IMPLEMENTASI *XML WEB SERVICES* PADA SITUS PENJUALAN BUKU DENGAN KOMBINASI ENKRIPSI RC2 DAN ENIGMA

Andy Wisnu Wardana[1)], **Soetam Rizky Wicaksono**[2)]
1) Program Studi Sistem Informasi, STIKOM Surabaya, email: andywisnu@stikom.edu
2) Program Studi Sistem Informasi, STIKOM Surabaya, email: soetam@stikom.edu

Abstract: Selling e-book is big dilemma for most website. E-book as one of biggest and most anticipated commodity in internet marketing has weaknes that can not be avoided for most of the vendors, that is called illegal duplication. Therefore, website that run book store need an agile, strong and unique security to avoid that. One of the solution is using XML Web Service implementation and combining it with unique encryption combination. The combination of RC2 and ENIGMA algorithm will create a very strong and unbeaten encryption for the e-book. And XML Web Service implementation will assure that a downloaded e-book will always ask an authorized login whenever and wherever the reader want to read it. Thus, an e-book would not be able to be illegally duplicated, unless that the customer own legit serial number from their own MAC Address.

Keywords: RC2, ENIGMA, XML Web Service, Ebook

Situs Penjualan Buku Online merupakan suatu media komersial di internet yang memperjualbelikan buku yang berbentuk file dimana yang bisa mendapatkan layanan berupa buku elektronik adalah pelanggan yang sudah terdaftar atau member. User secara umum hanya dapat melihat informasi yang bersifat umum pula, tetapi timbul kekhawatiran dari produsen buku elektronik ketika suatu buku elektronik yang sudah dibeli oleh member tersebut dibajak atau digandakan tanpa seizin dari instansi yang berwenang. Hal ini karena tidak ada kepastian bahwa informasi yang mempunyai nilai ekonomis ini tidak digandakan setelah member melakukan proses pembelian.

Dalam hal ini, penting bagi aplikasi jasa komersial di internet untuk melakukan konsep keamanan tertentu untuk melindungi atau mencegah dari hal-hal yang sudah disebutkan diatas. Contoh yang ada saat ini adalah pada situs www.selftestsoftware.com , situs ini menyediakan soal-soal latihan sertifikasi dimana pelanggan akan mendapat file terenkripsi yang hanya bisa dibuka ketika pelanggan melakukan autentifikasi ke server dengan menyertakan identitas-identitas tertentu.

Seperti halnya situs tersebut, maka dibutuhkan solusi baru demi mencapai proteksi yang dianggap cukup layak untuk sebuah situs penjualan buku. Proteksi tersebut seharusnya dapat melindungi hak cipta dari buku yang sudah dijual kepada pelanggan, sehingga terhindar dari masalah *copy-paste* secara ilegal dari pelanggan kepada pihak yang tidak ikut melakukan pembelian.

Solusi dari permasalahan diatas adalah dengan mengimplementasikan Extensible Markup language(XML) Web Services Security pada produk maupun situs penjualan buku online. XML Web Service yang harus diimplementasikan nantinya mampu menjadi jembatan antara aplikasi *reader* dari buku elektronik yang dijual dengan kunci yang terdaftar pada situs penjualan buku.

Dan dengan adanya kunci tersebut, maka proteksi dapat diimplementasikan dengan menggunakan metode enkripsi tertentu.Selain itu, agar tidak terjadi proses duplikasi ilegal, maka dibutuhkan semacam *fingerprint* dari komputer pelanggan yang nantinya menjadi kunci eksklusif dalam implementasi penjualan buku elektronik tersebut.

Sedangkan pemilihan algoritma enkripsi dilakukan berdasarkan kombinasi dari dua algoritma yang berbeda, demi tercapainya tingkat sekuritas yang unik dan tinggi. Diharapkan dari kombinasi tersebut, pemecahan kunci maupun proses duplikasi ilegal dapat dicegah semaksimal mungkin.

LANDASAN TEORI

Ada berbagai versi definisi mengenai XML Web Services, yang pada intinya menggambarkan karakteristik dari XML Web Services (Rusiawan, 2003), adalah

1. Merupakan application logic yang dapat diakses dan dipublikasikan menggunakan standard Internet (TCP/IP, HTTP, Web).

2. Dideskripsikan dalam format XML.
3. Bersifat loosely coupled, self-contained, modular dan terbuka (non proprietary).
4. Digunakan untuk mendukung interoperabilitas interaksi machine-to-machine melalui jaringan Internet/Intranet.

Kriptografi adalah ilmu yang mempelajari bagaimana supaya dokumen kita aman, tidak bisa dibaca oleh pihak yang tidak berhak. Dalam perkembangannya, kriptografi juga digunakan untuk identifikasi pengirim pesan. Berdasarkan jenis kuncinya (Kurniawan, 2004), algoritma kriptografi dibagi dua yaitu :

1. Algoritma Simetri
2. Algoritma Asimetri

Kriptografi tidak hanya memberikan kerahasiaan dalam telekomunikasi, namun juga memberikan komponen-komponen berikut ini :

1. Authentication adalah penerima pesan dapat memastikan keaslian pengirimnya. Authentication berkaitan dengan memastikan suatu komunikasi tersebut valid.
2. Integrity adalah penerima dapat memeriksa apakah pesan dimodifikasi di tengah jalan. Integrity memberikan jaminan bahwa data yang diterima sama dengan yang dikirim oleh pihak yang berwenang.
3. Nonrepudiation pengirim tidak dapat mengelak bahwa dialah pengirim pesan. Penerima dapat membuktikan bahwa pesan sebenarnya dikirim oleh pengirim yang mengklaim.
4. Authority adalah informasi yang ada hanya dapat diubah oleh pihak yang berwenang. Authority menjaga data dari campur tangan pihak yang tidak berwenang (Kurniawan, 2004).

RC2 adalah blok cipher yang didisain pada 1989 oleh Ron Rivest untuk RSA Data Security. Cipher diciptakan secara efisien pada 16 bit proses dan dengan ukuran blok 64 bit. RC2 diciptakan sebagai pengganti dari DES (Rivest, 1998). Fitur terbaru pada RC2 adalah flexibilitas yang diberikan kepada user untuk membentuk ukuran kunci. Selama bertahun-tahun RC2 digunakan luas oleh masyarakat secara umum.

Bagian dari RC2 adalah prosedur key expansion yang menyediakan panjang kunci antara 0 sampai 128 byte bersama dengan parameter. Selama proses key expansion 2 operasi digunakan yaitu operasi byte dan 16 bit word operation. Kemudian suatu Array K[.] mengembalikan 64 16 bit round key dengan 2 proses yaitu :

1. Untuk word operation posisi dari buffer menempati K[0] ... K[63] dimana setiap K[i] adalah 16 bit word.
2. Untuk byte operation array akan menempati L[0] ... L[127] dimana setiap L(i) adalah berupa 8 bit byte.

ENIGMA merupakan mesin rotor yang digunakan oleh tentara NAZI Hitler dalam perang Dunia II. Jerman menganggap bahwa ENIGMA adalah sistem enkripsi yang tidak mungkin untuk dipecahkan. Awalnya ENIGMA menggunakan 3 rotor untuk melakukan substitusi. Tiga rotor berarti 3 kali substitusi 26 x 26 x 26. Namun pada akhir tahun 1944, ENIGMA menggunakan 4 rotor untuk melakukan enkripsi yang berarti ada 26 x 26 x 26 x 26 (456976 kemungkinan) (Stalling, 2003). Untuk lebih mempersulit pemecahan kode dari ENIGMA dari referensi yang ada menyebutkan bahwa kode yang dienkripsi sebaiknya tidak melebihi dari 200 karakter.

Gambar 1. Rotor ENIGMA

Cara kerja ENIGMA merupakan terjemahan dari gambar rotor ENIGMA ke dalam sebuah tabel acuan berikut :

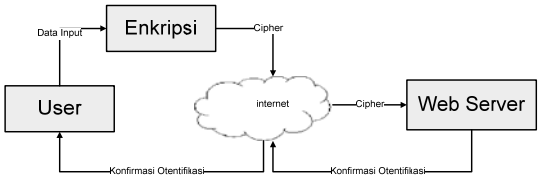
Tabel 1. Acuan Enigma

Plaintext	Rotor 1	Rotor 2	Rotor 3	Rotor 4	Cipher
A	CG	HE	BF	IA	I
B	BH	EF	GB	BA	H
C	FH	FG	HG	CD	G
D	GE	HI	DF	DC	F
E	FG	IH	AD	ED	E
F	HI	FH	FI	EF	D
G	AD	ED	IF	FI	C
H	FU	AC	HD	HG	B

Dari plaintext “A” ditarik garis lurus kekanan pada rotor 1, maka dijumpai “CG”, maka dari karakter “G” (karakter kedua dari “CG”) ditarik garis lurus kekanan pada rotor 2, maka dijumpai “ED”, dari karakter “D” tarik garis kekanan ke rotor 3 maka dijumpai “DF”, dari karakter “F” tarik garis kekanan ke rotor 4, maka dijumpai “EF”. Dari karakter “F” tarik garis lurus kekanan ke kolom cipher, maka dijumpai karakter “D”. Dengan demikian karakter “A” dikonversikan menjadi “D”.

PEMBAHASAN

Arsitektur dari sistem yang akan dibuat tergambar sebagai berikut :

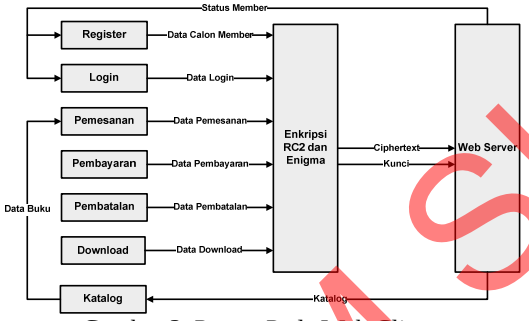


Gambar 2. Arsitektur Sistem

Sistem secara global mendefinisikan seorang user yang ingin registrasi, pembayaran,

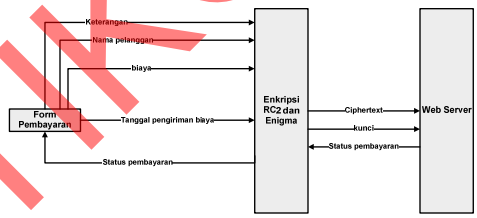
login dan pemesanan barang, maka aplikasi akan mengenerate sebuah text tertentu sebagai kunci yang berfungsi untuk mengenkripsi data-data pelanggan dengan kombinasi algoritma RC2 dan ENIGMA yang kemudian hasil dari enkripsi beserta kuncinya dikirimkan ke server untuk disimpan.

Ketika user ingin melakukan pembelian sebuah buku elektronik dan sudah melewati proses pembayaran maka ia akan diberikan 2 link untuk mendownload file. File yang pertama adalah file dengan format RTF (Rich Text Format) yang sudah dienkripsi dengan metode RC2 dan ENIGMA , kemudian file kedua adalah file RTF viewer yang berfungsi untuk mendekripsi file RTF tersebut. Untuk bisa membuka file RTF tersebut aplikasi akan mengambil data berupa MAC Address. Kedua data ini akan diproses dengan digest algorithm atau hash function yang kemudian disimpan ke database pada saat aplikasi dijalankan pertama kali. Untuk mendekripsi file diperlukan XML Web Services untuk mengambil kunci serta mencocokkan data MAC Address.



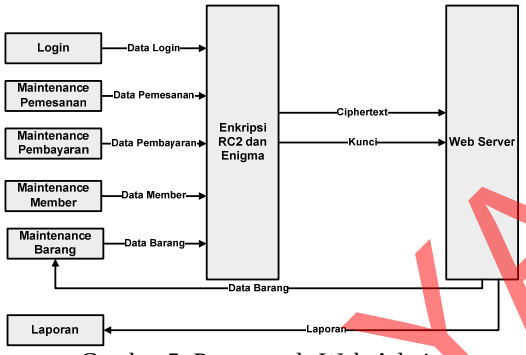
Gambar 3. Proses Pada Web Client

Apabila sesuai dan masih dalam batas waktu yang valid maka file akan terbuka dengan mode read-only, namun jika data yang ada sesuai namun batas waktu sudah lewat maka secara otomatis file yang terenkripsi akan terhapus



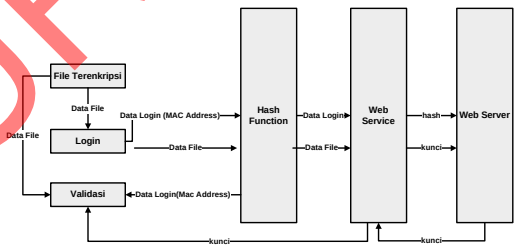
Gambar 4. Proses Pembayaran

Sistem penjualan buku online ini dapat diakses oleh admin maupun member. Untuk admin, ia harus login terlebih dulu. Setelah login, ia dapat melakukan proses maintenance barang dan menerima laporan (laporan pembayaran dan pendapatan). Data login maupun maintenance barang akan dienkripsi terlebih dahulu sebelum dikirim ke database



Gambar 5. Proses pada Web Admin

Untuk member, ia harus login terlebih dulu. Bila belum menjadi member, customer dapat melakukan proses register. Setelah login, member dapat melakukan proses pemesanan barang, dimana data barang dapat dilihat di katalog. Selain itu, ia dapat membatalkan pesanan, melakukan pembayaran, maupun melihat laporan transaksi yang dilakukannya. Data pemesanan, pembatalan, maupun pembayaran akan dienkripsi terlebih dahulu sebelum dikirim ke database



Gambar 6. Proses Pada Aplikasi Desktop

Berikutnya diuraikan hasil dan pembahasan penelitian terhadap perangkat lunak dimulai dari inputan ke proses validasi terhadap perangkat lunak. Berikut ini contoh gambar berupa seorang user yang telah terregistrasi melakukan transaksi terhadap buku elektronik yang akan dibeli.

Gambar 7. Tampilan pemesanan buku

Kemudian user bisa melakukan pembayaran dengan cara memasukkan data-data penting yang diperlukan

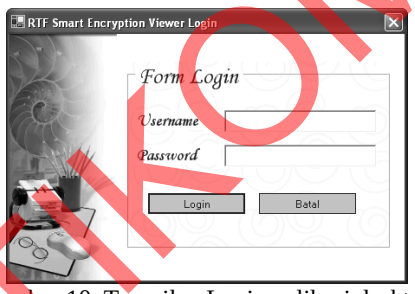
untuk bisa mendapatkan otoritas mendownload buku elektronik.

Gambar 8. Tampilan daftar pesanan dan pembayaran

Kemudian jika admin menyetujui *request* dari user maka user akan mendapatkan link untuk mendownload file-file yang diperlukan.

Gambar 9. Tampilan Download

Kemudian apabila user sudah mendownload file yang diperlukan maka user diharuskan login dari aplikasi dektop untuk membuka file buku elektronik.



Gambar 10. Tampilan Login aplikasi desktop

Kemudian apabila data-data user tervalidasi dengan benar maka akan tampil form utama yang membaca isi dari file dengan mendekripsi file tersebut dengan kunci yang dikirim via *XML Web Services*. Sebuah komputer klien diwajibkan untuk terkoneksi dengan internet agar bisa tervalidasi dengan baik.

Gambar 11. Tampilan Utama aplikasi desktop

Untuk mengetahui waktu yang dibutuhkan proses enkripsi dan dekripsi terhadap empat dokumen Rich Text Format berukuran 25 KB, 50 KB, 75 KB, dan 100 KB, dilakukan uji coba. Hasil pengujian waktu untuk proses enkripsi ditampilkan dengan tabel sebagai berikut

Tabel 2. Waktu Proses Enkripsi

Ukuran File	Ukuran Kunci
	128 bit
25 KB	5.36 s
50 KB	7.21 s
75 KB	8.22 s
100 KB	9.92 s

Agar Aplikasi ini bisa berjalan dengan yang diharapkan diasumsikan bahwa network adapter yang ada pada komputer klien adalah *onboard*. Hal itu karena MAC Address network adapter digunakan sebagai ID file yang disimpan dalam database, jika komputer klien menggunakan network adapter yang *offboard* memungkinkan user yang valid bisa membuka file *ciphertext* di komputer yang lain dengan cara memindah network adapter yang sudah teregistrasi di server.

SIMPULAN

Secara umum implementasi XML Web Services pada produk situs penjualan buku dengan kombinasi enkripsi RC2 dan Enigma telah berfungsi sebagaimana yang diharapkan. Untuk itu dapat diambil beberapa kesimpulan dari sistem ini sebagai berikut :

1. Algoritma RC2 dapat dikombinasikan dengan algoritma Enigma yang digunakan untuk mengenkripsi teks dan dokumen Rich Text Format.
2. Aplikasi tidak dapat melakukan dekripsi terhadap suatu file *ciphertext* jika network adapter atau lan card diganti.
3. File *ciphertext* tidak dapat didekripsi apabila aplikasi tidak terhubung dengan XML Web services via internet.

Adapun saran-saran untuk pengembangan sistem ini antara lain :

1. Aplikasi dapat dikembangkan dengan mengkombinasikan MAC address hardware yang lain agar tingkat keamanan data lebih terjamin.

2. Aplikasi dapat dikembangkan untuk mengenkripsi file-file lain selain dokumen Rich Text Format.
3. Algoritma RC2 atau Enigma dapat dikombinasikan dengan algoritma lain yang lebih kuat dengan ukuran kunci yang lebih besar untuk meningkatkan keamanan enkripsi data.
4. Proteksi terhadap file Rich Text Format yang terupload di server perlu dilakukan agar user secara umum tidak bisa mengambil file asli karena proses enkripsi file tidak terjadi saat Admin input dan upload data.

DAFTAR RUJUKAN

Altair Valasek, Michal. 2003. *WS-Security : XML Web Services the Secure Way, (*Online), (http://www.thecodeproject.com/soap/WS-Security.asp?print=true, diakses *29* September 2005).

Atkinson, Bob. 2002. *XML Web Services Security (WS-Security)*, (Online), (http://schemas.xmlsoap.org/specs/ws-security/ws-security.htm, diakses 5 April 2005).

Kurniawan, Yusuf. 2004. *Kriptografi Keamanan Jaringan Internet dan Jaringan Telekomunikasi*. Bandung : Informatika Bandung.

Purbo, Onno W. 2001. *Mengenal E-Commerce*. Jakarta : PT Elex Media Komputindo.

Rivest, Ronald. 1998. *On the design and security of RC2,* (Online), (http://www.rsa.com, diakses 28 Juli 2006).

Rusiawan, Dwi. 2003. *Tinjauan Aspek Keamanan Sistem Web Service.* Skripsi. Bandung : Program Studi Magister Teknologi Informasi ITB.

Short, Scott. 2003. *Building XML Web Services For The Microsoft .NET Platform*. Jakarta : PT. Elex Media Komputindo.

Stalling, William. 2003. *Cryptography and Network Security*. New Jersey : Prentice Hall.

Tjoenedi, Freddy Kresna. 2004. *Pembuatan Program Digital Signature authentication File dengan ECDSA di bidang penjualan Hardware*. Skripsi Surabaya : Program studi S1 STIKOM