

**Model Implementasi Keamanan *Web Service*
dengan Kriptografi dan Tanda Tangan Digital
Pada Sistem Informasi Akademik :
Studi Kasus Universitas XYZ**

TESIS



Oleh:

Indra Lasmana

1111601306

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCA SARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2014

**Model Implementasi Keamanan *Web Service*
dengan Kriptografi dan Tanda Tangan Digital
Pada Sistem Informasi Akademik :
Studi Kasus Universitas XYZ**

TESIS

Diajukan sebagai salah satu persyaratan
untuk mendapatkan gelar Magister Ilmu Komputer (MKom)



Oleh:

Indra Lasmana

1111601306

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR

JAKARTA

2014



PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Indra Lasmana
NIM : 1111601306
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Topik/Judul Tesis : Model Implementasi Keamanan *Web Service* dengan Kriptografi dan Tanda Tangan Digital pada Sistem Informasi Akademik : Studi Kasus Universitas XYZ.

Jakarta, 26 Februari 2014

Tim Penguji

Tanda Tangan

Ketua,

Dr. Moedjiono, M.Sc

Anggota,

Utomo Budiyanto, M.kom, M.Sc

Pembimbing,

Dr. Ir. Nazori AZ, M.T

Ketua Program Studi

Dr. Ir. Nazori AZ, M.T



PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Indra Lasmana
NIM : 1111601306
Program Studi : Magister Ilmu Komputer
Program : Rekayasa Komputasi Terapan

menyatakan bahwa Tesis yang berjudul:

Model Implementasi Keamanan Web Service dengan Kriptografi
dan Tanda Tangan Digital Pada Sistem Informasi Akademik :
Studi Kasus Universitas XYZ

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik pihak lain.
2. Saya izinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 26 Februari 2014


(Indra Lasmana)



ABSTRAK

Seiring dengan perkembangan teknologi, perguruan tinggi maupun universitas sudah memiliki sistem informasi akademik. Pada saat ini pengembangan aplikasi yang ditanamkan pada *mobile device* memungkinkan untuk dilakukan. Dengan teknologi *web service* yang memiliki kemampuan untuk pertukaran data antarplatform yang berbeda, baik perbedaan dari segi bahasa pemrograman maupun sistem operasi yang digunakan. Akan tetapi distribusi data dengan teknologi *web service* rentan terhadap penyadapan atau pencurian data, serta manipulasi data oleh pihak yang tidak berhak. Oleh karena itu, dibutuhkan suatu cara untuk mengamankan distribusi data pada *web service* agar data atau informasi tidak dapat dibaca oleh orang yang tidak berhak dan agar dapat diketahui jika data sudah dimanipulasi atau mengalami perubahan. Berdasarkan permasalahan di atas, penelitian ini membahas tentang teknik kriptografi dan tanda tangan digital (*Digital Signature*) untuk keamanan data atau informasi. Adapun algoritma kriptografi yang di gunakan adalah RSA (Rivest Shamir Adleman) dan Fungsi Hash MD5. Pada penelitian keamanan data pada *web service* yang telah diimplementasikan, hasil pengujian kualitas perangkat lunak dengan model ISO 9126, yang meliputi *functionality*, *reliability*, *usability*, dan *efficiency* menunjukkan kriteria sangat baik berdasarkan kuesioner yang telah diisi oleh responden. Sedangkan pada pengujian *black-box testing* kinerja *web service* berjalan dengan baik sesuai dengan hasil yang diharapkan.

Kata Kunci : *kriptografi, digital signature, rsa, web service, xml-rpc, fungsi hash*

ABSTRACT

Along with the development of technology, colleges and universities already have academic information system. At this time the development of applications that are embedded on a mobile device allows to do. With web services technology that has the ability to exchange data between different platforms, both in terms of differences in programming language or operating system used. However, the distribution of the data with web service technologies are vulnerable to eavesdropping or theft of data, as well as the manipulation of data by unauthorized parties. Accordingly, we need a way to secure the distribution of the data on a web service so that the data or information can not be read by unauthorized people, and it can be seen if the data has been manipulated or changed. based on the above problems, this study discusses the cryptographic techniques and digital signatures for security of data or information. The cryptographic algorithms used are the RSA (Rivest Shamir Adleman) and MD5 Hash Functions. In the study of data security in the web service that has been implemented, the results of testing the quality of the software by the ISO 9126 models, which include functionality, reliability, usability, and efficiency showed excellent criterion by respondents completed questionnaires. While the black-box testing of web service performance testing goes well in accordance with the expected results.

Keyword : cryptography, digital signature, rsa, web service, xml-rpc, hash function

KATA PENGANTAR

Assalamu'alaikum Warahamtullahi Wabarakatuh.

Segala puji hanya untuk dan kepada Allah swt, yang memberikan kekuatan, izin dan pertolongan, hingga akhirnya tesis yang berjudul “MODEL IMPLEMENTASI KEAMANAN *WEB SERVICE* DENGAN KRIPTOGRAFI DAN TANDA TANGAN DIGITAL PADA SISTEM INFORMASI AKADEMIK : STUDI KASUS UNIVERSITAS XYZ” ini dapat diselesaikan. Dalam penyusunan tesis ini, penulis ingin menyampaikan ucapan terima kasih kepada:

1. Allah swt, atas segala rahmat, izin dan pertolongan-Nya dalam proses penyusunan ini dari awal hingga akhir.
2. Kedua orang tua, Zainal Hakim dan Rahmah yang telah memberikan dukungan penuh serta doanya.
3. Isteri saya, Hairunnisa yang selalu setia menemani dan memberikan masukan dalam penyusunan tesis ini.
4. Muhammad Habibi, selaku anak tercinta yang telah memberikan motivasi dan semangat dalam penyusunan tesis ini.
5. Bapak Dr. Ir. Nazori AZ, MT, selaku pembimbing yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini.
6. Bapak Dr. Moedjiono, M.Sc, selaku Direktur Program Pascasarjana yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini.
7. Serta semua pihak yang tidak dapat dituliskan satu persatu.

Sebagai seorang manusia yang selalu memiliki kekurangan, penulis menyadari bahwa naskah akhir tesis ini masih banyak kekurangan. Oleh karena itu demi menyempurnakan naskah tesis ini, segala bentuk saran dan kritik mohon dapat dikirimkan melalui *e-mail* ke alamat indralasmana@gmail.com.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Jakarta, Februari 2014

Indra Lasmana

DAFTAR ISI

	Halaman
ABSTRAK	i
KATA PENGANTAR.....	iii
DAFTAR ISI.....	iv
DAFTAR GAMBAR.....	vii
DAFTAR TABEL	viii
BAB IPENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Masalah Penelitian.....	2
1.2.1 Identifikasi Masalah.....	2
1.2.2 Batasan Masalah	3
1.2.3 Rumusan Masalah.....	3
1.3 Tujuan dan Manfaat Penelitian.....	4
1.3.1 Tujuan Penelitian	4
1.3.2 Manfaat Penelitian.....	4
1.4 Sistematika Penulisan.....	4
1.5 Daftar Pengertian.....	5
BAB IILANDASAN PEMIKIRAN	6
2.1 Tinjauan Pustaka	6
2.1.1 Kriptografi	6
2.1.2 Algoritma RSA	13
2.1.3 Pembangkit Bilangan Prima	17
2.1.4 Faktor Persekutuan Terbesar (FPB)	20
2.1.5 Fungsi <i>Hash</i> Satu Arah.....	21
2.1.6 Tanda Tangan Digital (<i>Digital Signature</i>).....	22
2.1.7 XML	24
2.1.8 <i>Web Service</i>	25
2.1.9 XML-RPC	25
2.1.10 Kualitas Perangkat Lunak.....	28
2.1.11 Model ISO 9126	29
2.1.12 Pengujian Perangkat Lunak	33
2.2 Tinjauan Studi	34
2.3 Kerangka Pemikiran	37

2.4	Hipotesis Penelitian	38
BAB III METODOLOGI PENELITIAN		39
3.1	Tempat Penelitian	39
3.2	Metode Pengumpulan Data	39
3.3	Tahapan Penelitian	39
3.4	Teknik Pengujian Sistem	41
3.4.1.	Pengujian dengan ISO 9126	41
3.4.2.	Pengujian dengan <i>Black-box testing</i>	41
3.5	Arsitektur Sistem	41
3.6	Alat Bantu Penelitian	42
3.7	Jadwal Penelitian	43
BAB IV PEMBAHASAN HASIL PENELITIAN		44
4.1	Analisis Sistem	44
4.1.1.	<i>UseCaseDiagram</i>	44
4.1.2.	<i>ActivityDiagram</i>	47
4.2	Perancangan Sistem	51
4.2.1.	Perancangan Teknik Kriptografi dan Tanda Tangan Digital	51
4.2.2.	Perancangan Layar Aplikasi	55
4.3	Implementasi Sistem	59
4.3.1.	Spesifikasi Perangkat Keras	59
4.3.2.	Spesifikasi Perangkat Lunak	59
4.3.3.	Implementasi Program	59
4.4	Pengujian Sistem	63
4.4.1.	Pengujian Dengan ISO 9126	63
4.4.2.	Pengujian dengan <i>Black-box testing</i>	69
4.5	Implikasi Penelitian	73
4.5.1.	Aspek Sistem	73
4.5.2.	Aspek Manajerial	74
4.5.3.	Aspek Penelitian Lanjutan	74
4.6	Rencana Implementasi	74
BAB V PENUTUP		76
5.1	Kesimpulan	76
5.2	Saran	76
5.3	Rencana Implementasi	77
DAFTAR PUSTAKA		78

LAMPIRAN-LAMPIRAN	81
RIWAYAT HIDUP	88



DAFTAR GAMBAR

Gambar	Halaman
II-1 Alur Kriptografi Kunci Simetris	8
II-2 Alur Kriptografi Kunci Asimetris	9
II-3 Ilustrasi <i>ReplayAttacker</i>	13
II-4 Ilustrasi <i>Man-in-the-middle</i>	13
II-5 Ilutراسي Tanda Tangan Digital	23
II-6 Konsep Dasar XML-RPC	26
II-7 Kerangka Pemikiran	38
III-1 Tahapan Penelitian	40
III-2 Arsitektur Sistem	42
IV-1 <i>Use Case Diagram</i>	44
IV-2 Activity diagram login	48
IV-3 Activity diagram lihat data pribadi	49
IV-4 Activity diagram lihat jadwal kuliah	49
IV-5 Activity diagram lihat nilai semester	50
IV-6 Activity diagram lihat HSK	51
IV-7 Ilustrasi teknik kriptografi dan tanda tangan digital	54
IV-8 Rancangan layar <i>login</i>	55
IV-9 Rancangan layar <i>home</i>	55
IV-10 Rancangan layar data pribadi	56
IV-11 Rancangan layar pilih jadwal kuliah	56
IV-12 Rancangan layar data jadwal kuliah	57
IV-13 Rancangan layar pilih nilai semester	57
IV-14 Rancangan layar data nilai semester	58
IV-15 Rancangan layar hasil studi kumulatif	58
IV-16 Halaman Login	60
IV-17 Halaman <i>Home</i>	60
IV-18 Halaman data pribadi	61
IV-19 Halaman pilih jadwal kuliah	61
IV-20 Halaman jadwal kuliah	61
IV-21 Halaman pilih nilai semester	62
IV-22 Halaman nilai semester	62
IV-23 Halaman hasil studi kumulatif (HSK)	63

DAFTAR TABEL

Tabel	Halaman
II-1 Tipe Data Parameter XML-RPC	26
II-2 Karakteristik Kualitas Perangkat Lunak Model ISO 9126	31
II-3 Tinjauan Studi	35
III-1 Jadwal Penelitian	43
IV-1 deskripsi <i>Use Case</i>	45
IV-2 Deskripsi Aktor.....	47
IV-3 Kriteria presentase tanggapan responden	64
IV-4 Tanggapan responden berdasarkan aspek <i>functionality</i>	64
IV-5 Tanggapan responden berdasarkan aspek <i>reliability</i>	65
IV-6 Tanggapan responden berdasarkan aspek <i>usability</i>	67
IV-7 Tanggapan responden berdasarkan aspek <i>efficiency</i>	68
IV-8 Hasil Pengujian Kualitas ISO 9126	69
IV-9 Pengujian <i>Black Box</i> untuk <i>form Login</i>	70
IV-10 Pengujian <i>Black Box</i> untuk menu yang diakses <i>user</i>	70
IV-11 Pengujian <i>Black box</i> untuk WS-Client.....	71
IV-12 Pengujian <i>Black box</i> untuk WS-Server	72
IV-13 Rencana implementasi	75

DAFTAR PUSTAKA

- [Al-Qutaish 2009] Al-Qutaish, Rafa, E. *Quality Models in Software Engineering Literature : An Analytical and Comparative Study*, Journal of American Science, Vol. 6, pp 166-175, 2010.
- [Arifin 2009] Arifin, Zainal. *Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman*. Jurnal Informatika Mulawarman, Vol. 4, No. 3, Samarinda, 2009.
- [Azmi 2010] Azmi, Meri, dan Dwi Sudarno Putra, *Implementasi Teknologi XML Dalam Pertukaran Data Antar Server (Studi di Dinas Pendidikan dan Pengajaran Kota Yogyakarta)* ISSN : 1858-3709, Poli Rekayasa Vol 6, No. 1, pp.58-70, Padang, 2010.
- [Caroline 2010] Caroline, Maureen Linda. *Perbandingan Algoritma Kriptografi Kunci Publik RSA, Rabin, dan Elgamal*, Makalah Teknik Informatika, Bandung, 2010.
- [Dafid 2006] Dafid. *Kriptografi Kunci Simetris Dengan Menggunakan Algoritma Crypton*, Jurnal Ilmiah STMIK MDP, Vol 2, No 3, pp 20-27, 2006.
- [Fithria 2007] Fithria, Naila. *Jenis-Jenis Serangan Terhadap Kriptografi*, Makalah Jurusan Teknik Informatika, Bandung, 2007. www.informatika.stei.itb.ac.id. (Diakses 10 Oktober 2013).
- [Hartono 2004] Hartono, Budi. *Ruang Lingkup Kriptografi Untuk Mengamankan Data*, Dinamika Informatika ISSN : 0854-9524, Vol. IX, No. 2, pp. 1-7, 2004.