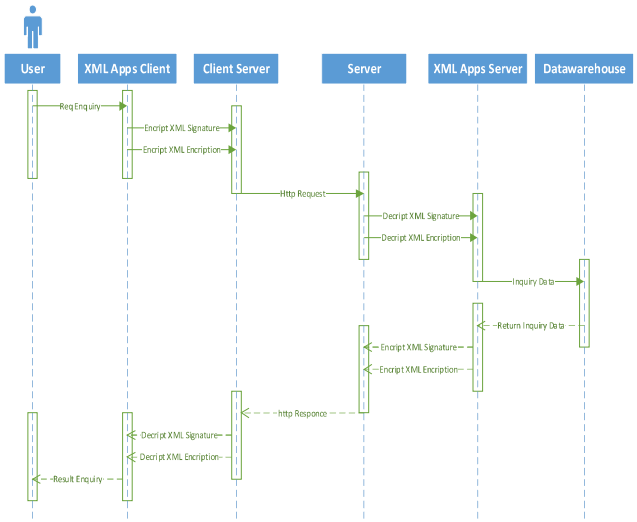
Tabel 4. Analisa Kebutuhan (*Non Functional*)

No	Analisa Kebutuhan (Non Functional)	M	D	I
1	Proses webservice maximal 5 detik	V		
2	Key Encryption di generate 5 menit sekali secara Otomatis	V		
3	Applikasi webservice harus menggunakan windows base	V		
4	Key Encryption harus di Encryption pada database penyimpanan		V	
5	Proses XML Signature & XML Encryption harus dibawah 1 detik		V	
6	Upgrade Webservice ke WCF			V

Keterangan:
M (*Mandatory*) = Penting
D (Desirable) = Tidak Terlalu Penting
I (Inessential) = Tidak Penting

4.3. Sequence Diagram

Diagram Class dan diagram Object merupakan suatu gambaran model statis. Namun ada juga yang bersifat dinamis, seperti *Diagram Interaction*. *Diagram sequence* merupakan salah satu *diagram Interaction* yang menjelaskan bagaimana suatu operasi itu dilakukan, *message* (pesan) apa yang dikirim dan kapan pelaksanaannya. Diagram ini diatur berdasarkan waktu. Obyek-obyek yang berkaitan dengan proses berjalannya operasi diurutkan dari kiri ke kanan berdasarkan waktu terjadinya dalam pesan yang terurut.



Gambar 2. *Sequense ProsesXML Signature* dan *Encription*

Dari table *sequence* diatas dapat dilihat proses berjalannya aplikasi dari *client to server*, dimana ada seorang *actor* (*user*) yang melakukan *inquiry* data, dalam proses ini user ingin melakukan proses *inquiry* data dengan user memasukkan kode nasabah dan akan mendapatkan keterangan seperti saldo, alamat dan dll, proses pertama user memasukan nomor rekening , kemudian dari user mengirimkan request dan masuk kedalam *XML_Apps_Client*, *XML_Apps_Client* kemudian melakukan *XML Signature*

4.4. Pengujian Model *Prototipe*

A. *Functional Testing*

Pengujian *Functional* bisa diartikan secara sederhana bahawa untuk menguji kemampuan perangkat lunak dalam menyediakan fungsi sesuai dengan kebutuhan pengguna, ketika digunakan dalam kondisi tertentu, penulis menggunakan indicator pengujian functional testing mengacu pada indicator fungsionalitas dari aplikasi tersebut apakah berjalan dengan baik

B. *Acceptance Testing*

Pengujian *Acceptance Testing* sebenarnya hampir sama dengan *Functional Testing*, perbedaanya terletak pada tester atau penguji applikasi yang kita biasa sebut QA (*Quality Assurance*) dan biasanya proses peng-inputan dalam applikasi.

V. PENUTUP

A. Kesimpulan

Dalam Perkembangan jaman *technology* komunikasi data antar *server* semakin canggih salah satunya adalah *webservice*, dengan konsep ini kita dengan mudah bisa mengirimkan data ke *multiplatform*, namun dikarnakan mudahnya komunikasi ini semakin rentan juga keamanan data yang dikirim oleh *webservice* tersebut , dengan keamanan yang ditawarkan penulis akan membantu meningkatkan keamanan dalam berkomunikasi dengan menggunakan *webservice* dengan data XML, berikut adalah kesimpulan yang diambil dari pembahasan diatas :

1. Dengan*XML signature* kita bisa melakukan validasi dan memastikan data yang dikirimitu sama dengan data yang diterima.
2. Kriptografi ditambahkan dalam metode *XML Signature* agar data XML tidak mudah untuk dibaca.
3. Dengan kombinasi *XML Signature* dan Kriptografi akan menambah keamanan dalam menggunakan *webservice*.

B. Saran:

1. *XML Signature & XML Encription* akan terjaga keamananya apabila Key Encription selalu berubah secara otomatis.
2. Tidak boleh *sharing password* sesama karyawan untuk menjaga keamanan data.
3. Semoga dengan diimplementasikannya Model Keamanan data
4. Pada webservice ini dapat berguna untuk perkembangan kedepan.

DAFTAR PUSTAKA

[1] Bernard Renaldy Suteja, S.Kom, M.Kom," Implementasi XML Signature pada dokumen XML untuk Transkrip Nilai Online",Univeritas Kristen Maranatha,bernard.rs@eng.maranatha.edu, bernardjogja@gmail.com

[2] Arisandi, Fachry, Prof. Dr. Ir. Harso Supangkat M. Eng, "Implementasi Service Oriented Architecture (SOA) pada pengembangan Sistem Pembelajaran Mobile". Konferensi Teknologi Informasi dan Komunikasi Untuk Indonesia e-Indonesia Initiative (eII2011), CGET, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Email : if17027@student.if.itb.ac.id. 2011

[3] Ilhami Gorgun, 2004. Deploying dan Invoking Secure Web Service Over JXTA Framework. The Graduate School og Natural dan Applied Sciences Of Middle East Technical University.

[4] Josuttis, Nicloai M., "SOA In Practice", O'Relly,pp 210.2007

[5] Prasetyo, HendroJoko, Jurnal, "Implementasi Service Oriented Architecture (SOA) Menggunakan Teknologi Web Service" : Universitas Widya Dharma Klaten Yogyakarta, E-mail : Hendrojogja@yahoo.com.