Available *online* at : http://bit.ly/InfoTekJar

InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600

Computer Security

Analisis Penerapan Digital Signature sebagai Otentikasi dan Pengamanan Data

Heri Santoso

Universitas Islam Negeri Sumatera Utara

KEYWORDS

Digital Signature; Otentikasi Dat; LSB Emmbedding; SHA; CRC3;

CORRESPONDENCE

Phone: 0821-6700-5000

E-mail: herisantoso@uinsu.ac.id

A B S T R A C T

Kemajuan teknologi informasi semakin mempermudah proses pertukaran informasi, dan kemajuan tersebut tidak terlepas dari adanya komputer dan internet. Akan tetapi disamping kemajuan teknologi tersebut muncul masalah baru yakni ancaman terhadap keamanan data. Saat pertukaran informasi berlangsung informasi yang dikirimkan merupakan data plainteks dan hal ini sangat beresiko ketika ada pihak yang berhasil menyadap informasi, maka pihak tersebut akan dengan mudah mengubah informasi tersebut sebelum sampai pada penerima sebenarnya. Penerapan Digital Siganture dalam proses pengiriman data merupakan solusi untuk masalah tersebut. Dikarenakan digital signature merupakan suatu cara matematis untuk menunjukkan keotentikan suatu data. Dari beberapa penelitian yanng pernah dilakukan digital signature telah banyak dipakai dan mampu membangun suatu sistem yang aman dengan mengkombinasikan digital signature dengan berbagai algoritma seperti LSB Embedding , SHA-256, CRC32, Kurva Elpitik, dll., akan sangat mendukung dalam pembangkitan sistem yang mampu mengamankan data khusus dalam proses otentikasi data.

PENDAHULUAN

Saat ini teknologi informasi sudah sangat maju, terlihat dari kemudahan dan kecepatan dalam berkomunikasi, komputer dan internet sudah menjadi kebutuhan utama. Sebagian besar orang menggunakan komputer maupun internet dalam kehidupan sehari – hari, baik dalam hal komunikasi, pendidian, hiburan, dan lain – lain.

Pertukaran informasi dimudahkan dengan hadirnya jaringan komputer dan internet. Salah satu manfaat internet yang kita ketahui adalah adanya layanan e-commerce yang semakin banyak diminati oleh masyarakat karena dapat memudahkan dalam hal pemilihan dan pembelian barang secara on-line. Bahkan pembayarannya pun dapat dilakukan secara elektronik. [1]

Akan tetapi masalah yang muncul dengan penggunaan jaringan komputer ataupun internet adalah informasi yang dikiriman merupakan data *plaintext*. Hal ini beresiko ketika ada pihak lain yang berhasil menyadap informasi ini, mereka akan dengan mudah membaca isi informasi tersebut. Resiko yang lain adalah file yang ditransmisikan dapat diubah atau bahkan diganti secara keseluruhan oleh pihak lain. [2]

Masalah keamanan yang sering terjadi adalah pencurian dan pemalsuan data atau dokumen. Pihak yang tidak bertanggung jawab dapat dengan mudah mengubah dan mencuri data yang telah terditribusi dalam internet maupun database, tidak hanya itu data atau dokumen yang telah dicetakpun dapat terancam keamanannya dari pihak yang tidak bertanggung jawab. Untuk itu dibutuhkan teknologi keamanan data yang dapat mencegah dan membantu membuat suatu tanda khusus yang dapat memastikan bahwa data tersebut otentik atau data yang benar dan memenuhi syarat integritas data. Teknologi yang sering digunakan dalam hal ini sering disebut dengan *digital signature*. [3]

Digital-signature adalah suatu cara matematis untuk menunjukkan keotentikan suatu dokumen. *Digital signature* memiliki fungsi sebagai penanda pada data yang memastikan bahwa data tersebut adalah data yang sebenarnya (tidak ada yang berubah). Dengan demikian, *Digital signature* dapat memenuhi syarat keamanan jaringan, yaitu *Authenticity*, *Integrity*, dan *Non-Repudiation*. [2]

TINJAUAN PUSTAKA

Pengamanan data dengan digital signature telah banyak diterapkan diberbagai lingkungan dan tak jarang digital signature dikombinasi dengan berbagai algoritma diantaranya pada penelitian "Implementasi Sistem Pengamanan *E-Commerce* menggunakan *Schnorr Digital Signature".* Pada penelitian ini didesain sebuah aplikasi *e-commerce* dengan sistem keamanan pada layer transport dan layer aplikasi. Keamanan pada layer transport diimplementasikan protokol SSL(Secure Socket Layer) sedangkan di sisi layer aplikasi untuk keabsahan pengguna diimplementasikan proses *digital signature* yang merupakan salah satu metode *public key cryptography* dimana kunci yang digunakan untuk proses enkripsi dan dekripsi berbeda nilai, salah satunya adalah metode hash dan *cryptography* dengan algoritma *Schnorr*. [1]

Pada penelitian yang berjudul "*Implementasi digital signature menggunakan LSB Embedding untuk uji keutuhan, otentikasi dan penyangkalan dokumen petahanan digital*"[2], menghasilkan sebuah aplikasi *digital signature* yang dapat menguji keutuhan, keotentikan, dan *non-repudiation* suatu dokumen *digital*.

Penelitian yang lain, yang membahas tentang pemanfaatan *digital signature* untuk mengamankan dokumen adalah "*Penerapan Digital Signature pada transkip nilai sebagai otentikasi data*" [3]. Digital signature pada penelitian tersebut digunakan pada transkip nilai yang berguna menjamin ke otentikan dari suatu trankip nilai.

Penelitian yang lain, yang membahas tentang pemanfaatan *digital signature* adalah *"Rancang Bangun Sistem Pengamanan Dokumen Pada Sistem Informasi Akademik Dengan Menggunakan Digital Signature* [4]. Penelitian tersebut membahas tentang model dan aplikasi keamanan dokumen elektronik pada Sistem Informasi Akademik (SIA) menggunakan digital signature

Penelitian yang lain, yang membahas tentang pemanfaatan *digital signature* untuk mengamankan dokumen adalah *"Rancang Bangun sistem informasi e-surat di fakultas teknologi informasi dengan penerapan digital signature dan algoritma base 64 berbasis web"* [5]. Pada penelitian tersebut membahas tentang penerapan digital signature untuk mengatasi masalah pengesahan surat.

Digital Signature

Digital signature adalah salah satu teknologi yang digunakan untuk meningkatkan keamanan jaringan. *Digital signature* memiliki fungsi sebagai penanda pada data yang memastikan bahwa data tersebut adalah data yang sebenarnya (tidak ada yang berubah).

Digital signature dapat memenuhi setidaknya dua syarat keamanan jaringan, yaitu *authenticity* dan *non-repudiation*, dan juga *integrity* (keutuhan data). *Authenticity* berarti bahwa dokumen tersebut berasal dari pemilik yang spesifik. *Non-repudiation* berarti bahwa berdasarkan *digital signature* di dalam suatu dokumen, pelaku/pengirim tidak dapat mengingkari bahwa yang bersangkutan melakukan pengiriman/manipulasi data. *Integrity* berarti bahwa keutuhan suatu dokumen dapat diketahui berdasarkan kondisi *digital signature* didalamnya.

Algoritma Schnorr

Algoritma tanda tangan digital Schnorr memanfaatkan kesulitan beberapa permasalahan logaritma diskrit untuk dipecahkan sebagai dasar dari kemanananya. Algoritma schnorr merupakan algoritma kriptografi yang cukup sederhana namun memberikan keamanan yang efisien dan cocok untuk diimplementasikan dalam aplikasi transaksi pembayaran, seperti electronic commerce, electronic payment, electronic toll collection dan lainnya.[1]

SHA-256

Fungsi hash dalam kriptografi adalah fungsi hash yang berupa sebuah algoritma yang mengambil sejumlah blok data dan mengembalikan bit string berukuran tetap. String yang dihasilkan tersebut merupakan hash value. Perubahan yang dilakukan pada data walaupun sangat kecil, sengaja ataupun tidak, akan menyebabkan perubahan yang sangat banyak pada hasil hash value. Bahkan hash value dapat menjadi berbeda sama sekali. Data yang di hash sering disebut pesan, hash value disebut digest. Hash umumnya disajikan dalam bentuk bilangan hexadecimal, yaitu kombinasi antara angka 0-9 dengan huruf a hingga f. Menurut jenisnya SHA dapat dispesifikasikan menjadi 4 bagian yaitu: SHA-1, SHA-256, SHA-384, dan SHA-512. [1]

LSB Embedding

LSB *embedding* merupakan teknik steganografi yang menggunakan pendekatan tergolong sederhana dan langsung. Sesuai dengan namanya, teknik LSB *embedding* menyisipkan pesan ke dalam LSB (*least significant bit*). Hal ini hanya akan mempengaruhi nilai warna pada piksel sebesar + 1, maka secara umum diasumsikan bahwa degradasi warna yang terjadi dapat tidak dikenali oleh mata. LSB embedding tidak menambahkan ukuran dokumen, karena proses yang terjadi adalah mengganti bit akhir tiap warna.

LSB *embedding* memiliki kelebihan dibandingkan dengan algoritma EOF *steganography* [9], dalam hal perubahan ukuran dokumen yang disisipi. LSB embedding tidak menambahkan ukuran dokumen, karena proses yang terjadi adalah mengganti bit akhir tiap warna. EOF bekerja dengan menambahkan informasi pada akhir dokumen. Algoritma steganografi yang lain adalah algoritma DCT. Algoritma ini menggunakan frequency domain dari citra digital untuk menyisipkan informasi. Kelemahan dari algoritma DCT adalah mata manusia dapat mengenali perubahan yang terjadi pada frekuensi rendah. [2]. Maka dari itu LSB merupakan algoritma yang lebih unggul dibandingkan EOF dan DCT.

Kurva Eliptik

Kriptografi kurva eliptik termasuk kedalam sistem kriptografi asimetris yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik.

Elliptic Curve Cryptography (ECC) mempunyai keuntungan jika dibandingkan dengan kriptografi asimetris lainnya yaitu dalam hal ukuran panjang kunci yang lebih pendek tetapi memiliki tingkat keamanan yang sama. Sebagai perbandingan, 160 bit Elliptic Curve Cryptography mempunyai tingkat keamanan (3.8.1010 MIPS/Million Instruction per Second year) yang sama dengan 1024 bit RSA mempunyai tingkat keamanan (3.10 12 MIPS year). Sehingga kecepatannya lebih tinggi, konsumsi daya yang lebih rendah, adanya penghematan bandwith. Keuntungan - keuntungan tersebut sangat berguna untuk aplikasi - aplikasi yang memiliki keterbatasan pada bandwith, kapasitas pemrosesan, ketersediaan sumber tenaga dan ruang. Aplikasi - aplilkasi tersebut antara lain: kartu chip, kartu kredit atau kartu debit, tiket elektronik, telepon selular, pager dan kartu identitas.

Kriptografi kurva eliptik (Elliptic Curve Cryptography) menggunakan dua kunci yaitu kunci publik dan kunci privat. Kunci publik pada kriptografi adalah sebuah titik pada kurva eliptik dan kunci privatnya adalah sebuah angka random. Kunci publik diperoleh dengan melakukan opersai perkalian terhadap kunci privat dengan titik generator G pada kurva eliptik. Titik generator G digunakan untuk melakukan pertukaran kunci Diffie

-Hellman. Sehingga menjadi dasar untuk memilih pertukaran kunci Diffie-Hellman. [10]

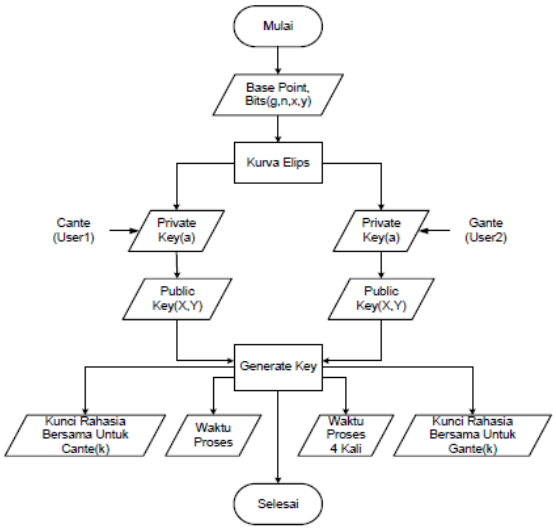
Algoritma Diffie - Hellman

Diffie-Hellman merupakan suatu algoritma kunci publik yang pertama kali ditemukan pada tahun 1976, meskipun NSA mengaku telah menemukan algoritma asimetrik jauh-jauh hari sebelumnya. Algoritma ini memperoleh keamanannya dari sulitnya menghitung logaritma diskrit pada bilangan yang sangat besar. Algoritma Diffie-Hellman hanya dapat digunakan untuk pertukaran kunci (simetri) dan tidak dapat digunakan untuk enkripsi dan dekripsi maupun untuk tanda tangan digital.

Diffie-Hellman pertama kali memperkenalkan algoritma kunci publik pada tahun 1976 dan sebelumnya ditemukan oleh Malcolm Williamson pada tahun 1974. Algoritma ini memiliki keamanannya dari kesulitan menghitung logaritma diskrit dalam *finite field*, dibandingkan kemudahan dalam menghitung bentuk eksponensial dalam *finite field* yang sama. Algoritma ini dapat digunakan dalam mendistribusikan kunci publik yang dikenal dengan protokol pertukaran kunci.

Sistem ini dipakai untuk menyandikan pertukaran pesan antar dua pihak secara interaktif. Pada awalnya, masing-masing pihak mempunyai sebuah kunci rahasia yang tidak diketahui pihak lawan bicara. Dengan berdasar pada masing-masing kunci rahasia ini, ke dua pihak dapat membuat sebuah kunci sesi (session key/kunci rahasia untuk komunikasi dengan kriptografi simetri) yang akan dipakai untuk pembicaraan selanjutnya.

Pembuatan kunci sesi ini dilakukan seperti halnya suatu tanya jawab matematis, hanya pihak yang secara aktif ikut dalam tanya jawab ini sajalah yang bisa mengetahui kunci sesinya. Penyadap yang secara aktif mengikuti tanya jawab ini tidak akan bisa mengetahui kunci sesi ini.



Gambar 1. Struktur Kunci Diffine-Hellman

METODE PENELITIAN

Metode yang digunakan pada penelitian e-commerce yakni informasi berupa pesan pembelian(M) dienkipsi(e) oleh buyer dengan enkripsi AES-128 bit menghaslkan chiper(c). Kemudian dilakukan *signing* terhadap *chiper* dengan algoritma *schnorr* dan menghasilkan *signature*, *signature* dan *chiper* dikirim ke seller. Seller melakukan pemisahan terhadap chiper dan *signature*. *Chiper* didekripsi dengan shared key menggunakan AES-128 bit dan diperoleh pesan asli. Seller melakukan verifikasi terhadap pesan asli dan *signature* menggunakan *public key* buyer.

Metode pada penelitian [2] yakni sistem dirancang terdiri dari dua proses, yaitu proses *signing* dan proses *verifiying*. Proses *signing* dilakukan oleh *signatory*, dengan menanamkan *digital signature* ke dalam dokumen. Proses *verifiying* dilakukan oleh *verifier*, dengan mengekstraksi *digital signature* dari dalam dokumen. Penyisipan digital signature dalam dokumen menggunakan LSB embedding sehingga tidak akan menambah ukuran dokumen.

Metode pada penelitian [3] yakni menggunakan metode *hashing* dengan algoritma CRC32, dengan membangkitkan nilai *hash (hash value)* yang akan menjadi kode *digital signature* pada transkrip mahasiswa menggunakan metode *hashing* dengan algoritma CRC32, sehingga pada setiap transkrip tersebut akan memiliki kode yang berbeda-beda yang dihasilkan atas dasar data mahasiswa dan perolehan nilai prestasi akademik masing-masing mahasiswa sebagai upaya untuk menciptakan suatu transkrip yang disertai dengan identitas yang unik dengan tujuan untuk mengamankan data dari upaya pemalsuan maupun manipulasi data transkrip. aplikasi *digital signature* tersebut juga dibuat dengan memperhatikan beberapa skema dari *digital signature* yaitu proses pemberian tanda tangan dengan proses hashing dan proses validasi untuk memastikan *digital signature* benar-benar terintegrasi dengan data transkrip pada database sebagai pendukung integritas data. Sehingga tingkat keamanan data bisa dijamin karena proses pengolahan transkrip *digital signature* harus melalui beberapa prosedur yang ketat.

Validasi hanya dapat diproses dan dilakukan pada level administrator sebagai proses integrasi kode *digital signature* transkrip yang telah dihasilkan dari proses *hashing* dengan database transkrip mahasiswa yang bersangkutan agar dalam proses otentikasi bisa dipastikan bahwa data tersebut otentik. Bukti validasi akan disertakan pada transkrip dari hasil pencarian di halaman pencarian dan ditampilkan pada "*DS Stored"*. Sedangkan level user hanya mempunyai hak akses pada halaman pencarian. Pada setiap proses pencarian, data transkrip yang akan ditampilkan selalu menyertakan proses *hashing* yang nilainya akan ditampilkan pada "*DS Processed"*, sehingga dapat diketahui apabila transkrip tersebut otentik atau tidak. Dapat dipastikan data otentik apabila nilai *digital signature* pada *DS processed* sama dengan nilai pada *DS Stored*.

Metode pada penelitian [4], yakni Tanda tangan digital (digital signature) akan dikonversikan dalam model barcode dari nilai hasil enkripsi digital signature dengan metode kurva eliptik, dan barcode ini akan dibaca kembali oleh barcode reader dengan menterjemahkan informasi yang ada pada barcode menjadi informasi yang dimengerti bagi yang membaca berkas. Dan aplikasi de-enkripsi (Deskripsi) yang akan menkonversikan kembali kode pada barcode menjadi informasi yang dimengerti oleh pengguna.

Metode pada penelitian [5], yakni melakukan pengenkripsian surat electronik (e-surat) menggunakan algoritma Base64.

HASIL DAN ANALISIS PENERAPAN DIGITAL SIGNATURE

Hasil yang didapat dalam penerapan digital signature adalah sistem transaksi online yang aman dengan penerapan digital signature Schnorr pada layer aplikasi untuk validasi keabsahan pengguna dan keamanan data transaksi. Dengan level security 2048 bit dan SHA-256, rata-rata waktu eksekusi yang dibutuhkan dalam pembangkitan kunci 89,24 menit, tanda tangan 36,7 mili detik dan verifikasi 72,3 mili detik. Total waktu yang dibutuhkan untuk satu kali transaksi penjualan adalah 224 mili detik.[1]

Digital Signature juga mampu mendeteksi manipulasi yang dilakukan pada dokumen, yaitu rotasi, *mirror*, *crop*, *resize*, dan manipulasi piksel. Proses verifikasi berlangsung lebih cepat daripada proses *digital signing*, karena pada proses *digital signing* terdapat proses *read* dan *writebit-bit* pada verifikasi hanya ada proses *read* saja.[2]

Digital Signature dapat membangun sistem keamanan data pada transkip nilai sebagai upaya otentikasi data. [3]

KESIMPULAN

Dari beberapa penelitian yang telah dilakukan dapat disimpulkan bahwa Digital signature merupakan teknologi yang tepat untuk menciptakan suatu sistem yang aman dengan mengkombinasikan digital signature dengan berbagai algoritma LSB Embedding , SHA-256, CRC32, dll., akan sangat mendukung dalam pembangkitan sistem yang mampu mengamankan data khusus dalam proses otentikasi data.

REFERENSI

[1] Samsul Huda, dkk. Implementasi Sistem Pengamanan E-Commerce menggunakan Schnorr Digital Signature. Legacy 1024 : 160, 2014.

[2] Fransiskus, dkk. Implementasi Digital Signature menggunakan LSB Embedding untuk Uji Keutuhan, Otentikasi dan Penyangkalan dokumen Pertanahan Digital. Jurnal Komputer & Informatika Vol.13, No.1, pp. 1-9, 2014.

[3] Ibnu, dkk. Penerapan Digital Signature pada Transkip Nilai Sebagai Otentikasi Data. Jurnal Script. ISSN. 2338 – 6304. Vol.1, No.2, pp. 130-137, Januari 2014.

[4] Ahmaddul Hadi. Rancang Bangun Sistem Pengamanan Dokumen Pada sistem Informasi Akademik Dengan Menggunkan Dogital Signature. Jurnal Teknologi Informasi & Pendidikan, ISSN.2086 – 4981, Vol.6, No.2, pp. 190-201, September 2013.

[5] Yoyok, Rancang Bangun Sistem Informasi E-Surat Di Fakultas Teknologi Informasi dengan Penerapan Digital Signature dan Algoritma Base 64 Berbasis Web. Jurnal Dinamika DotCom Vol.5, No.2, pp. 119-121, 2014.

[6] Quixia, dkk. The Improvement of digital signature algorithm based on elliptic curve cryptography. IEEE 978-1-4577-0536-6. 2011

[7] Nivetha, dkk. Knapsack-Based Elliptic Curve Cryptography using stern series for digital signature authentication. IEEE 978- 1 – 4244 – 7926 – 9. 2011

[8] Deng Jian Zhi, dkk. Design of Hyper Elliptic Curve Digital Signature. International Conference on Information Technology and Computer Science. 978 – 0 – 7695 – 3688 – 0. 2009

[9] Depaak, dkk. An Architectural Framework for Encryption & Generation Of Digital Signature Using DNA Cryptographi. IEEE 978 – 93 – 80544 – 12 – 0. 2009

[10] Metrilitna. Elliptic Curve Cryptography (Ecc) Pada Proses Pertukaran Kunci Publik Difflic-Hellman. *Visipena* ISSN 2086 –1397,Vol 6, No. 1, Juni 2015.