Prototype Single IP Login dan Kriptografi Asimetris *Digital Signature Algorithm* pada *User Auntentification*

Studi Kasus CV. Danofal's

Amras Mauluddin
Fakultas Teknik
Program Studi Informatika
Universitas Langlangbuana
amrasmauluddin@gmail.com

Irwin Supriadi
Fakultas Teknik
Program Studi Informatika
Universitas Langlangbuana
irwinshared@gmail.com

Awan Setiawan
Fakultas Teknik
Program Studi Informatika
Universitas Langlangbuana
awans2425@gmail.com

Abstrak - Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, seperti perusahaan, perguruan tinggi, lembaga pemerintahan, maupun individual. Masalah keamanan menjadi aspek penting dari sebuah perangkat lunak, tapi sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian. Keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. kelemahan-kelemahan perangkat lunak dituangkan kedalam rumusan masalah bagaimana membuat keamanan untuk setiap member atau user dari perangkat lunak yang telah dibangun pada CV. DANOFAL'S, Bagaimana menerapkan keamanan pada verifikasi user atau member login apabila perangkat lunak yang diakses menggunakan IP yang berbeda. Metode yang digunakan dalam penelitian ini adalah metode penelitian rekayasa dengan pendekatan *forward engineering* dan model pengembangan sistem *prototyping*. Model *prototyping* mendefinisikan obyektif umum dari perangkat lunak tanpa merinci kebutuhan input, pemrosesan dan outputnya. Perangkat lunak yang dibangun dengan menggunakan *single IP login* membantu *member* atau *user* untuk menjaga keamanan data saat melakukan akses dengan menggunakan IP yang lain. Penerapan algoritma enkripsi asimetris DSA pada login perangkat lunak mempunyai dua fungsi utama yaitu Pembentukan tandatangan digital (*signature* generation), dan Pemeriksaan keabsahan tandatangan digital (signature verivication) dengan menggunakan teknik pembangkitan nilai dokumen menggunakan fungsi *Hash public key*.

Kata kunci – *Keamanan, Forward engineering,* perangkat lunak*, prototyping, DSA*.

1. PENDAHULUAN

Informasi saat ini sudah menjadi sebuah *komoditi* yang sangat penting. Bahkan ada yang mengatakan bahwa masyarakat kita sudah berada di sebuah "*information-based society*". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, seperti perusahaan, perguruan tinggi, lembaga pemerintahan, maupun individual. Begitu pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Masalah keamanan menjadi aspek penting dari sebuah perangkat lunak, tapi sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola perangkat lunak, seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting.

CV. DANOFAL'S merupakan perusahaan yang baru terjun di bidang jual beli *online* dimana sebelumnya lebih banyak bergulat pada bidang arsitektur khususnya jasa konstruksi maupun konsultan tata ruang kota dengan sasaran market

proyek-proyek Pemerintah Daerah (PEMDA) Tingkat II. Oleh karena itu, maka CV. DANOFAL'S sangat membutuhkan sebuah perangkat lunak yang dapat memberikan keamanan bagi customer yang menggunakan jasanya, selain kemudahan baik dalam operasional maupun manajemen transaksi jual beli *digital currency* dengan tidak mengesampingkan aspek-aspek keamanan ataupun kerentanan yang terjadi dalam transaksi-transaksi berbasis *online*.

Melihat kelemahan-kelemahan perangkat lunak pada CV. DANOFAL'S, maka kekurangan perancangan dari perangkat lunak di atas dituangkan kedalam rumusan masalah, sebagai berikut:

1. Bagaimana membuat keamanan untuk setiap member atau *user* dari perangkat lunak yang telah dibangun pada CV. DANOFAL'S?
2. Bagaimana menerapkan keamanan pada verifikasi *user* atau member *login* apabila perangkat lunak yang diakses menggunakan *IP* yang berbeda?

Tujuan dari penelitian ini adalah membangun dan merancang *single IP login* member pada perangkat lunak CV.DANOFAL'S dan menerapkan perancangan enkripsi asimetris DSA (*Digital Singnature Algorithm*) pada *login* perangkat lunak CV.DANOFAL'S.

Keamanan komputer pada dasarnya adalah perlindungan sistem komputer dan informasi dari bahaya, pencurian, dan penggunaan yang tidak sah. Dalam buku karya Howard (1997) "*An Analysis of Security Incidents on The Internet*" mengatakan bahwa keamanan komputer merupakan tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab[1]. Keamanan komputer terutama berkaitan dengan tiga bidang utama[2]:

1. Kerahasiaan adalah memastikan bahwa informasi hanya tersedia untuk audiens yang dituju;
2. Integritas adalah melindungi informasi agar tidak diubah oleh pihak yang tidak berwenang;
3. K*etersediaan adalah* melindungi informasi agar tidak diubah oleh pihak yang tidak berwenang.

Menurut Hestanto (2020), tanda tangan digital *(digital signature)* merupakan tanda tangan yang dibuat secara elektronik yang berfungsi sama dengan tanda tangan biasa pada dokumen biasa yang bila tidak dipalsukan dapat digunakan untuk menyatakan bahwa orang yang namanya tertera dalam dokumen tersebut setuju dengan yang telah tercantum dalam dokumen yang ditandatangani[3]. Tanda tangan digital juga merupakan metode autentikasi yang menggunakan aplikasi teknologi asimetris kriptografi yaitu sistem pengacakan suatu pesan menggunakan sepasang kunci, yakni kunci privat dan kunci publik yang menjamin keaslian pesan elektronik dan menjamin integritas subtansi pesan[3].

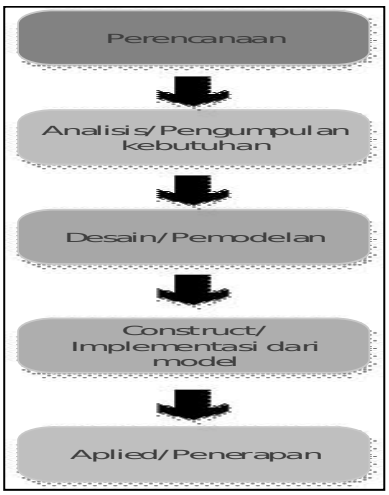
Digital Signature Algorithm (DSA) merupakan standar pemrosesan informasi federal untuk tanda tangan digital yang diusulkan pada tahun 1991 dan distandarisasi secara global pada tahun 1994 oleh *National Institute of Standards and Technology* (NIST), berfungsi pada kerangka eksponensial modular dan masalah logaritma diskrit, yang sulit untuk dihitung sebagai sistem *force-brute*[4]. Keaslian data digital dapat diperoleh dengan model matematika yang dikenal sebagai *Digital Signature Standard* (DSS). DSA memberikan lapisan validasi serta keamanan untuk pesan yang dikirim melalui saluran yang tidak aman. DSA didasarkan pada kesulitan komputasi dalam menemukan logaritma diskrit[5].

2. METODE

2.1. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian rekayasa dengan pendekatan *forward engineering.* Adapun tahapan tahapan penelitian tersebut adalah *plan, analysis, design, construct,* dan *applied.* Penelitian rekayasa merupakan penelitian yang menerapkan ilmu pengetahuan menjadi suatu rancangan guna mendapatkan kinerja sesuai dengan persyaratan yang ditentukan. Dari penelitian rekayasa yang dihasilkan berupa arsitektur, *artificial intelligence, robotic, software,* dan lain sebagainya. Rancangan tersebut merupakan sintesis unsur-unsur rancangan yang dipadukan dengan metode ilmiah menjadi suatu model yang memenuhi spesifikasi tertentu. Penelitian diarahkan untuk membuktikan bahwa rancangan tersebut memenuhi spesifikasi yang di tentukan.

Tahapan pendekatan forward engineering dijelaskan pada Gambar 1 berikut:

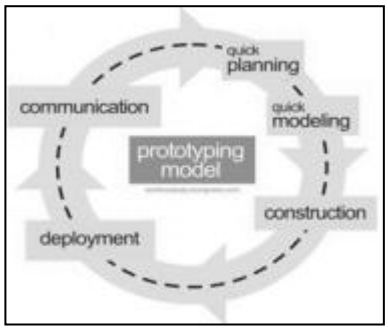


Gambar 1. Tahap pendekatan *forward engineering*

2.2. Metode Pengembangan Sistem

Pengembangan sistem dalam penelitian ini menggunakan metode pengembangan sistem prototipe. Model ini digunakan karena pengguna hanya mendefinisikan obyektif umum dari perangkat lunak tanpa merinci kebutuhan input, pemrosesan dan outputnya, sementara pengembang/developer tidak begitu yakin akan efisiensi algoritma, adaptasi sistem operasi, atau bentuk interaksi manusia-mesin yang harus diambil.

Prototipe ini digunakan untuk memungkinkan pengguna mengevaluasi dan mencobanya sebelum implementasi, sehingga membantu pengguna memahami persyaratan yang spesifik dan mungkin tidak dipertimbangkan oleh pengembang selama desain produk. Langkah-langkah pengembangan dengan model prototipe terlihat pada Gambar 2 beriktu.



Gambar 2. Pengembangan model prototipe

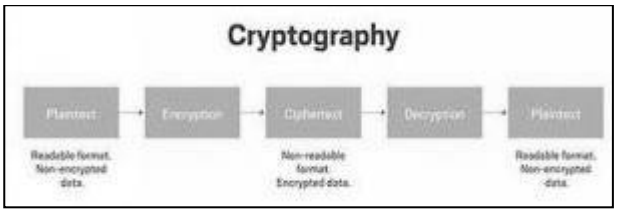
2.3. Kriptografi

Kriptografi adalah metode untuk melindungi informasi dan komunikasi melalui penggunaan kode, sehingga hanya pihak-pihak yang dituju yang dapat membaca dan memprosesnya[6]. Dalam ilmu komputer, kriptografi mengacu pada teknik informasi dan komunikasi yang aman yang diturunkan dari konsep matematika dan seperangkat perhitungan berbasis aturan yang disebut algoritma, untuk mengubah pesan dengan cara yang sulit diuraikan. Algoritma deterministik ini digunakan untuk pembuatan kunci kriptografi, penandatanganan digital, verifikasi untuk melindungi privasi data, penjelajahan web di internet dan komunikasi rahasia seperti transaksi kartu kredit dan email.

Kriptografi erat kaitannya dengan disiplin ilmu kriptologi dan kriptanalisis. Di dunia komputer sentris saat ini, kriptografi paling sering dikaitkan dengan mengacak plaintext (teks biasa, kadang-kadang disebut sebagai cleartext) menjadi ciphertext (proses yang disebut enkripsi), lalu kembali lagi (dikenal sebagai dekripsi).

Kriptografi modern memperhatikan empat tujuan berikut[6]:

1. **Confidentiality.** Informasi tersebut tidak dapat dipahami oleh siapa pun yang tidak diinginkan.
2. **Integrity.** Informasi tidak dapat diubah dalam penyimpanan atau transit antara pengirim dan penerima yang dituju tanpa perubahan yang terdeteksi.
3. **Non-repudiation.** Pencipta/pengirim informasi tidak dapat menyangkal pada tahap selanjutnya niat mereka dalam pembuatan atau transmisi informasi.
4. **Authentication.** Pengirim dan penerima dapat saling mengkonfirmasi identitas dan asal/tujuan informasi.



Gambar 3. Proses enkripsi dan deskripsi data[6]

3. HASIL DAN DISKUSI

3.1. Digital Signature Algorithm

Karena DSS mewajibkan penggunaan SHA-1, maka DSA atau RSA digunakan untuk mengenkripsi digest sebesar 160 bit. Ada 4 varian SHA dalam standard FIPS-180-2 dengan parameter yang berbeda yang dapat dilihat pada Tabel 1 di bawah ini.

Tabel 1. Varian SHA

Algoritma	Naskah (bit)	Blok (bit)	Word (bit)	Digest (bit)	Keamanan (bit)
SHA-1	$< 2^{64}$	512	32	160	80
SHA-256	$< 2^{64}$	512	32	256	128
SHA-384	$< 2^{128}$	1024	64	384	192
SHA-512	$< 2^{128}$	1024	64	512	256

Algoritma standar tanda tangan digital adalah sebagai berikut:

Kunci publik global:

Pertimbangkan bilangan prima p dan q pembagi prima dari (p-1) yang bergantung pada panjang bit L, dimana:

$p\ 2^{L-1} < p < 2^{L}$ dan

$q\ 2^{159} < q < 2^{160}$ dengan L=160 bits.

$g = h^{(p-1)/q} \bmod p$, dengan $1 < h < (p-1)$

pengirim private key:

Random or pseudorandom integer x dimana $0<x<q$

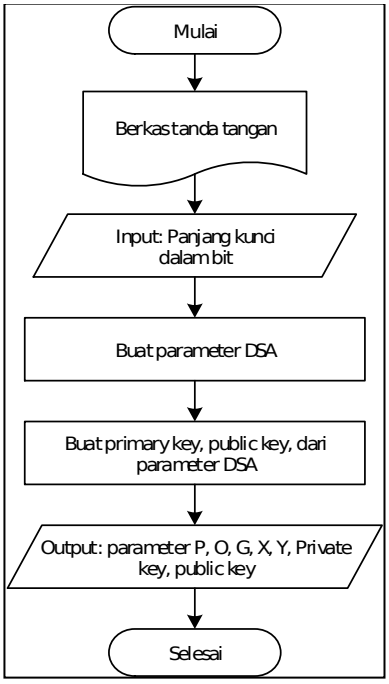
Pengirim kunci public:
$y = g^x \bmod p$

nomor rahasia:
Bilangan rahasia yang merupakan bilangan acak atau pseudorandom k dengan $0<k<q$

Pembuatan tanda tangan:
$r = (g^x \bmod p) \bmod q$
$s = [k\ l(H(m) + xr] \bmod q$
signature = (r,s)
verifikasi:
$W = (s')^{-1} \bmod q$
$U_1 = [H(m')w] \bmod q$
$U_2 = (r')w \bmod q$
$V = [(g^{U1}\ y^{U2}) \bmod p] \bmod q$

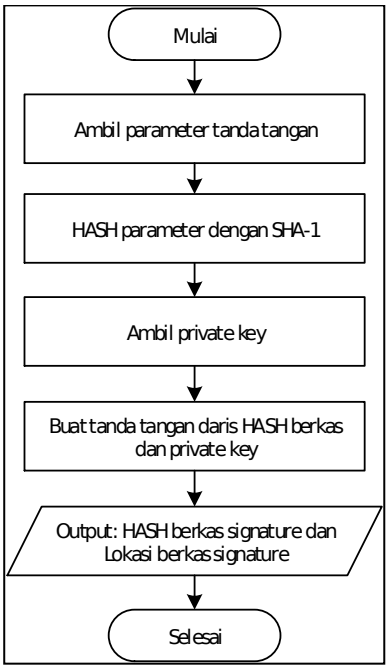
Flowchart dari langkah-langkah enkripsi DSA pembangkitan pasangan kunci (*create key*) diperlihatkan dalam Gambar 4 di bawah ini.

.



Gambar 4. Flowchart pembangkitan pasangan kunci

Konsep dari aplikasi ini adalah mengambil isi dari file untuk di bangkitkan tanda tangan digital yang kemudian di ubah ke suatu file lain oleh perangkat lunak yang berjenis EML. Proses pembangkitan tanda tangan ini terlihat dalam Gambar 5, *flowchart* pembangkitan tanda tangan seperti berikut.



Gambar 5. Flowchart pembangkit tanda tangan

Untuk melakukan proses pemberian tanda tangan, dibutuhkan sepasang kunci yaitu kunci privat dan kunci public serta parameter-parameter yang secara otomatis dibangkitkan oleh perangkat lunak yang kemudian disimpan dalam basis data. Hasil dari tanda tangan digital ini adalah dua baris string acak. Pengguna dapat menambahkan tanda-tangan asli yang berasal dari tulisan tangan yang sudah diubah ke bentuk file gambar dengan ukuran 64 x 64 pixels. Gambar tersebut akan diproses dan dijadikan kunci untuk menentukan hasil dari tanda tangan digital.

3.2. Karakteristik Pengguna

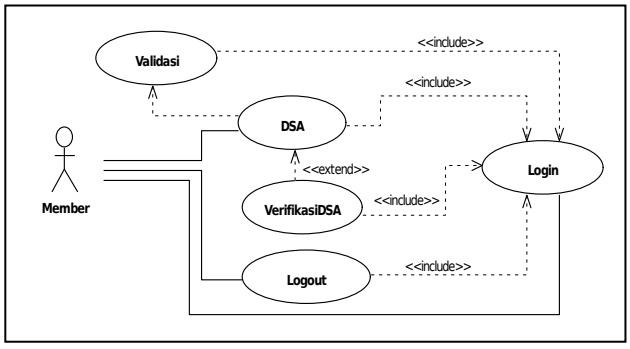
Perangkat lunak yang akan dikembangkan memliki kebutuhan berdasarkan sumber daya manusia yang diperlukan untuk menjalankan perangkat lunak tersebut, oleh karena itu di bawah ini adalah hal–hal yang harus terdapat dan di butuhkan untuk menangani sistem ini agar bekerja dengan baik dan maksimal adalah dengan menentukan karakteristik pengguna seperti pada Tabel 2 berikut:

Tabel 2. Identifikasi Karakteristik Pengguna

Level Autorisasi	Sumber Daya Manusia		
	Tingkatan Pengguna	Keahlian	Hak Akses
Member	Member	a. Mengerti pengoperasian komputer secara global. b. Dapat berinteraksi secara lancar dengan komputer / sistem. c. Mematuhi syarat dan ketentuan member yang berlaku dalam melakukan aktifitas pada perangkat lunak	Melakukan *autentifikasi login* agar masuk kedalam member area perangkat lunak dengan tujuan agar dapat melakukan order transaksi jual maupun beli dengan syarat menggunakan *IP* yang sama atau *autentifikasi* DSA apabila menggunakan alamat *IP* berbeda dari *session login* terakhir

3.3. Use case aplikasi kriptografi asimetris DSA

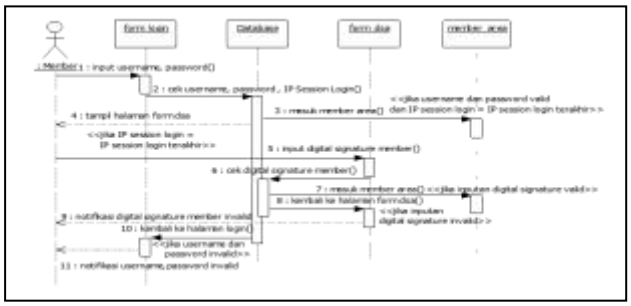
Dalam menganalisa kebutuhan perangkat lunak diperlukan pemahaman masalah secara menyeluruh dan mendefinisikan kebutuhan perangkat lunak yang berorientasi objek dilaksanakan berdasarkan proses-proses bisnis dan kebutuhan pemakai yang sudah diidentifikasikan untuk kemudian diekpresikan dengan menggunakan "use case" (diagram use case dengan high level use case) seperti Gambar 6 di bawah ini.



Gambar 6. Use case global

3.4. Sequence Digram DSA dan Verifikasi DSA

Proses bagaimana algoritma dalm sistem bekerja memverifikasi tanda tangan digital dijelaskan dalam *sequence diagram* seperti Gambar 6 berikut ini.



Gambar 7. Sequence diagram verifikasi DSA

Gambar 7 di atas menjelaskan dan menampilkan interaksi antar objek-objek bagaimana proses member berinteraksi dengan objek login dan DSA dalam sistem secara terperinci.

3.5. Implementasi Perangkat Lunak

Dengan menggunakan pendekatan berorientasi objek, hasil perancangan yang telah dibuat diterjemahkan ke dalam bahasa pemrograman yang dapat dieksekusi oleh komputer. Implementasi antarmuka untuk autentifikasi tanda tangan digital (DSA) member CV.DANOFAL'S dapat dilihat pada Gambar 8 di bawah ini.

Gambar 8. Autentifikasi Tanda Tangan Digital (DSA)

4. KESIMPULAN

Penggunaan Sistem Perangkat dengan menggunakan sistem keamanan merupakan hal yang sudah umum dilakukan oleh para programmer. Dengan penelitian yang dilakukan ini diharapkan dapat diketahui tingkat unjuk kerja Sistem Keamanan Single IP Login dan Kriptografi Asimetris DSA. Berdasarkan analisa dan implementasi yang dilakukan, dapat ditarik simpulan seperti berikut.

1. Sistem keamanan untuk setiap member dari perangkat lunak dibuat dengan teknik kriptografi agar tidak dapat diduplikasi oleh pengguna lainnya.
2. Penerapan algoritma enkripsi asimetris DSA (*Digital Signature Algorithm*) pada *login* perangkat lunak ini mempunyai dua fungsi utama yaitu Pembentukan tandatangan digital (*signature generation*), dan Pemeriksaan keabsahan tandatangan digital *(signature verivication)* dengan menggunakan teknik pembangkitan nilai dokumen menggunakan fungsi *Hash public key*, sehingga dengan metode ini sistem keamanan dapat di perketat.

UCAPAN TERIMAKASIH

Terlaksananya penelitian ini tentu saja tidak terlepas dari peran serta berbagai pihak. Ucapan terima kasih terutama disampaikan kepada pihak CV. DANOVAL'S yang berkenan memberikan informasi dan juga tempat pelaksanaan dari penelitian ini. Selain itu juga, ucapan terima kasih disampaikan kepada program studi teknik informatika, universitas Langlangbuana yang telah memberikan bantuan dana penelitian, sehingga penelitian ini dapat terlaksana dengan baik dan maksimal seperti yang telah direncanakan.

DAFTAR PUSTAKA

[1] M. S. Hasibuan, "Keylogger pada Aspek Keamanan Komputer," *Teknovasi*, vol. 3, no. 1, pp. 8–15, 2016.

[2] A. Choudary, "What is Computer Security? Introduction to Computer Security," *Edureka*, 2021. https://www.edureka.co/blog/what-is-computer-security/ (accessed Feb. 18, 2022).

[3] A. Yulianti, *Urgensi Digitalisasi Sistem Pendaftaran Tanah*. Bandung: Alumni, 2022.

[4] Simplilearn, "Digital Signature Algorithm (DSA) in Cryptography: How It Works and Advantages," 30483BC. https://www.simplilearn.com/tutorials/cryptography-tutorial/digital-signature-algorithm#what_is_the_dsa_algorithm (accessed Feb. 26, 2022).

[5] S. Babu, "Medical Image Authentication Using Quartic Digital Signature Algorithm," *Int. J. Intell. Inf. Syst.*, vol. 7, no. 4, p. 38, 2018, doi: 10.11648/j.ijiis.20180704.11.

[6] K. Richards, "Cryptography," *Techtarget*, 2021. https://www.techtarget.com/searchsecurity/definition/cryptography (accessed Feb. 25, 2022).