IMPLEMENTASI AES-256 UNTUK MENGAMANKAN DATABASE *E-COMMERCE*

Nuraini, Safrina Amini
Program Studi Teknik Informatika,Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : raini.ai@gmail.com, safrina.amini@budiluhur.ac.id

Abstrak

Kebutuhan sistem berbasis online terus mengalami peningkatan.Hal tersebut dikarenakan kebutuhan pengguna yang ingin selalu terhubung dengan data atau informasi secara fleksibel tanpa batasan tempat dan waktu.Dalam dunia usaha, sistem berbasis online dimanfaatkan untuk dapat menjual produk atau jasa dan melakukan kegiatan promosi produk dalam bentuk E-Commerce atau biasa disebut toko online.Dengan banyak keuntungan sistem berbasis online, perlu diperhatikan resiko ancaman pencurian data yang dapat merugikan pemilik usaha maupun pelanggan.Oleh karena resiko keamanan tersebut dan meningkatkan rasa nyaman bagi pelanggan atau pengguna sistem, maka perlu dilakukan tindakan-tindakan pencegahan untuk mengamankan database sistem.Tindakan tersebut dengan melakukan teknik enkripsi menggunakan metode Advanced Encryption Standart (AES) 256. Enkripsi akan dilakukan pada alamat URL yang digunakan untuk mengakses database.

Kata Kunci :*E-Commerce*, Enkripsi, Dekripsi, Kriptografi, Algoritma, AES-256

1. PENDAHULUAN

Kebutuhan sistem berbasis online terus mengalami peningkatan.Dalam dunia usaha, sistem berbasis online dimanfaatkan untuk dapat menjual produk atau jasa dan melakukan kegiatan promosi produk dalam bentuk *E-Commerce* atau biasa disebut toko online.

Yang menjadi permasalahan saat ini dari banyak keuntungan sistem berbasis online, perlu diperhatikan resiko ancaman pencurian data. Ancaman yang menjadi resiko pada sistem online, salah satunya adalah *SQL Injection.SQL (Structure Query Language) Injection* merupakan jenis ancaman yang menggunakan kode *querySQL*, untuk dapat mengakses isi database sistem, sehingga dapat dilakukan pencarian data atau perusakan data.Sistem *E-Commerce* yang tidak aman, mengakibatkan pelanggan tidak nyaman untuk melakukan transaksi, sehingga pelanggan tidak mau menggunakan sistem tersebut.

Oleh karena resiko keamanan tersebut, maka perlu dilakukan tindakan-tindakan pencegahan untuk mengamankan database sistem.Tindakan tersebut dengan melakukan teknik enkripsi menggunakan metode *Advanced Encryption Standart (AES) 256.*

2. LANDASAN TEORI

2.1. Sistem

Referensi [1] menunjukan bahwa sistem merupakan suatu kumpulan dari unsur, variable-variabel yang terorganisasi, saling berinteraksi, saling memerlukan satu sama lain dan terpadu.

2.2. Kemanan Data

Tujuan utama dari keamanan data adalah memastikan serta melindungi data baik milik pribadi maupun perusahaan. Keamanan data tidak hanya bergantung pada teknologi saja, tetapi dari aspek prosedur dan kebijakan keamanan yang telah diterapkan serta kedisiplinan Sumber Daya Manusia (SDM), bila panduan keamanan tidak diikuti maka data ataupun informasi sensitif yang tersimpan akan sangat beresiko untuk diakses oleh pihak yang tidak berwenang [2].

Berikut beberapa aspek Keamanan komputer yaitu:

a. ***Authentication*** **:**yaitu penerima informasi dapat memastikan bahwa pesan tersebut datang dari orang yang dimintai informasi.
b. ***Integrity*** **:**Memastikan bahwa informasi yang dikirim tidak diubah(modifikasi) oleh orang yang tidak berkepentingan dalam proses pengiriman informasi tersebut.
c. ***Nonrepudiation*** **:**Berhubungan dengan pengirim, yang mengirim informasi tersebut. Pengirim tidak dapat mengelak bahwa dia adalah si pengirim pesan.
d. ***Authority*** **:** informasi yang terdapat pada sistem jaringan tidak mudah diubah atau dimodifikasi oleh pihak yang tidak memiliki hak atas akses tersebut.
e. ***Confidentiality*** **:**Usaha yang dilakukan untuk menjaga informasi dari orang yang tidak memiliki hak untuk mengakses.
f. ***Privacy*** **:**Ke arah data-data atau infrmasi yang sifatnya pribadi.
g. ***Availability*** **:** aspek availability atau ketersediaan, ketersediaan yang dimaksud adalah tentang ketersediaan informasi saat

sedang dibutuhkan. Sistem informasi yang dihack dapat menghambat atau meniadakan akses ke informasi.

2.3. *E-Commerce*

E-Commerce adalah suatu proses jual beli produk-produk secara elektronik oleh konsumen dan/atau dari perusahaan ke perusahaan dengan komputer sebagai perantara transaksi bisnis.

2.4. Kriptografi

Kriptografi adalah ilmu pengetahuan dan seni menjaga pesan *agar* tetap aman. Kriptografi merupakan cabang dari ilmu matematika yang memiliki banyak fungsi dalam pengamanan data. Kriptografi ialah proses mengambil pesan(*message)*dan menggunakan beberapa fungsi untuk menggenerasi materi kriptografis (sebuah *digest* atau *message* terenkripsi) [3].

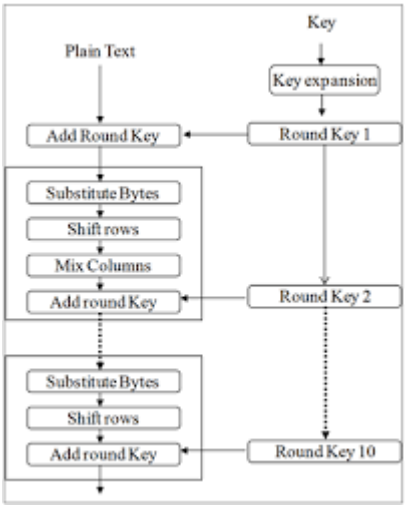
Terdapat empat tujuan dasar dari ilmu kriptografi yaitu :

a. Kerahasiaan (*Confidentiality*).
b. Integritas data (*Data Integrity*).
c. Otentikasi (*Authentication*).
d. Nirpenyangkalan (*non-repudiation*).

2.5. *Advance Encryption Standart (AES)*

Pengelompokkan jenis AES yaitu berdasarkan panjang kunci yang digunakan. Angka-angka yang berada di belakang kata AES menerangkan panjang kunci yang digunakan pada tipa-tiap AES. Selain itu, hal yang membedakan dari masing-masing AES ini adalah banyaknya round yang dipakai. AES-128 menggunakan 10 round, AES-192 sebanyak 12 round, dan AES-256 sebanyak 14 round.

AES mempunyai ukuran blok yang tetap yaitudengan panjang 128 bit dengan ukuran panjang kunci 128, 192, atau 256 bit. Berbeda dengan Rijndael yang blok dan kuncinya dapat berukuran kelipatan 32 bit dengan ukuran minimumnya 128 bit dan maksimumnya 256 bit. Dengan ukuran blok yang tidak berubah, AES bekerja pada matriks dengan ukuran 4x4 di mana setiap sel matriks terdiri dari 1 byte (8 bit). Sedangkan Rijndael bekerja pada matriks denganukuran yang lebih dari itu hanya dengancara memberi tambahan kolom sebanyak yang diperlukan. Blok *chiper*di sini dapat diasumsikan sebagai sebuah kotak. Setiap plainteks sebelumnyaakan dikonversikan ke dalam blok-blok tersebut dalam bentuk heksadesimal. Metode pemrosesan AES secara umum dapat dilihat pada gambar berikut.

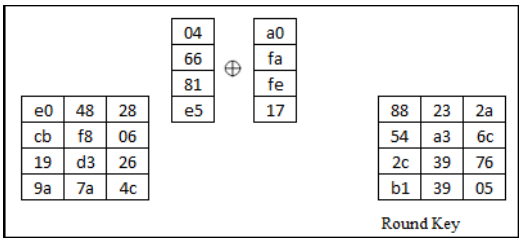


Gambar 1: Diagram AES

Berikut keterangan dari Gambar 1:Diagram AES :

a. *Add Round Key*

Add Round Key merupakan kombinasi *chiper* teks yang sudah ada dengan *chiper key* yang *chiper key* dengan hubungan XOR. Bagannya dapat dilihat pada gambar di bawah ini.



Gambar 2: Add Round Key

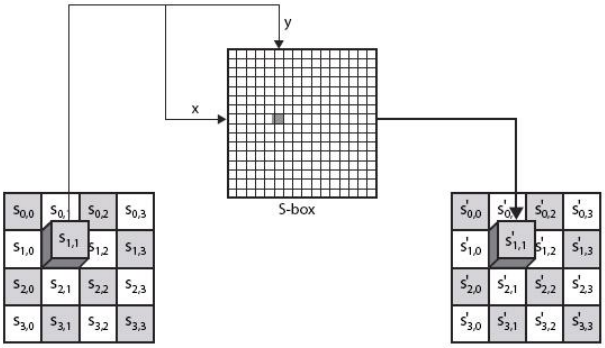
Pada gambar tersebut table yang di kiri merupakan chiper teks dan table yang sebelah kanan merupakan *round key*. Proses XOR dilakukan pada tiap kolom yaitu *chipper* teks pada kolom-1 di XOR dengan round key pada kolom-1 dan seterusnya.

b. *Sub bytes*

Proses Sub Bytes adalah menukar isi matriks/tabel yang ada dengan matriks/tabel lain yang disebut dengan Rijndael S-Box. Berikut adalah contoh *Sub Bytes* dan Rijndael S-Box.

Table 1: Sub Bytes

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

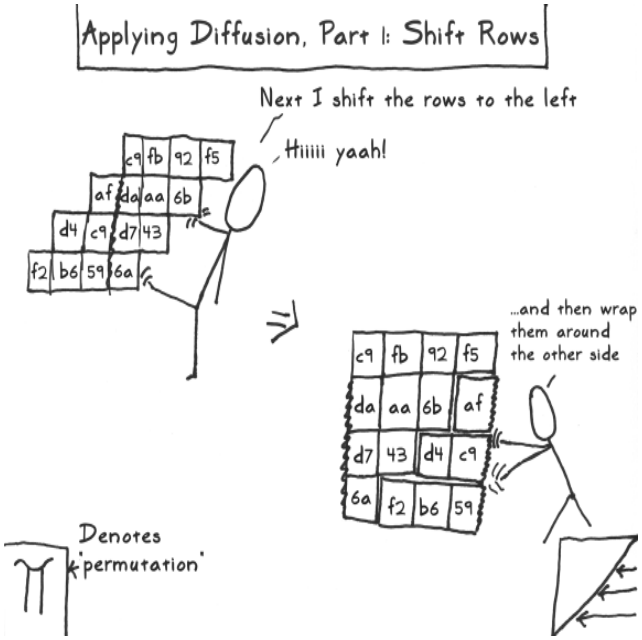


Gambar 3: Illustrasi Sub Bytes

Gambar 3 merupakan Rijndael S-Box, dimana ada nomor kolom dan nomor baris.Setiap isi kotak dari blok*chiper* berisi informasi dalam bentuk heksadesimal yang terdiri dari dua digit, seperti yang telah disebutkan sebelumnya.Langkahnya ialah dengan mengambil salah satu isi kotak matriks,dan melakukan pencocokan dengan digit yang ada di sebelah kiri sebagai baris dan digit yang ada di sebelah kanan sebagai kolom. Dengan mengetahui kolom dan baris, dapat diambil sebuah isi tabel pada Rijndael S-Box. Langkah terakhir ialah mengubah keseluruhan blok*chiper* menjadi blok yang baru yang isinya merupakan hasil penukaran semua isi blok dengan isi langkah yang telah disebutkan tadi.

c. *Shift Rows*

Shift Rows ialah proses pergeseran(shift) pada setiap variable blok/tabel yang dilakukan pada setiap barisnya. Tidak dilakukan pergeseran pada baris pertama, dilakukan pergeseran 1 byte pada baris kedua , dan seterusnya sampai baris keempat. Pergeserannya terlihat dalam sebuah blokialah sebuah pergeseran setiap elemen ke kiri tergantung berapa byte pergesernya, tiap pergeseran 1 byte berarti bergeser ke kiri sebanyak satu kali. Ilustrasi dari tahap ini dapat dilihat pada gambar di bawah ini.



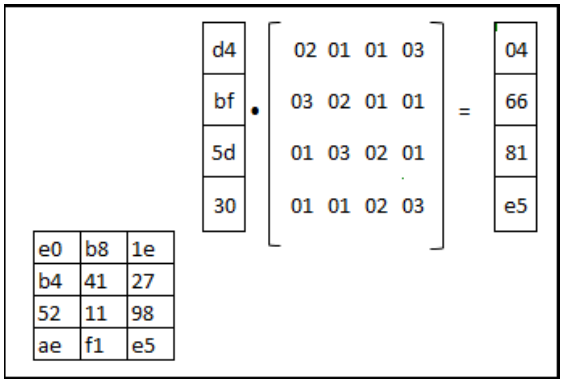
Gambar 4: Shift Rows

d. *Mixt column*

Langkah akhir adalah Mix Column. Proses*Mix Column*yaitu mengalikan setiap elemen dari blok*chiper* dengan matriks yang dapat dilihatpada Gambar 4. Ilustrasi pada gambar 5 akan menjelaskan bagaimanacara perkaliannya. Demikian penjelasan seluruh rangkaian proses yang terjadi pada sistem AES.

Table 2: Mixt Column

0	2	0	1	0	1	0	3
0	3	0	2	0	1	0	1
0	1	0	3	0	2	0	1
0	1	0	1	0	2	0	3

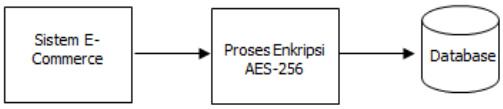


Gambar 5: Mixt Column

3. RANCANGAN SISTEM DAN APLIKASI

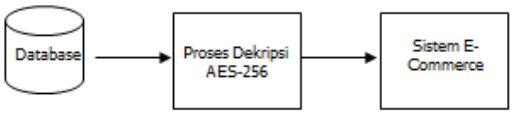
Pada pengembangan keamanan database sistem web *E-Commerce* terdiri dari 2 proses yaitu enkripsi dan dekripsi. Proses enkripsi menjalankan

algortima AES untuk mengaburkan informasi dari setiap data yang dimasukkan pengguna pada sistem web *E-Commerce*pada saat masuk ke database. Sedangkan proses dekripsi mengembalikan isi dari informasi kebentuk semula pada saat masuk ke system web *E-Commerce*. Berikut ini arsitektur kerja sistem diterapkan pada sistem.



Gambar 8: Arsitektur Kerja Sistem Enkripsi

Informasi yang dimasukkan dan disimpan melaui sistem *E-Commerce* akan dilakukan proses enkripsi terlebih dahulu sebelum masuk ke sistem database.

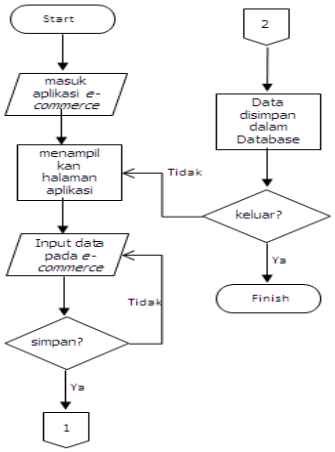


Gambar 9: Arsitektur Kerja Sistem Dekripsi

Sebelum menampilkan isi yang akan dilihat oleh pengguna di dalam sistem *E-Commerce*, terlebih dahulu sistem akan melakukan proses dekripsi dari data yang diambil dalam sistem database.

3.1 *Flowchart* Proses Enkripsi Pada *E-Commerce*

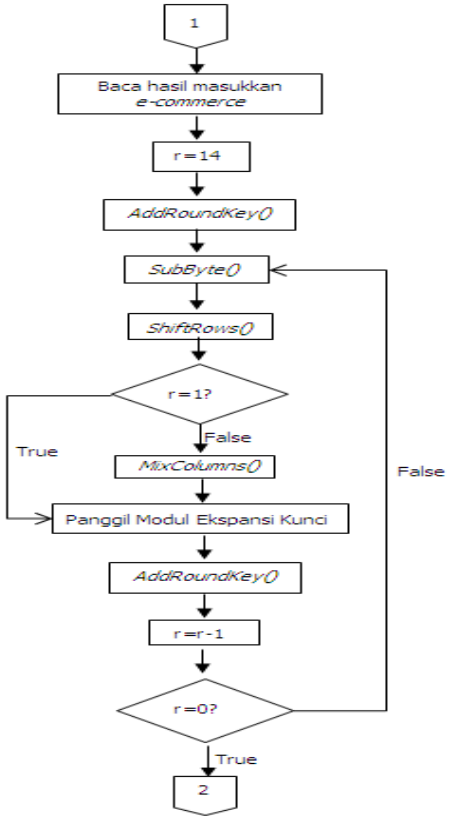
Flowchart dibawah ini menggambarkan alur proses enkripsi pada sistem *E-Commerce*, proses enkripsi akan berjalan otomatis ketika pengguna menyimpan data saat melakukan transaksi pada sistem *E-Commerce*.



Gambar 10:Proses Enkripsi Pada Sistem E-Commerce

3.2 Flowchart Proses Enkripsi AES-256

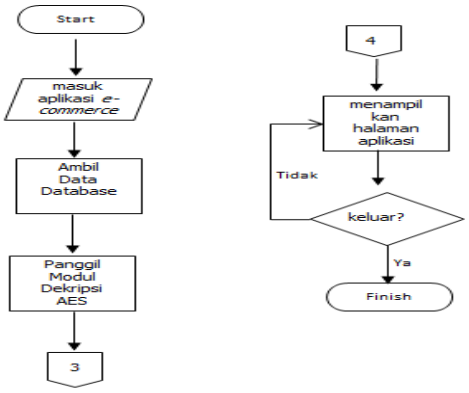
Setelah data masukkan di sistem *E-Commerce* disimpan, sebelumnya program akan memanggil modul enkripsi AES-256 untuk mengubah tampilan isi dari data tersebut, agar tidak dapat dibaca oleh mata manusia. Setelah itu, baru kemudian data tersebut disimpan di dalam database. Berikut flowchart pada proses Enkripsi AES-256.



Gambar 11:Detail Proses Enkripsi AES

3.3 Flowchart Proses Dekripsi pada Sistem

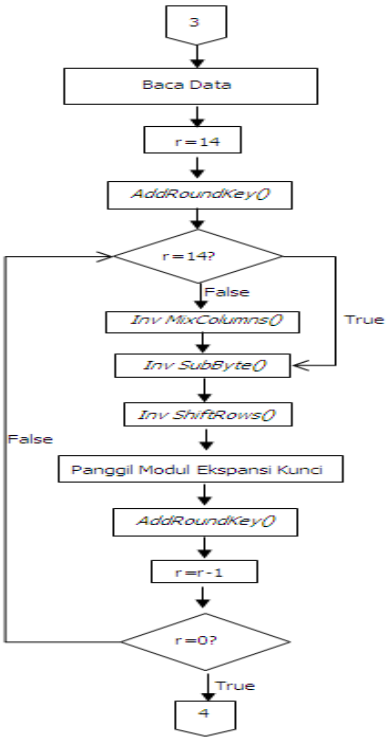
Sedangkan proses dekripsi dimulai dengan masuk aplikasi *e-commerce* membaca data pada table databsse yang akan didekripsi. Kemudian proses dekripsi berjalan secara otomatisdengan memanggil modul dekripsi *AdvanceEncryption Standard*. Setelah proses dekripsi selesai, system akan menampilkan data yang dapat dibaca kembali oleh mata manusia atau yang disebut dengan *plaintext* melalui sistem *E-Commerce*.



*Gambar 12:*Proses Dekripsi Pada Sistem *E-Commerce*

3.4 Flowchart Proses Dekripsi AES

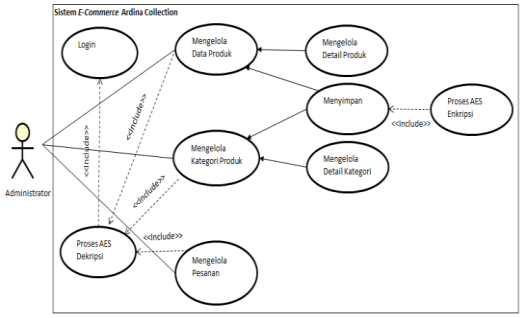
Secara detail proses modul dekripsi AES dapat dilihat pada diagram alur dibawah ini.



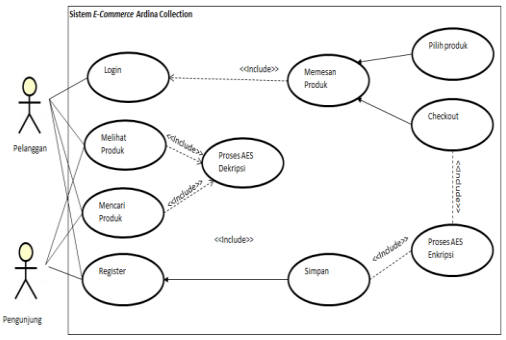
Gambar 13 : Detail Proses Dekripsi AES

3.5 Use Case Diagram

Use Case Diagram adalah gambaran relasi antara aktor dengan aktivitas yang dilakukannya dalam bentuk *case*.*Use case diagram* sistem ini terbagi menjadi dua, yaitu *use case diagram* untuk aktor Administrator, serta *use case diagram* untuk aktor Pelanggan dan Pengunjung, berikut tampilan use case yang telah ditambahkan program enkripsi dan dekripsi.



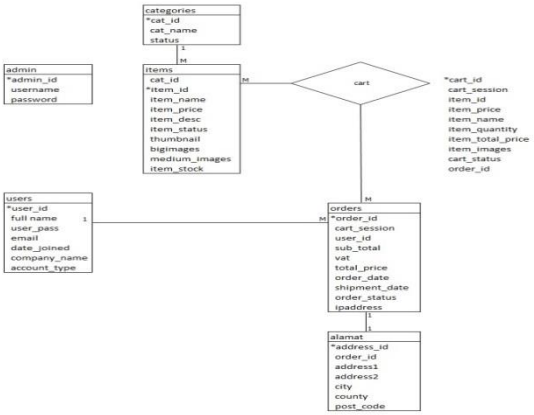
Gambar 14 : Use Case Diagram Administrator



Gambar 15: Use Case Diagram Pelanggan dan Pengunjung

3.6 ERD (*Entity Relationship Diagram*)

ERD merupakan suatu model yang menjelaskan hubungan antar data pada basis data didalam basis data berdasarkan objek-objek dasar data yang mempunyai hubungan antar relasi.Berikut tampilan ERD pada aplikasi *e-commerce.*



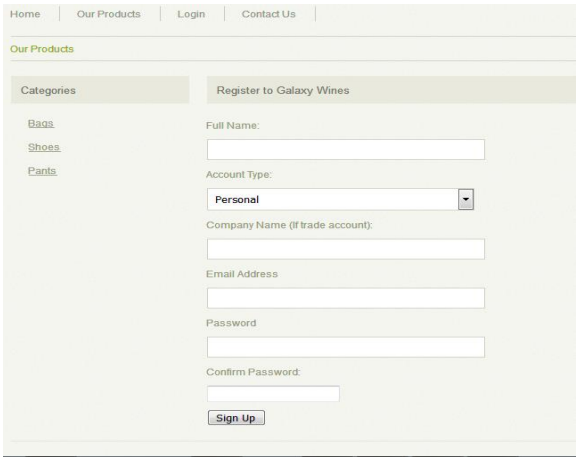
Gambar 16: ERD Sistem E-Commerce

4. HASIL DAN PEMBAHASAN

Pengujian terhadap perangkat lunak ini dilakukan untuk mengetahui apakah hasil perangkat lunak telah berjalan sesuai dengan rancangan atau tidak.Berikut merupakan hasil dari sistem yang telah dibuat.

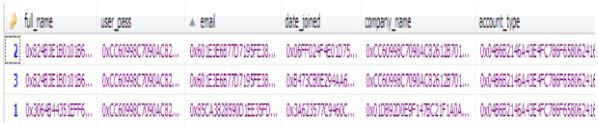
4.1 Hasil Enkripsi Pada Halaman Register Pelanggan Baru

Halaman Register Pelanggan Baru berfungsi untuk menampung data pelanggan seperti Nama, Alamat Email (sebagai *username*), dan Password. Pada halaman ini pengguna dapat menjadi pelanggan dengan cara melengkapi form yang tersedia. Bila pengguna sudah menjadi pelanggan, mereka dapat memesan produk yang diinginkan. Berikut tampilan halaman Register Pelanggan Baru.



Gambar 18 : Halaman Register Pelanggan Baru

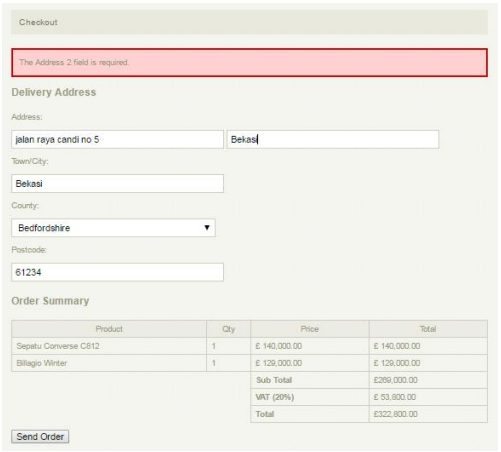
Berikut merupakan tampilan database setelah dienkripsi pada menu Register pelanggan Baru.



Gambar 19 : Tampilan Database setelah di Enkrip

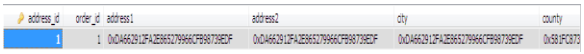
4.2 Hasil Enkripsi Pada Halaman *Checkout*

Halaman ini berfungsi untuk menginputkan alamat pengiriman dan mengkonfirmasi order yang dilakukan oleh pelanggan. Berikut ini tampilan dari halaman *checkout.*



Gambar 20 :Halaman Checkout

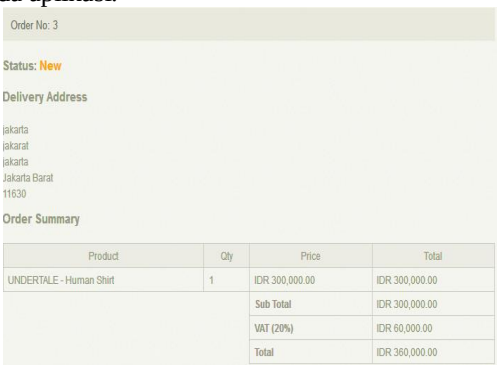
Proses terakhir dari proses pemesanan adalah memasukkan data alamat pengiriman. Sebelum data alamat masuk kedalam database, data tersebut dienkrip secara otomatis oleh system, agar data alamat aman dan tidak disalah gunakan oleh orang yang tidak bertanggung jawab.Berikut tampilan database alamat pengiriman.



Gambar 21 : Tampilan Enkripsi Database Alamat Pengiriman

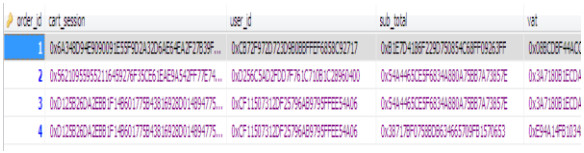
4.3 Hasil Enkripsi Data Order

Sesuai dengan tujuan penelitian ini, agar data order lebih aman dan tidak diketahui oleh orang yang tidak berkepentingan, maka dilakukan proses enkripsi pada data order. Berikut ini hasil data order pada aplikasi.



Gambar 22 :Halaman Data Order pada Aplikasi

Setelah melalui proses enkripsi, maka data order tidak dapat dibaca dengan mudah. Hasil proses enkripsi data order adalah sebagai berikut.



Gambar 23: Halaman Enkripsi Database Pada Menu Data Order

5. KESIMPULAN

Berdasarkan analisa yang telah dilakukan mulai dari mengumpulan informasi, pemecahan masalah hingga pengembangan aplikasi, maka dapat diambil kesimpulan dan juga terdapat beberapa saran yang perlu diperhatikan demi kelancaran aplikasi yang dibangun ini.

5.1 Kesimpulan

Dari hasil analisa permasalahan dan cara penyelesaiannya, dapatdisimpulkan bahwa mengimplementasikan algoritma AES-256 dapat mengamankan database *E-Commerce*, sehingga database terjaga keamanan dan keasliannya.

5.2 Saran

Beberapa saran untuk pengembangan tugas akhir ini :

a. Pengembangan selanjutnya agar dapat mengenkripsi gambar.
b. Pada pengembangan selanjutnya dapat ditambahkan metode enkripsi lainnya.

6. DAFTAR PUSTAKA

[1] Sutabari, Tata, 2004,Analisa Sistem Informasi, Yogyakarta, Andi.

[2] Komputer, Wahana, 2010,*The Best Encryption Tools*, Jakarta, PT Elex Media Komputindo.

[3] Schneier, Bruce, 1996, *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*, Wiley Computer Publishing, Jhon Wiley & Sons, inc.