Penerapan Sistem Keamanan Transaksi Bisnis Menggunakan Base64 dan *Verification Code* Pada Sistem Jejaring Klaster

Artikel Ilmiah

Peneliti :

Dwi Kurniawan (672012711)

Suprihadi, S.Si., M.Kom.

Dian W. Chandra, S.Kom, M.Cs.

Program Studi Teknik Informatika

Fakultas Teknologi Informasi

Universitas Kristen Satya Wacana

April 2013

FAKULTAS TEKNOLOGI INFORMASI
Universitas Kristen Satya Wacana

Memo

Tanggal : 4 Juli 2013
Dari : Kaprogdi TI
Kepada : Bagian Sirkulasi Perpustakaan UKSW
Perihal : CD TA Mahasiswa

Dengan hormat.

Melalui memo ini, kami beritahukan bahwa Kaprogdi TI Bpk Dian W. Chandra, M.Cs sedang berada di Malaysia dari tgl 1 Juli sampai tgl 6 Juli 2013 dan tidak bisa menandatangani Pernyataan Tidak Plagiat dan Persetujuan Akses atas nama mahasiswa :

Nama : Dwi Kurniawan
NIM : 672012711

Demikian memo ini kami sampaikan.
Terima kasih atas perhatian dan bantuan yang diberikan.

Salam,

Teguh Wahyono, S.Kom., M.Cs
Wakil Dekan FTI

Penerapan Sistem Keamanan Transaksi Bisnis Menggunakan Base64 dan *Verification Code* Pada Sistem Jejaring Klaster

Oleh,

Dwi Kurniawan
NIM : 672012711

Artikel Ilmiah

Diajukan Kepada Program Studi Teknik Informatika , Fakultas Teknologi Informasi guna memenuhi sebagian dari persyaratan untuk mencapai gelar Sarjana Komputer

Disetujui oleh,

Suprihadi, S.Si., M.Kom.	Dian W. Chandra, S.Kom., M.Cs.
Pembimbing 1	Pembimbing 2

Diketahui oleh,

Dr. Dharmaputra T. Palekahelu, M.Pd.	Dian W. Chandra, S.Kom., M.Cs.
Dekan	Ketua Program Studi

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
SALATIGA
2013

Lembar Pengesahan

Judul Tugas Akhir	: Penerapan Sistem Keamanan Transaksi Bisnis Menggunakan Base64 dan *Verification Code* Pada Sistem Jejaring Klaster
Nama Mahasiswa	: Dwi Kurniawan
NIM	: 672012711
Program Studi	: Teknik Informatika
Fakultas	: Teknologi Informasi

Menyetujui,

Suprihadi, S.Si., M.Kom.	Dian W. Chandra, S.Kom., M.Cs.
Pembimbing 1	Pembimbing 2

Mengesahkan,

Dr. Dharmaputra T. Palekahelu, M.Pd.	Dian W. Chandra, S.Kom., M.Cs.
Dekan	Ketua Program Studi

Dinyatakan Lulus Ujian tanggal: 21 Mei 2013

Penguji:

1. Indrastanti R. Widiasari, M.T.
2. Teguh Indra Bayu, S.Kom., M.Cs.

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN TIDAK PLAGIAT DAN PERSETUJUAN AKSES

Sebagai sivitas akademik Universitas Kristen Satya Wacana, saya yang bertanda tangan di bawah ini:

Nama : Dwi Kurniawan

NIM : 672012711 Email : dwikyankcola@gmail.com

Fakultas : Teknologi Informasi Program Studi : Teknik Informatika

Judul tugas akhir : Penerapan Sistem Keamanan Transaksi Bisnis Menggunakan Base64 Dan Verificationcode Pada Sistem Jaringan Klaster

Dengan ini menyerahkan karya tersebut di atas untuk disimpan dalam Koleksi Digital Perpustakaan Universitas dengan ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

☑ a. Saya mengijinkan karya tersebut diunggah ke dalam aplikasi Koleksi Digital Perpustakaan Universitas, dan/atau portal GARUDA.

☐ b. Saya tidak mengijinkan karya tersebut diunggah ke dalam aplikasi Koleksi Digital Perpustakaan Universitas, dan/atau portal GARUDA. *

* *pilih b harus dilampiri dengan surat dari Dekan/ Kaprodi atau pembimbing TA dengan diketahui oleh pimpinan fakultas yang menjelaskan alasan pilihan. Yang akan ditampilkan adalah halaman judul + abstrak*

Dengan ini saya juga menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/ terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/ implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
5. Saya menyerahkan hak non-eksklusif kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik di atas dan norma hukum yang berlaku.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

05 Juli 2018
Tanggal penyerahan

Dwi Kurniawan
Tanda tangan & nama terang mahasiswa

Mengetahui,

SUPRIHADI, S.Si, M.Kom
Tanda tangan & nama terang pembimbing I

Tanda tangan & nama terang pembimbing II

Penerapan Sistem Keamanan Transaksi Bisnis Menggunakan Base64 dan *Verification Code* Pada Sistem Jejaring Klaster

[1)]Dwi Kurniawan, [2)]Suprihadi, [3)] Dian W. Chandra

Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50711, Indonesia
Email: [1)]672012711@student.uksw.edu, [2)]suprihadi@staff.uksw.edu,
[3)]dian.chandra@staff.uksw.edu

Abstract

Information of technology is grow up now, for example is a e-commerce. Network clusters system is an e-commerce application that is for an UKM and cluster in Indonesia. A things that be an important factor in e-commerce is there are guarantee that show that a people that do this business transaction is a member in this e-commerce. Because of that reason, we need a system or mechanism to make it safety. A researcher made a safety system in business transactionin e-commerce transaction, this system cluster of network use base64 method and verification method through an email. This system implementation is using framework codeIgniter technology in the use of PHP programming. The result is a security system on login process and purchases data transmission using base64. Verification code used as formal authentication on the purchasing process for members cluster networking.

Keywords*: *security system, base64, cluster networking system

Abstrak

Teknologi informasi saat ini sangat berkembang pesat, salah satu contohnya adalah *e-commerce*. Sistem jejaring klaster adalah sebuah aplikasi *e-commerce* yang diperuntukkan bagi para UKM dan klaster di Indonesia. Salah satu faktor penting dalam suatu *e-commerce* adalah adanya jaminan bahwa yang melakukan transaksi bisnis adalah seorang pelanggan yang sudah terdaftar di *e-commerce* tersebut. Oleh karena itu, pada aplikasi *e-commerce* dibutuhkan sistem atau suatu mekanisme untuk mengamankan transaksi bisnis. Pada penelitian ini telah dirancang sebuah sistem keamanan transaksi bisnis pada aplikasi *e-commerce* Sistem jejaring klaster menggunakan metode base64 dan *verification code* melalui *e-mail*. Sistem ini diimplementasikan menggunakan teknologi Framework CodeIgniter pada bahasa pemrograman PHP. Hasil penelitian ini didapatkan pengamanan menggunakan base64 dan *verification code* sehingga Sistem jejaring klaster menjadi lebih aman dibandingkan sebelumnya.

Kata Kunci : sistem keamanan, base64, sistem jejaring klaster

---

[1)] Mahasiswa Fakultas Teknologi Informasi Universitas Kristen Satya Wacana
[2)] Staf Pengajar Fakultas Teknologi Informasi Universitas Kristen Satya Wacana
[3)] Staf Pengajar Fakultas Teknologi Informasi Universitas Kristen Satya Wacana

1. Pendahuluan

Aspek keamanan data merupakan salah satu aspek penting dari sebuah sistem informasi, apalagi sistem informasi tersebut menyangkut bisnis dan informasi penting dari suatu lembaga atau *privacy* seseorang. Keamanan data juga sangat dibutuhkan pada suatu aplikasi *online* mengingat kejahatan di dunia maya semakin marak, antara lain tindakan *spy* dan *crack* oleh seseorang dengan maksud dan tujuan yang tidak mau dipertanggungjawabkan. Salah satu keamanan data yang dibutuhkan adalah penyandian data atau informasi yang disebut dengan teknologi kriptografi.

Teknologi kriptografi pada prinsipnya merupakan suatu metode untuk pengamanan data dengan cara penyandian data, yaitu data (*plaintext*) menjadi sandi (*chipertext*) dimana orang tidak dapat membaca karena berisi kode dan simbol. Teknologi kriptografi dibutuhkan apabila data tersebut melewati media transmisi sehingga sangat rentan untuk disadap oleh pihak lain. Data penting pada aplikasi *online* seperti *password*, data transaksi bisnis pada *e-commerce* misalnya nomor tagihan dan nomor konfirmasi pembayaran, dan data rahasia atau *privacy* seseorang sangat disarankan untuk disandikan pada level media transmisi maupun pada basis data.

Berdasarkan dari uraian diatas, maka pada penelitian ini telah dirancang sebuah sistem atau mekanisme kerja untuk mengamankan suatu data transaksi bisnis pada *e-commerce* sistem jejaring klaster. Pada perancangan sistem menerapkan sebuah *tools* pengamanan data, yaitu metode penyandian data atau enkripsi data yang ada dalam PHP, yaitu base64. Base64 yang diterapkan pada aplikasi *client* memungkinkan data transaksi bisnis pada aplikasi *e-commerce* yang melalui media transmisi dapat disandikan. Base64 tersebut tidak mengamankan sepenuhnya apabila seorang *spy* atau terdapat *spyware* yang mampu men-*decode* data hasil *encode* base64. Oleh karena itu, dibutuhkan mekanisme tambahan pada transaksi bisnis pada aplikasi *e-commerce* sistem jejaring klaster yaitu verifikasi *e-mail* pada transaksi pembelian guna proses autentikasi pelanggan, Apabila *password login* pelanggan telah dibobol, tetapi sistem masih dapat menjamin bahwa yang melakukan transaksi pembelian adalah pelanggan *e-commerce* sistem jejaring klaster.

2. Kajian Pustaka

Penelitian terdahulu adalah penelitian tentang perancangan dan implementasi sebuah aplikasi *web* yang berfungsi sebagai sistem jejaring klaster. Hasil penelitian tersebut berupa suatu sistem jejaring klaster menggunakan metode *Model View Controller* (MVC) dengan teknologi *framework CodeIgniter* (CI) yang mampu menyediakan *website* bagi klaster anggota dengan memanfaatkan satu alamat domain[1]. Pada sistem jejaring klaster tersebut juga sudah dilengkapi dengan aplikasi *e-commerce* untuk pembeli dan memiliki layanan konfirmasi pembayaran. Akan tetapi, pada penelitian tersebut belum

terdapat aplikasi Sistem keamanan data *e-commerce* untuk pembeli serta belum memiliki sistem keamanan saat proses pembayaran.

Pada penelitian sistem jejaring klaster sebelumnya belum menerapkan keamanan pada data *e-commerce*. Hal ini menimbulkan permasalahan keamanan data *e-commerce* jika jatuh di tangan orang yang tidak bertanggung jawab. Dari hal tersebut maka pada penelitian ini akan dilakukan perancangan aplikasi sistem keamanan transaksi bisnis pada sistem *web* iKlaster menggunakan base64 untuk mengamankan proses transaksi bisnis. Sistem keamanan akan diletakkan antara *client* dan *server*.

iKlaster merupakan sebuah Sistem Jejaring Klaster, yaitu aplikasi *web* yang memanfaatkan satu alamat domain dengan menggunakan pendekatan *e-commerce* model *marketplace concentrator* dan konsep *social network* yang dikembangkan dengan metode *prototyping model* supaya aplikasi yang dihasilkan sesuai dengan kebutuhan Klaster serta sebagai sarana promosi dan pemasaran bagi produk anggota klaster. Sedangkan konsep *social network* dipergunakan pada aplikasi ini sebagai sarana berjejaring dan berkomunikasi bisnis antar anggota klaster[1]. Klaster merupakan konsentrasi geografis perusahaan dan institusi yang saling berhubungan pada sektor tertentu. Mereka berhubungan karena kebersamaan dan saling melengkapi. Klaster mendorong industri untuk bersaing satu sama lain. Selain industri, klaster termasuk juga pemerintah dan industri yang memberikan dukungan pelayanan seperti pelatihan, pendidikan, informasi, penelitian, dan dukungan teknologi.

Sistem adalah suatu jaringan kerja dari prosedur yang saling berhubungan, berkumpul bersama sama untuk melakukan atau untuk menyelesaikan suatu sasaran tertentu[2]. Keamanan adalah suatu kinerja dalam menghadapi masalah baik internal maupun eksternal yang terjadi terhadap suatu ruang lingkup demi terciptanya suatu keadaan yang seharusnya. Dalam sistem Keamanan Jejaring klaster ini terdapat ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentikasi data, yang didefinisikan sebagai Kriptografi [3]. Kriptografi berasal dari dua kata Yunani, yaitu *Crypto* yang berarti rahasia dan *Grapho* yang berarti menulis. Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu data.

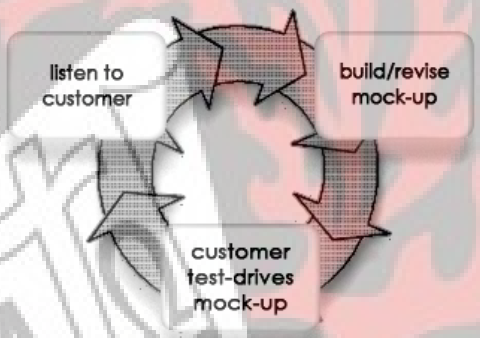
Base64 adalah sebuah skema *encoding* yang merepresentasikan data biner ke dalam format ASCII. Umumnya digunakan pada berbagai aplikasi, seperti e-*mail* via MIME, data XML, atau untuk keperluan *encoding* URL. Prinsip *encoding*-nya adalah dengan memilih kumpulan dari 64 karakter yang dapat di-*print*. Data dapat disimpan dan ditransfer melewati media yang didesain untuk menangani data tekstual. penggunaan lain *encoding* base64 adalah untuk melakukan *obfuscation* atau pengacakan data. Fungsi kegunaan dari base64 dalam sistem Jejaring Klaster pada sisi layer *client* yaitu dengan upaya menyandikan Proses Login dan proses Checkout Pembelian. Dan fungsi pada media transmisi dapat di sandikan dalam bentuk kode lalu di-*decode* pada *layer* aplikasi *server*.

Verification Code adalah kode yang diberikan kepada pengguna atau pihak yang bersangkutan sebagai *feedback* dari transaksi yang telah dilakukan. Kode

verifikasi digunakan sebagai cara untuk melakukan validasi apakah pengguna atau pihak yang bersangkutan telah melakukan transaksi. Kode verifikasi juga dapat digunakan sebagai sarana untuk melakukan pengecekan apakah pengguna benar-benar melakukan sebuah transaksi. Cara pemberian *verification code* pada umumnya dilakukan melalui media email, sms dan lain-lain. Dalam penelitian ini *verification code* digunakan sebagai media pengecekan apakah pelanggan dari iKlaster pada proses registrasi dan pembayaran melalui rekening. Jika kode verifikasi yang sesuai dengan yang ada pada sistem iKlaster maka transaksi yang dilakukan pelanggan dapat dinyatakan valid.

3. Metode dan Perancangan Sistem

Metode penelitian menggunakan model *prototype*, model *prototype* merupakan suatu teknik untuk mengumpulkan informasi tertentu mengenai kebutuhan-kebutuhan informasi pengguna secara cepat. Dengan metode *prototype*, pengembang dan pelanggan dapat saling berinteraksi selama proses pembuatan sistem. Pada Gambar 1 merupakan alur model *prototype*.



Gambar 1. *Prototype Model* [5]

Pada tahapan pertama, yaitu *listen to customer* atau *information gathering* tentang kebutuhan aplikasi yang akan dibangun, dilakukan tahap wawancara dengan klaster. Informasi yang dicari yang berhubungan dengan proses transaksi bisnis. Setelah mengetahui kebutuhan umum aplikasi yang akan di bangun maka dilakukan studi pustaka tentang bagaimana membuat suatu sistem keamanan yang dapat memenuhi kebutuhan.

Tahapan selanjutnya dalam metode *prototype* yaitu *build/revise mock-up* atau membangun aplikasi secara cepat. Pada tahap ini dilakukan pembuatan sistem keamanan aplikasi secara cepat, lebih memfokuskan pada keamanan data transaksi bisnis aplikasi sesuai dengan kebutuhan umum yang diketahui pada tahap pertama. Tahap ini menghasilkan *prototype* 1.

Tahap akhir adalah melakukan uji dan evaluasi *prototype* oleh *user*. Evaluasi *prototype* digunakan untuk mendapatkan umpan balik apakah aplikasi sudah sesuai dengan kebutuhan klaster. Evaluasi dilakukan dengan cara wawancara. Jika hasil uji dan evaluasi *prototype* belum sesuai dengan kebutuhan

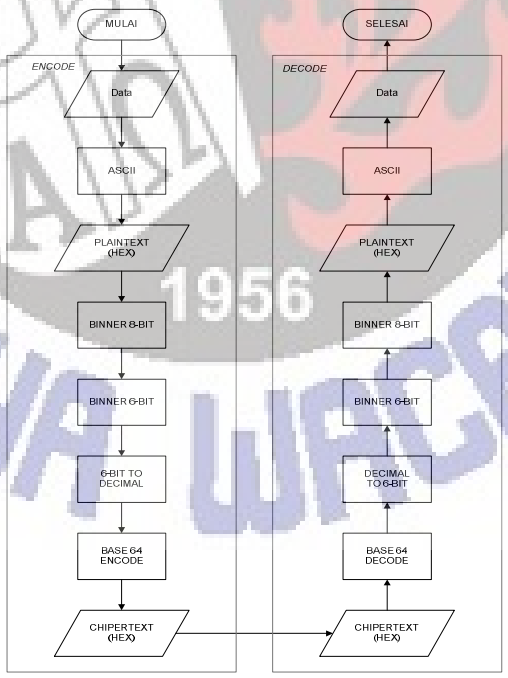
klaster, maka dilakukan proses perbaikan dimulai kembali ke tahap awal dan dilanjutkan ke tahap berikutnya.

Sistem keamanan transaksi bisnis *e-commerce web* iKlaster akan menggunakan base64. Base64 dipilih karena memastikan data tetap utuh tanpa ada perubahan selama proses pengiriman. Base64 *alphabet* dapat dilihat pada Gambar 2.

Value	Encoding	Value	Encoding	Value	Encoding	Value	Encoding
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v		
14	O	31	f	48	w	(pad)	=
15	P	32	g	49	x		
16	Q	33	h	50	y		

Gambar 2. Base64 *Alphabet* [6]

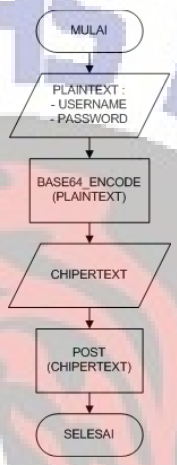
Pada Gambar 2 merupakan tabel base64 *alphabet*. *Value encoding* data berasal dari *alphabet* A-Z dan angka 0-9 ditambah karakter + dan /. *Padding* yang diletakkan menggunakan karakter =.



Gambar 3. Diagram Alir Proses Pengodean Metode Base64

Gambar 3 merupakan alir proses pengkodean dengan menggunakan base64. Pada proses *encrypt* data akan diproses dengan menggunakan ASCII agar data

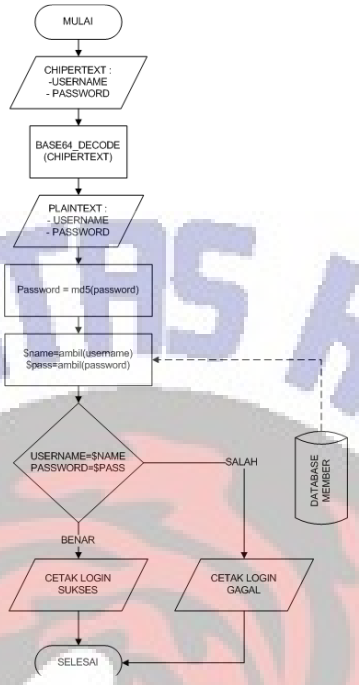
plaintext berubah menjadi *plaintext hexa*. Dari data *plaintext hexa* akan diproses menggunakan biner 8 bit, 6 bit, dan 6 bit *to decimal*. Kemudian akan di *encode* menggunakan base64 yang menghasilkan *chipertext hexa*. Pada proses *decrypt*, data *chipertext hexa* di *encode* menggunakan base64. Hasil *decode* akan diproses menggunakan 6 bit *to decimal*, 6 bit dan 8 bit. Setelah data kembali dalam bentuk *plaintext hexa*, data akan kembali diproses dengan ASCII untuk dikembalikan ke bentuk data awal.



Gambar 4. Diagram Alir Proses Enkripsi *Login* Pada Aplikasi *Client*

Proses *login* ke aplikasi *client* pada *web* iKlaster disajikan dalam *flowchart* pada Gambar 4. Data yang digunakan untuk login ke aplikasi *client web* iKlaster adalah *username* dan *password* dalam bentuk *plaintext*. Pada Gambar 4 merupakan proses *login* ke aplikasi *client web* iKlaster. Data *username* dan *password* yang akan dikirim sebelumnya akan di-*encode* menggunakan metode base64. Hasil dari proses *encode* adalah *chipertext username* dan *password* yang siap di *post*.

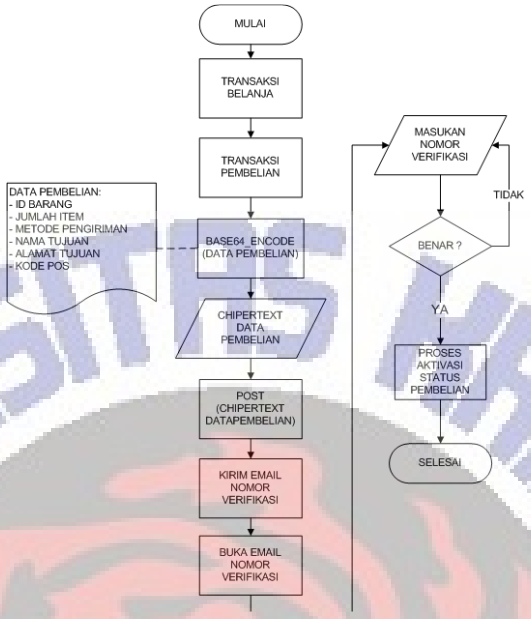
Proses *login* ke aplikasi *server* pada *web* iKlaster disajikan dalam alir proses *flowchart*. Data yang digunakan untuk *login* ke aplikasi *server web* iKlaster adalah *username* dan *password* yang sudah di *encode* dengan metode base64. Alir proses *login* ke aplikasi *server web* iKlaster dapat dilihat pada Gambar 5.



Gambar 5. Diagram Alir Proses *Login* Aplikasi Server

Pada Gambar 5 merupakan alir proses *login* ke aplikasi *server web* iKlaster. Data *username* dan *password* dikirim dalam bentuk *chipertext* hasil dari proses *encoding* base64. Data *username* dan *password* kemudian di *decode* dengan menggunakan base64 agar kembali menjadi *plaintext*. Untuk keamanan data *password* akan disandikan menggunakan md5. Data *username* dan *hash* md5 *password* akan dicocokkan dengan data yang ada pada *database*. Data *login* akan diverifikasi jika berhasil akan dilanjutkan ke proses selanjutnya, jika gagal akan diberikan informasi gagal *login*.

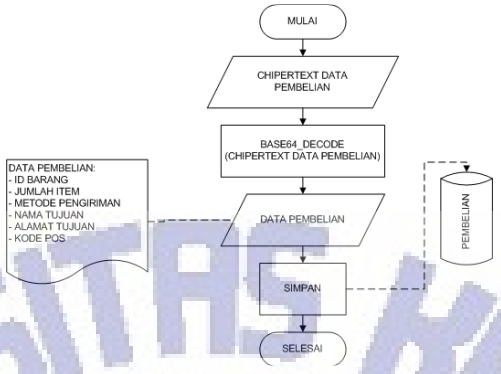
Dalam sistem keamanan proses transaksi bisnis *web* iKlaster data pembelian akan di *encode* dengan menggunakan base64. *Encode* data pembelian bertujuan agar keamanan data pembelian dapat terjaga dengan baik. Data pembelian hanya dapat dilihat oleh pihak yang memiliki otoritas terhadap data. Proses *encoding* data pembelian dengan menggunakan base64 akan disajikan dalam bentuk *flowchart*. Alir proses *encoding* data pembelian dengan metode base64 dapat dilihat pada Gambar 6.



Gambar 6. Alir Proses *Encoding* Data Pembelian Menggunakan base64

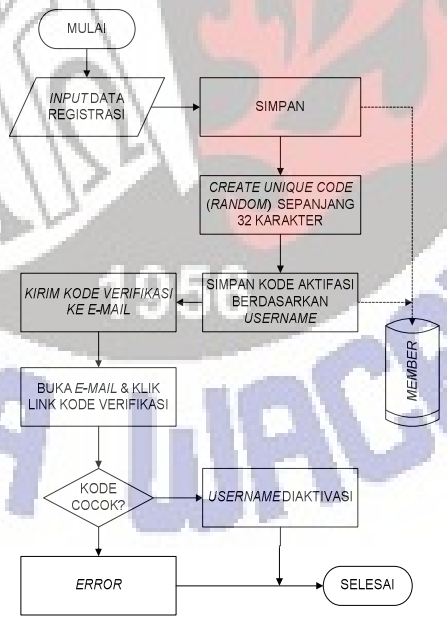
Pada Gambar 6 merupakan alir proses *encoding* menggunakan metode base64. Pada proses *encoding* data di *input* melalui proses transaksi belanja kemudian diteruskan ke proses transaksi pembelian. Data pembelian kemudian akan di *encode* dengan menggunakan metode base64. Data pembelian yang di *encode* adalah *id* barang, jumlah *item*, metode pengiriman, nama tujuan, alamat tujuan dan kode pos. Data pembelian tersebut akan menjadi data pembelian menjadi bentuk *chipertext*. Data *chipertext* pembelian kemudian akan di *post*. Proses selanjutnya adalah pengiriman kode nomor verifikasi melalui email ke pelanggan. Pelanggan akan membuka email kode nomor verifikasi tersebut dan memasukkan kode nomor verifikasi. Jika *input* kode nomor verifikasi benar maka transaksi pembelian akan di ubah statusnya menjadi aktif.

Dalam sistem keamanan proses transaksi bisnis *web* iKlaster data pembelian yang sudah di *encode* dengan metode base64 akan di *decode* kembali agar dapat dibaca oleh pihak yang memiliki otoritas data. Proses *decoding* data pembelian dengan menggunakan metode base64 akan disajikan dalam bentuk *flowchart*. Alir proses *decoding* data pembelian dengan metode base64 dapat dilihat pada Gambar 7.



Gambar 7. Alir Proses *Decoding* Data Pembelian Menggunakan base64

Pada Gambar 7 merupakan alir proses *decoding* data pembelian menggunakan metode base64. Pada proses *decoding* data pembelian yang di *encode* menjadi *chipertext* data akan di *decode* dengan menggunakan base64. Setelah proses *decoding* berhasil data pembelian akan kembali menjadi data dalam bentuk *plaintext*. Data pembelian tersebut antara lain adalah id barang, jumlah *item*, metode pengiriman, nama tujuan, alamat tujuan dan kode pos. Data pembelian yang sudah dalam bentuk *plaintext* akan disimpan ke *database*.

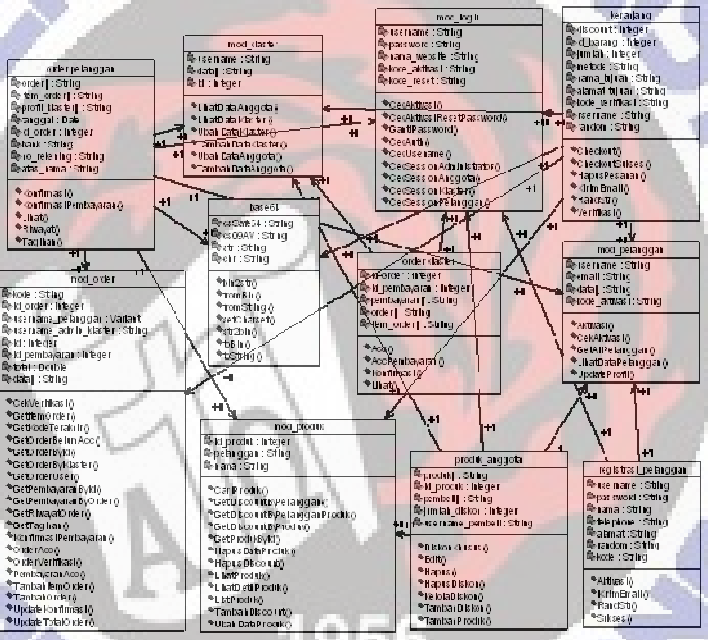


Gambar 8. DiagramAlir Proses *Verification Code*

Gambar 8 merupakan diagram alir proses *verification code* pada proses registrasi, Dimulai dari *input* data registrasi, kemudian data tersebut akan disimpan ke dalam *database member* sistem jejaring klaster. Setelah itu akan dibuat kode unik yang merupakan kode aktivasi akun secara *random* sepanjang 32

karakter dan kode aktivasi tersebut disimpan dalam *database* berdasarkan *username*. Kemudian kode tersebut dikirimkan pada *e-mail* yang digunakan untuk melakukan registrasi yang berupa *link* aktivasi. Check e-mail dilakukan oleh user, selanjutnya klik link, secara otomatis akan mencocokan kode *username* yang diaktifkan. Jika benar maka aktivasi berhasil, jika tidak maka akun gagal di aktivasi.

Class diagram menggambarkan interaksi antar *class* serta atribut-atribut yang melekat pada *class* tersebut. Pada Gambar 9 merupakan *Class* dari sistem keamanan *web* iKlaster yang dikembangkan. Pada *web* iKlaster ini terdapat 10 *class* dari *web* iKlaster dan 1 *class* tambahan untuk mendukung proses pengamanan data menggunakan metode base64.



Gambar 9. *Class Diagram* iKlaster

Pada Gambar 9 merupakan *class diagram* pada *web* iKlaster. *Class* yang ada pada *class diagram* tersebut adalah *class* order pelanggan berisi fungsi untuk mengelola proses pengorderan oleh pelanggan, *class* mod_login berisi fungsi *query* untuk melakukan *login*, *class* keranjang berisi fungsi untuk pemesanan produk klaster, *class* mod_pelanggan berisi fungsi *query* untuk pelanggan, *class* registrasi_pelanggan berisi fungsi untuk registrasi pelanggan, *class* order klaster berisi fungsi untuk melakukan order klaster, *class* mod_klaster berisi fungsi *query* untuk klaster, *class* mod_order berisi fungsi *query* untuk order, *class* mod_produk berisi fungsi *query* untuk produk, *class* produk_anggota berisi fungsi untuk mengelola produk anggota klaster dan *class* base64 berisi fungsi untuk melakukan *encoding decoding*. *Class* base64 merupakan *class* yang digunakan untuk mendukung sistem keamanan proses transaksi bisnis dengan menggunakan metode base64.

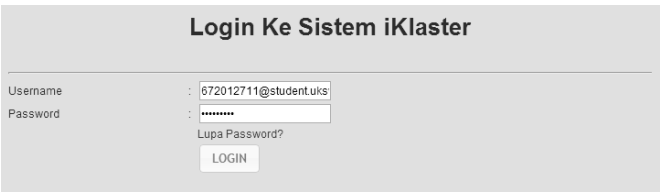
Setelah merancang sistem dengan UML langkah selanjutnya adalah perancangan *database*. Tabel merupakan salah satu komponen penting dalam pembuatan *database*. Tabel-tabel tersebut digunakan untuk menyimpan data yang berisi *field-field* sebagai kolom penyimpanan data pada setiap tabel. Dalam pembuatan sistem keamanan ini akan terdapat 7 (tujuh) tabel dalam *database* dan tentunya antara tabel yang satu dengan tabel yang lain saling berhubungan. Dalam penelitian ini di fokuskan pada beberapa tabel yaitu tabel-tabel yang berpengaruh dalam aktivitas pelanggan ke sistem *web* iKlaster, Tabel 1 yang digunakan antara lain sebagai berikut.

Tabel 1. Tabel Pendukung Aplikasi

No	Tabel	Kegunaan
1.	tbl_diskon_pembeli	Digunakan untuk menentukan diskon pembeli
2.	tbl_item_order	Digunakan untuk data item
3.	tbl_konfirmasi_pembayaran	Digunakan untuk mencatat konfirmasi pembayaran
4.	tbl_order	Digunakan untuk mencatat order
5.	tbl_pelanggan	Digunakan untuk menyimpann data pelanggan
6.	tbl_login	Digunakan untuk login
7.	tbl_produk_barang	Digunakan untuk data produk

4. Implementasi dan Pembahasan

Untuk pengaturan awal pada *framework CodeIgniter* yaitu mengunduh *plugin CodeIgniter* dari *CodeIgniter.com,* kemudian mengganti nama *folder* dengan *cluster* dan meletakkannya di *directory sites/www* pada Spanel iKlaster.com. Pengaturan kedua adalah pengaturan *base_url*, yang terletak pada directory *Spanel/sites*/iKlaster*.com/www/config/config.*php. Untuk menentukan halaman pertama yang akan terbuka saat aplikasi dijalankan maka perlu pengaturan *controller* utama yang akan dipanggil. Pengaturan tersebut terletak pada *directory application/config/routes.*php. *Library* yang otomatis dipanggil ketika aplikasi dijalankan adalah *library database.* Pengaturannya adalah pada file *autoload* yang terletak pada *directory application/config/autoload.*php. Untuk menghubungkan basis data yang sudah dibuat dengan aplikasi yang dibuat dibutuhkan beberapa pengaturan. Pengaturan ini dilakukan pada *file database.php* yang terdapat dalam *application/config/database.php.*



Gambar 10. Tampilan *Login* Pelanggan

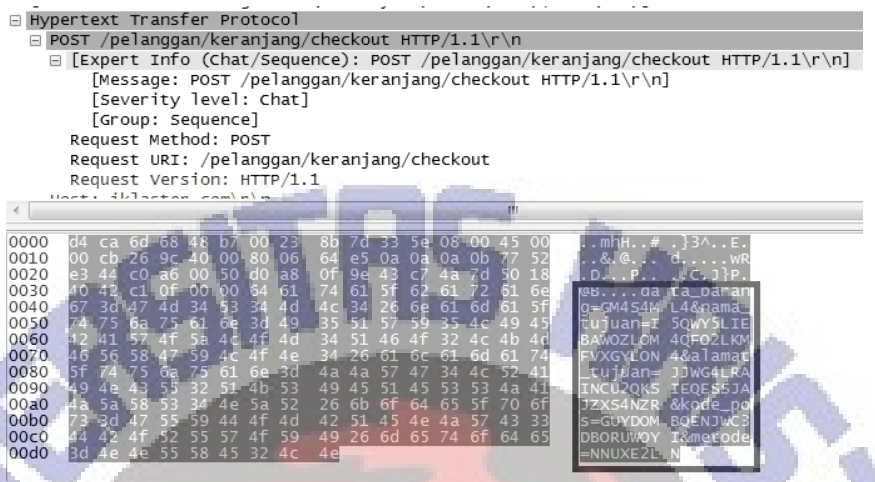
Gambar 10 merupakan tampilan untuk *login* sebagai pelanggan ke *web* iKlaster. Pada *field username* diisi dengan email yang digunakan pada saat registrasi. Untuk mengetahui apakah data *login* yang dikirim dalam keadaan aman ter-enkripsi dengan base64, maka akan dilakukan *capture* paket menggunakan Wireshark. *Capture* paket *login* dapat dilihat pada bagian pengujian. Pada halaman *login* dibagi menjadi 3 yaitu *view*, *controller* dan *model*. Hasil pengamatan dengan menggunakan Wireshark dapat dilihat pada Gambar 11.

Gambar 11. Data Pengamatan Proses *Login*

Setelah melakukan *login* ke dalam sistem *e-commerce web* iKlaster pelanggan dapat melakukan pemesanan. Tampilan untuk melakukan pemesanan barang dapat dilihat pada Gambar 12.

Gambar 12. Tampilan Pemesanan Barang

Setelah melakukan pemesanan barang pelanggan harus melakukan proses *check-out*. Pada proses *check-out* ini berisi data barang, nama tujuan, alamat tujuan, kode pos dan metode. Untuk keperluan keamanan data maka data *check-out* disandikan dengan menggunakan base64. Hasil dari pengamatan data *check-out* dengan menggunakan Wireshark dapat dilihat pada Gambar 13.



Gambar 13. Hasil Pengamatan Data *Checkout*

Gambar 14. Tampilan Email Verifikasi Pembayaran

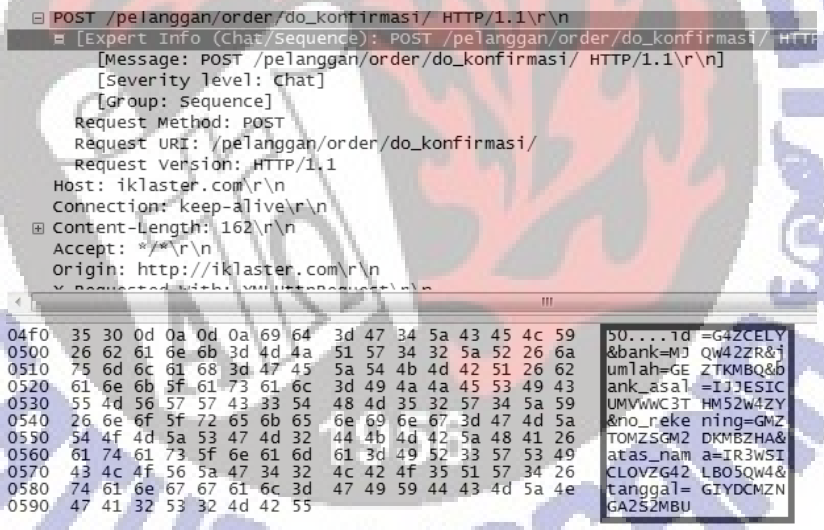
Gambar 14 merupakan verifikasi pembayaran yang dikirim oleh *server* iKlaster. Setelah *link* pada email tersebut dibuka maka pelanggan akan di *redirect* ke halaman konfirmasi pembayaran.

Gambar 15. Tampilan Verifikasi Pembayaran

Pada Gambar 15 merupakan verifikasi pembayaran yang didapat pelanggan setelah melakukan klik *link* pada email verifikasi. Pelanggan harus melakukan klik pada *link* konfirmasi pada bagian status.

Gambar 16. Konfirmasi Pembayaran

Pada Gambar 16 merupakan *form* untuk melakukan konfirmasi pembayaran. Pelanggan wajib mengisikan data sesuai dengan rekening bank yang dimilikinya. Hasil pengamatan menggunakan Wireshark dapat dilihat pada Gambar 17.



Gambar 17. Paket Data Konfirmasi

Untuk kode program *encode decode* pada nibbler.js dengan metode base64 dapat dilihat pada Kode Program 1.

Kode Program 1. *Encode Decode* base64

```
1.  encode = function (input) {return translate(input, dataBits,
    codeBits, false);};
2.  decode = function (input) {return translate(input, codeBits,
    dataBits, true);};
3.  translate = function (input, bitsIn, bitsOut, decoding) {
4.  var i, len, chr, byteIn, buffer, size, output, write;
5.  write = function (n) {
6.  if (!decoding) {
7.  output.push(keyString.charAt(n));
```

```
8.  } else if (arrayData) {
9.  output.push(n);
10. } else {
11. output.push(String.fromCharCode(n));
12. }
13. };
14. buffer = 0;
15. size = 0;
16. output = [];
17. len = input.length;
18. for (i = 0; i < len; i += 1) {
19. size += bitsIn;
20. if (decoding) {
21. chr = input.charAt(i);
22. byteIn = keyString.indexOf(chr);
23. if (chr === pad) {
24. break;
25. } else if (byteIn < 0) {
26. throw 'the character "' + chr + '" is not a member of ' +
    keyString;}
27. } else {
28. if (arrayData) {
29. byteIn = input[i];
30. } else {
31. byteIn = input.charCodeAt(i);
32. }
33. if ((byteIn | max) !== max) {
34. throw byteIn + " is outside the range 0-" + max;}
35. }
36. buffer = (buffer << bitsIn) | byteIn;
37. while (size >= bitsOut) {
38. size -= bitsOut;
39. write(buffer >> size);
40. buffer &= mask[size];}}
41. if (!decoding && size > 0) {
42. write(buffer << (bitsOut - size));
43. len = output.length % group;
44. for (i = 0; i < len; i += 1) {
45. output.push(pad);}}
46. ‘return (arrayData && decoding) ? output :
    output.join('');};
```

Berikut ini adalah penjelasan dari Kode Program 1, baris 1 proses melakukan *encode*, baris 2 proses melakukan *decode.* Baris 3 penamaan fungsi untuk memproses *decode* / *encode.* Baris 4 membuat *variable* yang diperlukan. Baris 5-13 proses untuk mengubah *bytes* ke dalam *string.* Baris 14-16 mengisi *variable* baris 4 dengan nilai *default.* Baris 17-40 proses *decode* / *encode.* Baris 41-45 proses pengubah *bytes* ke dalam *string.* Baris 46 pengembalian data. Untuk *encode* menggunakan base64 dengan php dapat dilihat pada Kode Program 2.

Kode Program 2. *Encode php* base64

```
1.  class Base64
2.  public function toString($str) {
3.  $str = strtoupper($str);
4.  if ($this->_charset == self::csSafe) {
5.  $str = str_replace('O','0',$str);
6.  $str = str_replace(array('I','L'),'1',$str);}
7.  return $this->bin2str($this->tobin($str));
8.  }
9.  public function toBin($str) {
10. if (!preg_match('/^['.$this->_charset.']+$/', $str))
11. throw new Exception('Must match character set');
12. $str = join('',array_map(array($this, '_mapbin'),
    str_split($str)));
```

```
13. $str = preg_replace('/000(.{5})/', '$1', $str);
14. $length = strlen($str);
15. $rbits = $length & 7;
16. if ($rbits > 0)
17. $str = substr($str, 0, $length - $rbits);
18. return $str;
19. }
20. public function bin2str($str) {
21. if (strlen($str) % 8 > 0)
22. throw new Exception('Length must be divisible by 8');
23. if (!preg_match('/^[01]+$/', $str))
24. throw new Exception('Only 0\'s and 1\'s are permitted');
25. preg_match_all('/.{8}/', $str, $chrs);
26. $chrs = array_map('bindec', $chrs[0]);
27. array_unshift($chrs, 'C*');
28. return call_user_func_array('pack', $chrs);
29. }
```

Berikut ini adalah penjelasan Kode Program 2, baris 1 penamaan *class*, baris 2 penamaan fungsi. Baris 3 membuat *input* menjadi *capital.* Baris 4 - 8 proses menghasilkan hasil *encode.* Baris 9 penamaan fungsi untuk mengubah *string* menjadi *binary string.* Baris 10-19 proses mengubah inputan *string* menjadi *binary* string. Baris 20 penamaan fungsi untuk mengubah *binary string* menjadi string. Baris 21-29 proses encode *binary string* dan mengubahnya ke dalam *string* (*chippertext*).

5. Uji Sistem

Berdasarkan hasil dari uji validasi yang dilakukan pada bagian registrasi, *login*, pembelian, *checkout* pembelian, email konfirmasi, tagihan dan konfirmasi pembayaran didapat kesimpulan bahwa sistem dapat berjalan dengan baik. Hasil uji validasi dapat dilihat pada Tabel 2.

Tabel 2. Uji Validasi

No	Aktivitas dan *Event*	*Input*	*Output*	Status Pengujian
1.	Registrasi Pelanggan	Data Pelanggan	Berhasil melakukan registrasi dan mendapat email verifikasi	Valid
2.	*Login*	Data *Username* dan *Password*	Berhasil melakukan *login* dengan akun yang telah di verifikasi	Valid
3.	Pembelian Produk	Data pembelian	Berhasil melakukan pembelian dan masuk ke dalam proses *checkout*	Valid

4.	Checkout Pembelian	Klik Checkout	Berhasil melakukan checkout dan mendapat email verifikasi	Valid
5.	Terima email konfirmasi pada email pelanggan	*Login* email pelanggan	Email kofirmasi	Valid
6.	Melihat tagihan	Verifikasi email	Tagihan berhasil ditampilkan	Valid
7.	Isi *form* pembayaran	Data pembayaran	Berhasil mengirim data konfirmasi pembayaran ke *server* untuk di verifikasi admin	Valid

Dari hasil pengujian tabel 2 dapat disimpulkan bahwa *e-commerce* pada *web* iKlaster dapat berjalan dengan baik. Mulai dari proses registrasi sampai dengan proses konfirmasi pembayaran. Untuk pengujian keamanan enkripsi data transaksi bisnis dilakukan dengan menggunakan Wireshark, dimana hasil *coding* sudah ter-*encode* dan sudah tidak terbaca.

6. Simpulan

Berdasarkan hasil penerapan Sistem Keamanan Transaksi Bisnis Menggunakan base64 dan *Verification Code* Pada Sistem Jejaring Klaster, maka dapat diperoleh kesimpulan bahwa sistem keamanan data diperoleh dua rancangan desain proses keamanan menggunakan base64 yaitu pada proses *login* dan transaksi pembelian. Sedangkan *verification code* dirancang pada transaksi pembelian dengan tujuan sebagai autentikasi formal untuk transaksi pembelian oleh pelanggan. Penerapan pengamanan base64 dengan menggunakan *library* nibbler.js dan *verification code* menggunakan *link update* status *code* pada *database server*.

7. Daftar Pustaka

[1] Suharto H., Suprihadi, 2012, *Perancangan dan Implementasi Sistem Jejaring Klaster Berbasis Web Menggunakan Metode Model View Controller*, Salatiga: FTI – UKSW,

[2] Jogiyanto, 2003, *Pengertian Sistem Informasi*, Yogyakarta : Skripta Media,

[3] Akbar, 2002, *Diktat Kuliah Keamanan Komputer*, http://www.akbar.staff.gunadarma.ac.id/, Diakses tanggal 21 Februari 2013,

[4] Porter, M.E., 1998, *On Competition.* Boston: Havard Business School Publishing,
[5] Pressman, 2001, *Software Enginering: A Practicioner's Approach 5th Edition*, America : Mc. Graw Hill,
[6] S. Josefsson, 2006, *The Base16, Base32, and Base64 Data Encodings*, http://tools.ietf.org/pdf/rfc4648.pdf, Diakses tanggal 21 Februari 2013,