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 antar*platform*yang berbeda, baik perbedaan dari segi bahasa pemrograman maupun sistem operasi yang digunakan. Akan tetapi ditribusi 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 kemanan 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

DAFTAR GAMBAR

Gambar **Halaman**

DAFTAR TABEL

Tabel **Halaman**

DAFTAR PUSTAKA

[Al-Qutaish 2009] Al-Qutaish, Rafa, E.*Quality Models in Software Engineering Literature : An Analytical andComprative 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 Informtika 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.