IMPLEMENTASI ALGORITMA AES-128 DAN *QR CODE* UNTUK VALIDASI TIKET PADA PERUSAHAAN TRAVEL PT. BUMINDO JAYA CEMERLANG SKRIPSI

Oleh

Hamdan Hidayatulloh

NIM 102410101119

PROGRAM STUDI SISTEM INFORMASI

UNIVERSITAS JEMBER

2017

IMPLEMENTASI ALGORITMA AES-128 DAN *QR CODE* UNTUK VALIDASI TIKET PADA PERUSAHAAN TRAVEL PT. BUMINDO JAYA CEMERLANG

SKRIPSI

diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat untuk menyelesaikan pendidikan di Program Studi Sistem Informasi Universitas Jember dan mendapat gelar Sarjana Sistem Informasi

Oleh

Hamdan Hidayatulloh

NIM 102410101119

PROGRAM STUDI SISTEM INFORMASI

UNIVERSITAS JEMBER

2017

PERSEMBAHAN

Skripsi ini saya persembahkan untuk :

1. Allah SWT yang selalu memberikan rahmat serta hidayahNya dalam kelancaran dan kemudahan penulisan skripsi;
2. Kedua orang tua saya, Bapak Tajudin Ali dan Ibu Habibah Qomar yang telah memberikan kasih sayang serta dukungan;
3. Kepada kakak-kakak saya, Mbak Heni, Mas Tiar, Mbak Lia yang selalu memberikan dukungan dan do'a terbaik;
4. Segenap keluarga besar saya;

MOTTO

"Hadapi masalah hidup dengan sabar dan ikhlas"

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Hamdan Hidayatulloh

NIM : 102410101119

menyatakan dengan sesungguhnya bahwa karya ilmiah yang berjudul "Implementasi Algoritma *AES*-128 dan *QR Code* untuk Validasi Tiket pada Perusahaan Pt. Bumindo Jaya Cemerlang", adalah benar-benar hasil karya sendiri, kecuali jika dalam pengutipan substansi disebutkan sumbernya, belum pernah diajukan pada institusi mana pun, dan bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa ada tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika di kemudian hari pernyataan ini tidak benar.

Jember, 28 April 2017

Yang menyatakan,

Hamdan Hidayatulloh

NIM 102410101119

SKRIPSI

IMPLEMENTASI ALGORITMA AES-128 DAN *QR CODE* UNTUK VALIDASI TIKET PADA PERUSAHAAN TRAVEL PT. BUMINDO JAYA CEMERLANG

Oleh

Hamdan Hidayatulloh

NIM 102410101119

Pembimbing :

Dosen Pembimbing Utama : Dr. Saiful Bukhori, ST., M.Kom.

Dosen Pembimbing Pendamping : Yanuar Nurdiansyah, ST., M.Cs

RINGKASAN

Implementasi *AES*-128 dan *QR Code* untuk Validasi Tiket pada Perusahaan Travel Pt. Bumindo Jaya Cemerlang; Hamdan Hidayatulloh, 102410101119; 2017; 150 halaman; Program Studi Sistem Informasi Universitas Jember.

Perusahaan jasa travel yang memanfaatkan media internet untuk pengembangan perusahaan jasa, contohnya adalah pemesanan tiket perjalanan menggunakan internet atau secara *online*. Penggunaan media internet digunakan karena proses untuk melihat dan mengirim data dan informasi tanpa bertemu satu sama lain, dengan kata lain mempermudah alur transaksi dengan konsumen. Efek negatif dari penggunaan media internet untuk kegiatan seperti ini, keamanan dan kerahasiaan data yang disampaikan melalui media internet sangatlah rawan terhadap pencurian data oleh pihak yang tidak berkepentingan.

Berdasarkan permasalahan diatas, maka diperlukan cara atau metode untuk menjaga keamanan dan kerahasiaan data tersebut. Disamping itu diperlukan sistem yang mampu mengelola keseluruhan data yang ada di perusahan Pt. Bumindo Jaya Cemerlang. Sehingga Pt. Bumindo Jaya Cemerlang mampu menjaga keamanan data dan mampu mengelola data yang bersangkutan dengan konsumen

Pada penelitian ini dibangun sistem informasi yang mampu mengamankan data dari perusahaan dan konsumen. Proses keamanan menggunakan metode kriptografi dan *QR Code*. Penelitian ini menggunakan beberapa kunci sama yang digunakan untuk proses enkripsi dan dekripsi. Data yang disimpan juga diubah menjadi bentuk *QR Code,* sehingga keamanan data bisa terjamin.

PRAKATA

Puji syukur kehadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul Implementasi Algoritma *AES*-128 dan *QR Code* untuk Validasi Tiket pada Perusahaan Pt. Bumindo Jaya Cemerlang. Skripsi ini disusun untuk memenuhi salah satu syarat menyelesaikan pendidikan Strata Satu (S1) pada Program Studi Sistem Informasi Universitas Jember.

Penyusunan skripsi ini tidak lepas dari bantuan berbagai pihak. Oleh karena itu, penulis menyampaikan terima kasih kepada:

1. Prof. Drs. Slamin, M.Comp.Sc., Ph.D., selaku Ketua Program Studi Sistem Informasi Universitas Jember;
2. Dr. Saiful Bukhori, S.T., M.Kom selaku Dosen Pembimbing Utama dan Yanuar Nurdiansyah, ST., M.Cs selaku Dosen Pembimbing Anggota yang telah meluangkan waktu, pikiran dan perhatian dalam penulisan skripsi;
3. Seluruh dosen dan staf tata usaha Program Studi Sistem Informasi;
4. Kedua orang tua saya Bapak Tajudin Ali dan Ibu Habibah Qomar yang selalu mendukung dan mendoakan;
5. Kakak – kakakku mbak Heni, mas Tiar, mbak Lia yang selalu memberi dukungan;
6. Keluarga besar Mapala Balwana yang menjadi rumah kedua;
7. Keluarga besar UKLAM yang telah banyak membantu;
8. Keluarga bapak Budiarto yang telah menjadi rumah kostan terbaik;
9. Adik – adikku di keluarga balwana pari, penjes, alis, ganja, bohay, colan, bendot, karak, engkol, busi, rambu, landep, bakar, klakson, odeng, kowar, gertak, cekar, gulay, ganes, abang, cantigi, langit, tsunami, geni, longsor, centang, cepeng;
10. Khasanul Alfiani yang selalu mendukung dan menemani skripsi;
11. Semua pihak yang tidak dapat disebutkan satu persatu.

Penulis menyadari bahwa laporan ini masih jauh dari sempurna, oleh sebab itu penulis mengharapkan adanya masukan yang bersifat membangun dari semua pihak. Penulis berharap skripsi ini dapat bermanfaat bagi semua pihak.

Jember, 28 April 2017

Penulis

DAFTAR ISI

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

No table of figures entries found.

BAB 1. PENDAHULUAN

Bab ini merupakan langkah awal dari penulisan tugas akhir ini. Bab ini berisi latar belakang, perumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian dan sistematika penulisan.

1.1 Latar Belakang

Semakin banyak perusahaan jasa travel yang memanfaatkan media internet untuk pengembangan perusahaan jasa, contohnya adalah pemesanan tiket perjalanan menggunakan internet atau secara *online*. Penggunaan media internet digunakan karena proses untuk melihat dan mengirim data dan informasi tanpa bertemu satu sama lain, dengan kata lain mempermudah alur transaksi dengan konsumen. Efek negatif dari penggunaan media internet untuk kegiatan seperti ini, keamanan dan kerahasiaan data yang disampaikan melalui media internet sangatlah rawan terhadap pencurian data oleh pihak yang tidak berkepentingan. Ada bermacam-macam cara atau metode untuk menjaga keamanan dan kerahasiaan data tersebut, cara atau metode yang paling sering digunakan adalah kriptografi dan *QR Code*.

Metode kriptografi adalah metode yang bertujuan untuk menjaga agar data atau informasi tetap aman saat dikirimkan. *Cryptography* adalah seni dan ilmu pengetahuan untuk menjaga pesan tetap aman (Scheiner, 1996). Menggunakan metode kriptografi data tidak dapat dibaca atau dimengerti oleh pihak-pihak yang tidak berwenang terhadap data tersebut, sehingga keamanan data tersebut akan terjamin. Terdapat dua proses dasar dalam pengamanan data menggunakan metode kriptografi, yaitu proses enkripsi dan dekripsi. Enkripsi adalah sebuah proses untuk menjadikan data yang bisa dibaca menjadi bentuk yang tidak bisa dibaca atau dimengerti melalui proses perhitungan yang rumit. Dekripsi adalah proses yang diperlukan untuk dapat membaca kembali data atau mengembalikan data kembali ke bentuk semula yang telah dienkripsi.

Terdapat banyak algoritma kriptografi yang digunakan untuk mengamankan data, salah satunya adalah algoritma *Advanced Encryption Standard* (AES). Algoritma AES merupakan algoritma simetris yaitu menggunakan kunci yang

sama untuk proses enkripsi dan dekripsi. Pada penelitian yang telah dilakukan oleh (Nurdiansyah, Istiyadi, & I, 2014), algoritma AES dipilih karena memiliki tingkat keamanan yang tinggi dengan tiga pilihan tipe kunci yaitu AES-128, AES-192 dan AES-256. Algoritma AES yang digunakan dalam penelitiannya adalah algoritma AES-128 untuk menyandikan *filedigital*. Informasi yang terkandung dalam *file* tersebut menjadi lebih aman setelah diubah ke dalam bentuk data tersandi karena informasi hanya dapat dibaca oleh pihak yang berhak.

QR Code adalah suatu jenis kode matrik yang dikembangkan oleh perusahaan Jepang dan sudah sangat lazim digunakan di negara tersebut, tujuan utama dari *QR Code* ini adalah untuk menyampaikan informasi dengan cepat dan mendapatkan respon yang cepat pula. *QR (Quick Response) Code* adalah image matriks dua dimensi yang merepresentasikan suatu data, terutama data berbentuk teks (Pasca Nugraha & Munir, 2011). *QR Code* merupakan evolusi dari *barcode* yang awalnya satu dimensi menjadi dua dimensi. Kemampuan untuk menyimpan data di dalamnya. *QR Code* merupakan tingkatan yang lebih tinggi bila dibandingkan *barcode* dalam hal kapasitas penyimpanan data, *QR Code* merupakan evolusi dari kode batang (*barcode*) (Rahayu, Nana Ramadijanti, & Yuliana Setiowati, 2010). *Barcode* merupakan sebuah simbol penandaan objek nyata yang terbuat dari pola batang-batang berwarna hitam dan putih agar mudah untuk dikenali komputer.

Penggunaan *QR Code* telah menjadi kebiasaan oleh masyarakat umum, terutama dalam ponsel pintar (*smartphone*), hal ini dikarenakan setiap *Operating System* memiliki pemindai *QR Code* sendiri. Selain dalam bidang *smartphones*, *QR Codes* juga banyak diterapkan di perusahaan-perusahaan makanan untuk menandai produk yang dihasilkan oleh mereka. Informasi yang disampaikan menjadi lebih banyak daripada menjelaskan secara langsung.

Penelitian ini akan dilakukan implementasi algoritma AES-128 dan *QR Code* pada pemesanan tiket di perusahaan travel Pt. Bumindo Jaya Cemerlang berbasis android. Penggunaan algoritma tersebut akan diimplementasikan pada data pengguna aplikasi ini, antara lain data member, data transaksi, data kota, data jadwal, data user dan lain sebagainya, sedangkan pengaplikasian *QR Code*

diimplementasikan pada aplikasi android. Diharapkan pengimplementasian algoritma AES-128 dan *QR Code* dapat melindungi keaslian tiket travel tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, ditemukan beberapa permasalahan sebagai berikut:

a. Bagaimana membuat aplikasi *QR Code Reader* berbasis android yang menjaga keamanan data terjaga atau keaslian dari tiket.
b. Bagaimana pemanfaatan algoritma AES-128 untuk keamanan data pada aplikasi travel Pt. Bumindo Jaya Cemerlang.

1.3 Tujuan dan Manfaat

Tujuan dan manfaat berisi tentang tujuan dari penelitian pengimplementasian algoritma AES-128 dan *QR Code* untuk keamanan atau keaslian data tiket travel Pt. Bumindo Jaya Cemerlang. Sedangkan pada bagian manfaat berisi tentang manfaat apa yang akan diperoleh pada penelitian ini, baik bagi peneliti sendiri maupun bagi objek pada penelitian ini.

1.3.1 Tujuan

Tujuan dari penelitian ini adalah:

a. Membuat aplikasi *QR Code reader* berbasis android yang keamanan atau keaslian data tetap terjaga.
b. Mengetahui pemanfaatan algoritma AES-128 untuk keamanan data pada aplikasi Pt. Bumindo Jaya Cemerlang.

1.3.2 Manfaat

Manfaat penelitian ini adalah:

a. Manfaat Akademis

   Hasil penelitian ini diharapkan dapat memberikan kontribusi dan masukan bagi siapa saja yang membutuhkan informasi yang berhubungan dengan judul penelitian ini. Selain itu, hasil penelitian ini merupakan suatu upaya untuk menambah varian judul penelitian yang ada di Program Studi Sistem Informasi Universitas Jember.

b. Manfaat bagi peneliti

1) Mengetahui bagaimana proses penerapan algoritma AES-128 pada aplikasi Pt. Bumindo Jaya Cemerlang.
2) Mengetahui bagaimana proses penerapan *QR Code* berbasis pada aplikasi Pt. Bumindo Jaya Cemerlang.

c. Manfaat bagi objek penelitian
1) Memberikan inovasi baru kepada instansi (Pt. Bumindo Jaya Cemerlang) mengenai penggunaan *QR Code* berbasis android.
2) Membantu instansi untuk mengembangkan sistem pelayanan bagi pelanggan yang mudah diakses dan digunakan kapan saja dan dimana saja.

1.4 Batasan Masalah

Adapun batasan masalah dalam penelitian ini antara lain:

a. Dalam penelitian ini dikhususkan untuk mengetahui implementasi algoritma AES-128 untuk proses enkripsi dan *QR Code* dalam menjaga keaslian data tiket pada Pt. Bumindo Jaya Cemerlang.
b. Aplikasi yang nantinya dibangun merupakan aplikasi berbasisweb.
c. Aplikasi *QR Code reader* yang nantinya dibangun merupakan aplikasi berbasis *android.*
d. Aplikasi yang dibangun hanya menitikberatkan pada pelayanan Pt. Bumindo Jaya Cemerlang.
e. Aplikasi *QR Code reader* yang dibangun hanya menampilkan keaslian tiket travel Pt. Bumindo Jaya Cemerlang.

1.5 Sistematika Penulisan

Sistematika penulisan dalam penyusunan tugas akhir ini adalah sebagai berikut:

a. Pendahuluan

Bab ini terdiri atas latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah dan sistematika penulisan

.

b. Tinjauan Pustaka

Bab ini berisi tentang kajian materi, penelitian terdahulu dan informasi apa saja yang digunakan dalam penelitian ini. Dimulai dari kajian pustaka mengenai pengertian dari keamanan data, algoritma AES-128, dan perlunya menggunakan *QR Code*.

c. Metodologi Penelitian

Bab ini menguraikan tentang metode apa yang dilakukan selama penelitian. Dimulai dari tahap pencarian permasalahan hingga pengujian aplikasi Pt. Bumindo Jaya Cemerlang dan *QR Code reader* yang akan dibuat.

d. Hasil dan Pembahasan

Bab ini menjelaskan tentang hasil dan pembahasan dari penelitian yang telah dilakukan. Dengan menggambarkan dampak apa yang terjadi pada saat sebelum penggunaan sistem dan setelah penggunaan sistem.

e. Penutup

Bab ini berisi kesimpulan dari penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya.

BAB 2. TINJAUAN PUSTAKA

Penelitian pengimplementasian algoritma AES-128 dan *QR Code* untuk validasi tiket pada Pt. Bumindo Jaya Cemerlang, dibutuhkan beberapa landasan teori yang digunakan untuk memperkuat dan mengarahkan penelitian agar tidak keluar dari kaidah keilmuan yang ada.

2.1 Pengertian Keamanan Informasi

Menurut G. J. Simons, "Keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik" (Raharjo, 1999). Lebih lanjut dalam masalah kemanan informasi terdapat beberapa aspek yang dinilai sangat penting untuk menjaga kemanan data dan informasi. Menurut Garfinkel, "kemanan komputer (*computer security*) melingkupi empat aspek, yaitu *privacy*, *integrity*, *authentication,* dan *availability*" (Raharjo, 1999). *Privacy/confidentially* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses, *integrity* aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi, *authentication* aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli , atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan (Raharjo, 1999). Aspek-aspek yang telah disebutkan diatas sangat penting untuk mendukung keamanan data dan informasi.

2.2 Pengertian Kriptografi

Secara etimologi (ilmu asal usul kata) kata kriptografi berasal dari bahasa Yunani, yaitu *kryptos* yang artinya tersembunyi dan *graphein* yang artinya tulisan. Kriptografi sudah digunakan sejak zaman dahulu, hal ini dibuktikan dengan penggunaan *hieroglyph* oleh bangsa mesir 4000 tahun yang lalu. Diketahui *hieroglyph* bukanlah bentuk standar untuk menulis pesan.

Kriptografi adalah teknik dasar untuk keamanan data dan komunikasi. Hal itu menjadi sangat diperlukan dimana saluran komunikasi tidak bisa dibuat aman

secara sempurna (Bokhari, Alam, & Masoodi, 2012), sedangkan menurut (Scheiner, 1996) “Kriptografi adalah seni dan ilmu pengetahuan untuk menjaga pesan tetap aman”

“Kriptografi adalah suatu metode kemanan untuk melindungi suatu informasi dengan menggunakan kata-kata sandi yang hanya bisa dimengerti oleh orang yang berhak mengakses informasi tersebut. Kriptografi merupakan satu-satunya metode yang digunakan untuk melindungi informasi yang melalui jaringan komunikasi yang menggunakan *landline* (kabel di bawah tanah), satelit komunikasi, dan fasilitas *microwafe* (gelombang mikro). Prosedur-prosedur kriptografi juga bisa digunakan untuk autentifikasi pesan, digital signature, dan identifikasi pribadi untuk mengotorisasi transfer uang secara digital melalui ATM, kartu kredit, dan melalui suat jaringan” (Nuur & Rahman, 2013).

Menurut Garfinkel “Keamanan computer melingkupi empat aspek, yaitu *privacy, integrity, authentication, availability.*” (Raharjo, 1999) .Penjelasan lebih lanjut tentang aspek-aspek keamanan data dalam kriptografi adalah sebagai berikut:

a. *Privacy/Confidentiality*

   Merupakan usaha untuk menjaga informasi atau kerahasiaan data dari orang yang tidak punya hak. Data hanya boleh diakses oleh orang yang berwenang atau mempunyai hak. Contohnya data-data pribadi, data-data bisnis, data nasabah danlainnya. Serangan terhadap aspek ini dilakukan dengan penyadapan, misalnya *sniffer* atau *logger*.

b. *Integrity*

   Aspek ini menekankan bahwa informasi yang dikirim tidak mengalami modifikasi/diubah oleh pihak yang tidak berhak. Contoh serangan terhadap aspek ini berupa pengubahan data oleh orang yang tidak berhak, misalnya dengan menggunakan virus yang dapat mengubah informasi.

c. *Authentication*

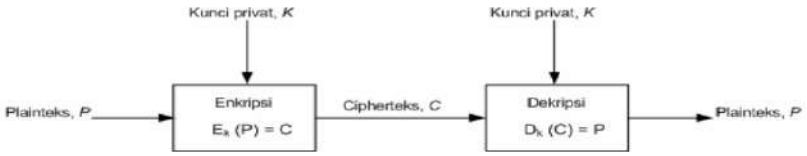
Aspek ini berhubungan dengan metode untuk meyakinkan keaslian data atau dokumen, sumber data, orang yang mengakses data, dan server yang digunakan. Ada beberapa cara yang bisa digunakan untuk mengatasi permasalahan dalam aspek ini yaitu dengan *watermarking* untuk data atau dokumen dan penggunaan *password* sebagai bukti dialah orang yang berhak mengakses.

d. *Availability*

Aspek ini menekankan pada ketersediaan informasi ketika dibutuhkan. Serangan yang terjadi dapat menghambat atau meniadakan akses ke informasi.

2.3 Jenis Algoritma Kriptografi

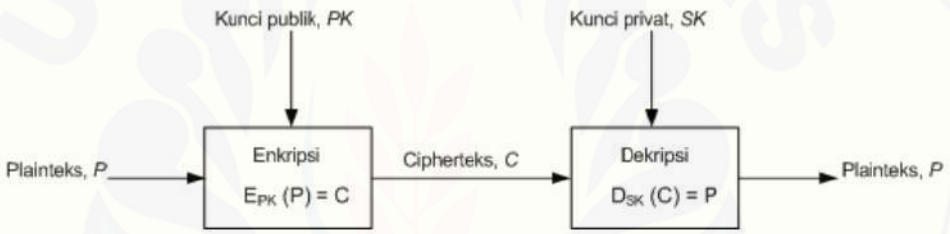
Kriptografi dibagi menjadi 2 berdasarkan kunci yang untuk proses enkripsi dan dekripsi, yaitu kriptografi simetris dan kriptografi asimetris Menurut Anonymous (dalam Nuur & Rahman, 2013) "berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi 2 macam, yaitu kriptografi simetri (*symmetric cryptography*) dan kriptografi asimetri(*asymetric cryptography*)." Sistem kriptografi simetris merupakan kroptografi yang dimana kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Keamanan system kriptografi simetris terletak pada kerahasiaan kunci, menurut (Scheiner, 1996) "membocorkan kunci berarti siapapun bisa mengenkripsi dan mendekripsi pesan. Selama komunikasi tetap menjadi rahasia, kunci harus tetap dirahasiakan". Istilah lain untukkriptografi simetris adalah kriptografi kunci privat (*private keycryptography*) atau kriptografi konvensional (*conventional cryptography*). Gambaran kriptografi simetri dapat dilihat pada Gambar 2.1.



Gambar 2.1 Kriptografi simetri

Sumber: (Nuur & Rahman, 2013)

Sistem kriptografi asimetris dirancang agar kunci yang digunakan untuk proses enkripsi tidak sama dengan kunci untuk proses dekripsi. Istilah lain untuk kriptografi asimetris adalah kriptografi kunci publik (*public keycryptography*), sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun, sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan. Menurut (Scheiner, 1996) "algoritma asimetris juga disebut *public key* karena kunci enkripsi dapat dibuat publik. Orang asing dapat menggunakan kunci enkripsi untuk mengenkripsi pesan, tapi hanya orang tertentu dengan kunci dekripsi yang sesuai yang dapat mendekripsi pesan tersebut. Dalam kriptografi ini, kunci enkripsi biasa disebut *public key* dan kunci dekripsi biasa disebut *private key*" Gambaran kriptografi asimetri dapat dilihat pada Gambar 2.2.



Gambar 2.2 Kriptografi asimetri

Sumber: (Nuur & Rahman, 2013)

2.4 Algoritma AES

Algoritma AES merupakan standar enkripsi dengan kunci simetris yang diadopsi oleh pemerintahan Amerika Serikat. Menurut (Lusiana, Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma AES-128, 2011) "algoritma AES merupakan algortima simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi"

Sejarah dari algoritma AES, berawal dari algoritma kriptografi bernama Rijndael yang didesain oleh oleh Vincent Rijmen dan John Daemen asal Belgia keluar sebagai pemenang kontes algoritma kriptografi pengganti DES yang diadakan oleh NIST (*National Institutes of Standards and Technology*) milik pemerintah Amerika Serikat pada 26 November 2001. Algoritma Rijndael inilah yang kemudian dikenal dengan *Advanced Encryption Standard* (AES). Setelah mengalami beberapa proses standardisasi oleh NIST, Rijndael kemudian diadopsi

menjadi standard algoritma kriptografi secara resmi pada 22 Mei 2002. Pada 2006, AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik.

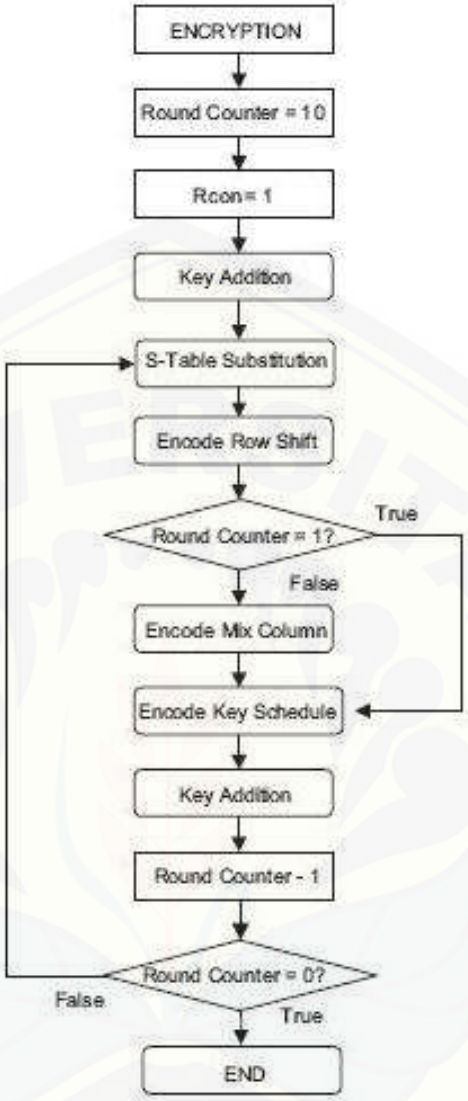
AES ini merupakan algoritma block cipher dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) bukan dengan jaringan Feistel sebagaiman *block cipher* pada umumnya.. Pengelompokkan jenis-jenis AES terbagi 3, yaitu .AES-128, AES-192, AES-256, hal ini didasarkan panjang kunci yang digunakan. Angka-angka di belakang kata AES menggambarkan 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 memiliki ukuran *block* yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128, 192, atau 256 bit.

2.5 Algoritma AES-128

Menurut Lusiana (2011), proses putaran (*round*) enkripsi AES-128 dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

a. *Add round key*
b. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap putaran adalah: *Sub Bytes, Shift Rows, Mix Columns, dan Add Round Key.*
c. *Final round*, adalah proses untuk putaran terakhir yang meliputi *Sub Bytes, Shift Rows, dan Add Round Key.*

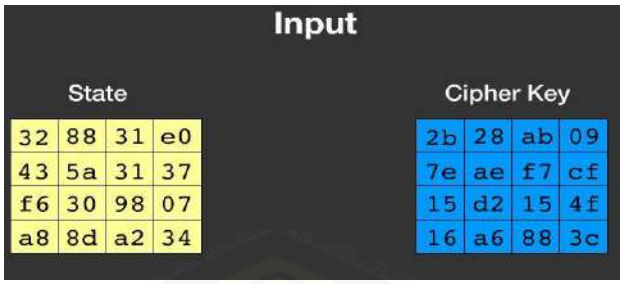
Diagram alir proses enkripsi AES-128 dapat dilihat pada Gambar 2.3.



Gambar 2.3 Enkripsi AES-128

Sumber: (Lusiana, 2011)

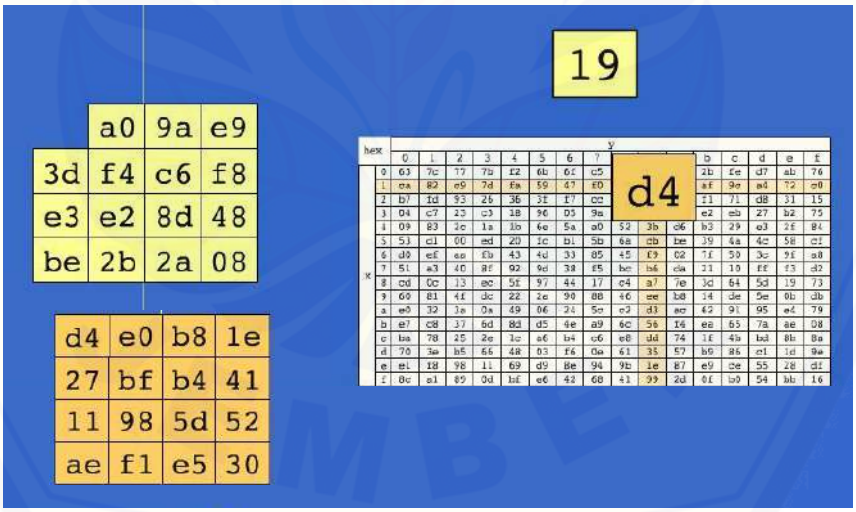
Lebih lanjutnya dalam memahami algoritma AES-128. Kita misalkan sajatelah disiapkan teks berita yang sudah dikonversikan dan diolah sedemikian rupa ke dalam bentuk bit menggunakan kode ASCII, sehingga menjadi matriks (*array*) berukuran 4x4 dan begitu pula kata kuncinya yang nampak pada Gambar 2.4.



Gambar2.4 Matriks berita 4x4

Sumber: (R12K4, 2008)

Setelah didapatkan *Round Key 1* di atas, selanjutnya state yang telah dikonversi ke dalam kode ASCII akan di *SubBytes* menggunakan *S-Box*. Cara penggunaan Sub Bytes yaitu dengan cara mensubstitusikan 1 sel pada State dengan 1 sel yang bersesuaian pada S-Box. Elemen-elemen pada S-Box itu sendiri telah ditentukan sebelumnya.Misal, kita akan menggantikan elemen 19 pada State. Maka elemen yang bersesuaian pada S-Box terletak pada baris ke-1 dan kolom ke-9. Begitu pun seterusnya seperti pada Gambar 2.5.

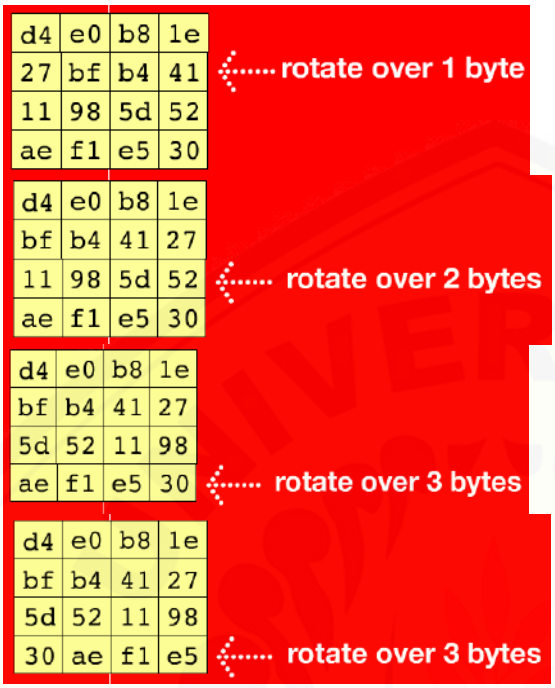


Gambar 2.5 *Sub Bytes State*

Sumber: (R12K4, 2008)

Setelah melalui tahap *SubBytes*, tahap selanjutnya yaitu *ShiftRows*. Transformasi *ShiftRows* dilakukan dengan cara menggeser baris secara *wrapping* (siklik) pada 3 baris terakhir dari *array state*. Jumlah pergeseran bergantung pada nilai baris (r). Baris *r* = 1 digeser sejauh 1 *byte*, baris r = 2 digeser sejauh 2 *byte*,

dan baris r = 3 digeser sejauh 3 *byte*. Baris r = 0 tidak digeser. Gambaran transformasi *ShiftRows* dapat dilihat pada Gambar 2.6.



Gambar 2.6 *ShiftRows*

Sumber: (R12K4, 2008)

Proses selanjutnya yaitu MixColumns, menurut (Surian, 2006) Proses *MixColumns* akan beroperasi pada tiap kolom dari tabel *state*. Operasi ini menggabungkan 4 *bytes* dari setiap kolom tabel *state* dan menggunakan transformasi linier. Operasi *Mix Columns* memperlakukan setiap kolom sebagai polinomial 4 suku dalam *Galois field* dan kemudian dikalikan dengan c(x) modulo (x4+1), dimana $c(x)=3x_3+x_2+x+2$. Kebalikkan dari polinomial ini adalah $c(x)=11x_3+13x_2+9x+14$. Operasi *MixColumns* juga dapat dipandang sebagai perkalian matrix.

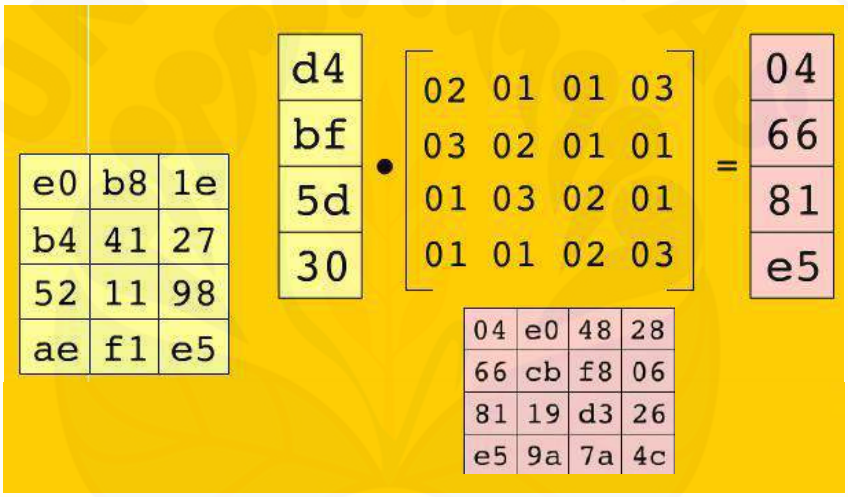
Transformasi ini dinyatakan sebagai perkalian matriks pada Gambar 2.7. Implementasi *Mix Columns* pada state dapat dilihat pada Gambar 2.8.

$$s'(x) = a(x) \otimes s(x)$$

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Gambar 2.7 Perkalian Matriks a(x)

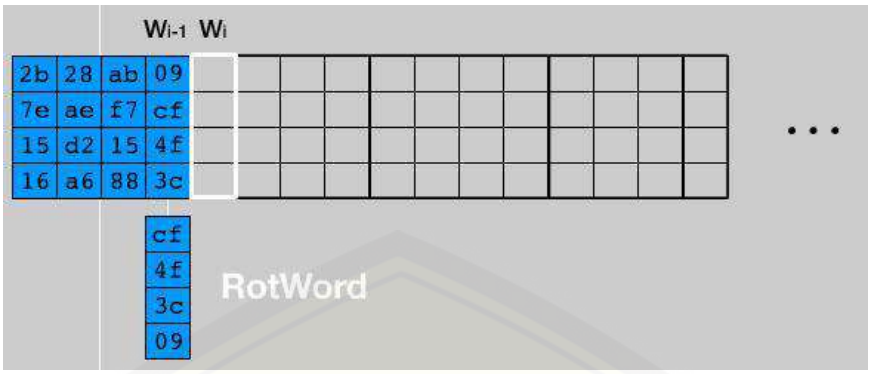
Sumber: (R12K4, 2008)



Gambar 2.8 Implementasi *MixColumns* pada *state*

Sumber: (R12K4, 2008)

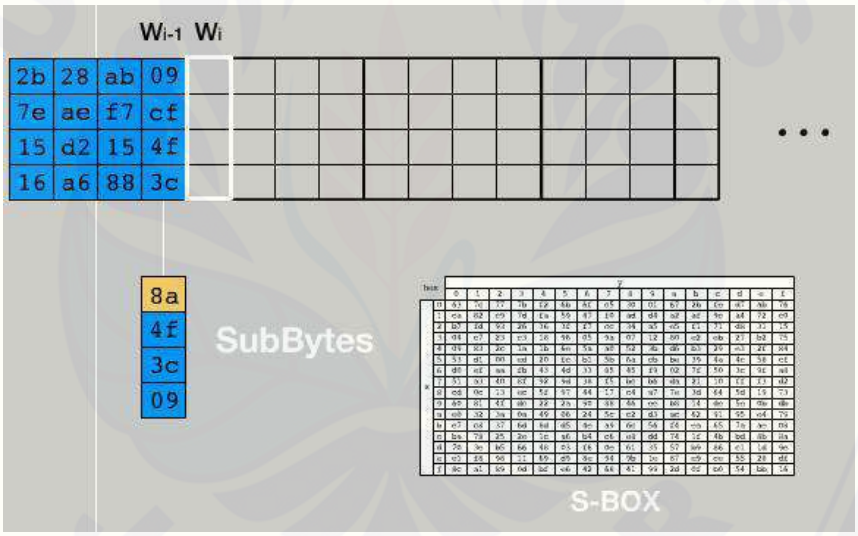
Langkah selanjutnya adalah proses pembangkitan kunci menjadi 10 buah *round key*. Untuk membangkitkan *array* kunci ini menjadi 10 buah *round key*, maka langkah awal yang dilakukan adalah dengan cara menukar posisi antarbaris. Baris ke-1 menjadi baris ke-4, ke-2 menjadi ke-1, ke-3 menjadi ke-2, dan ke-4 menjadi ke-3. Kolom terakhir yangsudah ditukar posisinya bernama *RotWord*, yang nampak pada Gambar 2.9.



Gambar 2.9 *RotWord*

Sumber: (R12K4, 2008)

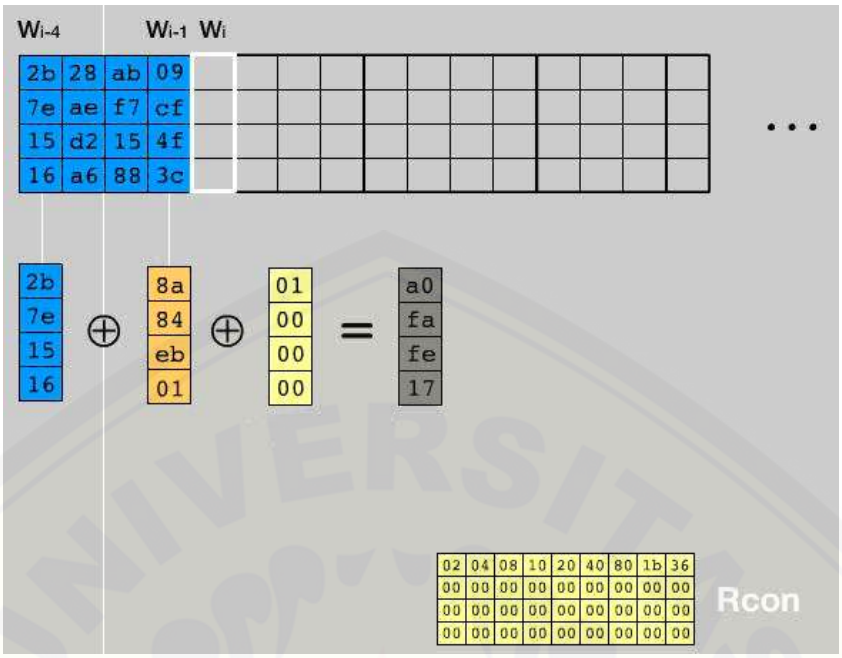
Setelah itu, masing-masing elemen yang telah di *RotWord* di-*SubBytes* seperti Gambar 2.10.



Gambar 2.10 *SubBytes*

Sumber: (R12K4, 2008)

Setelah data satu kolom pada *RotWord* telah di-*SubBytes*-kan, maka kolom ke-1 array kunci di-XOR-kan dengan hasil *SubBytes* dari *RotWord* dan *Rcon* kolom1 yang nampak pada Gambar 2.11.



Gambar 2.11 XOR

Sumber: (R12K4, 2008)

Hasil XOR-an tersebut menjadi kolom ke-1 *RoundKey1*, seperti Gambar 2,8.

Gambar 2.12 *Round Key* 1

Sumber: (R12K4, 2008)

Lakukan langkah-langkah di atas hingga *roundkey* ke-10 seperti pada Gambar 2.13.

Gambar 2.13 Proses enkripsi AES-128 secara lengkap

Sumber: (R12K4, 2008)

2.6 *QR Code*

Menurut Law dkk dalam (Meimaharani & Laily, 2014) "*QR code* adalah jenis *barcode* yang berbentuk dua dimensi yang dikembangkan oleh Denso Wave, sebuah divisi Denso *corporation,* sebuah perusahaan di Jepang, yang dipublikasikan pada tahun 1994". Pada awal penggunaannya *QR code* digunakan untuk pelacakan kendaraan bagian manufaktur, namun semakin luasnya penggunaan *QR code* bisa dilihat dalam penerapannya di aplikasi komersial dan kemudahan pelacakan aplikasi berorientasi yang ditujukan untuk pengguna telepon selular. Negara Jepang telah menerapkan penggunaan *QR code,* hampir semua jenis ponsel di Jepang bisa membaca *QR code* sebab sebagian besar pengusaha telah memilih *QR code* sebagai alat tambahan dalam program promosi produknya, baik yang bergerak dalam perdagangan maupun dalam bidang jasa.

Fungsionalitas utama dari *QR code* adalah agar mudah dibaca oleh pemindai *QR* merupakan singkatan dari *quick respond* (respon cepat), sesuai dengan tujuannya adalah untuk menyampaikan informasi dengan cepat dan mendapatkan respon yang cepat pula, oleh karena itu *QR code* dapat dengan mudah dibaca oleh pemindai. *QR code* biasanya berisi sampai 2.844 dan bentuk dari *QR code* diperoleh dengan acak. Berbeda dengan *barcode* biasa yang berbentuk satu dimensi dan menyimpan informasi secara horizontal. *QR code* mampu menyimpan informasi secara horizontal dan vertical, oleh karena itu secara otomatis *QR code* dapat menampung informasi yang lebih banyak daripada kode batang (*barcode*). Contoh *QR code* bisa dilihat pada gambar 2.14

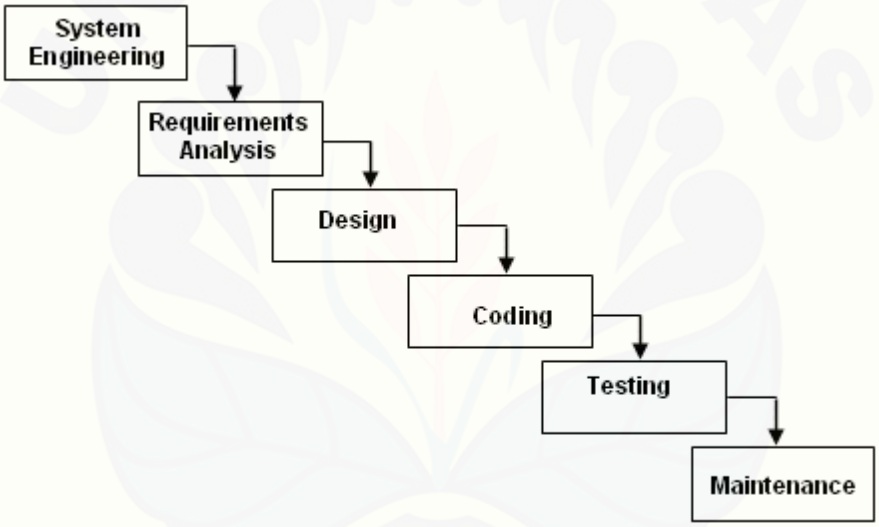
Gambar 2.14 QR Code

Sumber: (Meimaharani & Laily, 2014)

2.7 Model *Waterfall*

Model *Waterfall* adalah sebuah model pengembangan perangkat lunak yang membutuhkan pendekatan sistematis dan sekuensial, dimana satu tahap dilakukan setelah tahap sebelumnya selesai dilakukan, biasanya model ini disebut alur hidup klasik (*classic life cycle*). Menurut (Mangiwa & Wicaksana, 2008) "metode ini membutuhkan pendekatan sistematis dan sekuensial dalam pengembangan perangkat lunak, dimulai dari tingkat sistem dan kemajuan analisis, desain, koding, testing, dan pemeliharaan".

Gambar ilustrasi untuk model *waterfall* dapat dilihat pada Gambar 2.15.



Gambar 2.15 Model *waterfall*

Sumber: (Mangiwa & Wicaksana, 2008)

Keterangan Gambar 2.15 menurut(Mangiwa & Wicaksana, 2008):

a. Rekayasa dan Pemodelan Sistem/Informasi (*System/Information Engineering and Modeling*).

   Tahap ini juga kadang disebut dengan *Project Definition*

b. Analisis Kebutuhan Perangkat Lunak (*Software Requirement Analysis*)

   Proses pengumpulan kebutuhan diintensifkan ke perangkat lunak. Hasilnya harus didokumentasikan dan di-*review* ke pelanggan

c. Desain (*Design*)

   Proses desain mengubah kebutuhan-kebutuhan menjadi bentuk karakteristik yang dimengerti perangkat lunak sebelum dimulai penulisan program.

d. Penulisan Program (*Coding*)

   Desain tadi harus diubah menjadi bentuk yang dimengerti mesin (komputer). Maka dilakukan langkah penulisan program.

e. Testing

   Setelah kode program selesai dibuat, dan program dapat berjalan, testing dapat dimulai. Testing difokuskan pada logika *internal* dari perangkat lunak, fungsi *eksternal,* dan mencari segala kemungkinan kesalahan.

f. *Support/Maintenance*

   Perangkat lunak setelah diberikan pada pelanggan, mungkin dapat ditemui *error* ketika dijalankan dilingkungan pelanggan. Pemeliharaan ini dapat berpengaruh pada semua langkah yang dilakukan sebelumnya.

Adapun beberapa kelebihan dan kekurangan yang dimiliki model *waterfall.* Menurut (Mangiwa & Wicaksana, 2008), “kelebihan metode ini masih lebih baik digunakan walaupun sudah tergolong kuno, daripada menggunakan pendekatan asal-asalan. Kekurangan metode ini pada kenyataannya, jarang mengikuti urutan sekuensial seperti pada teori. Iterasi sering terjadi menyebabkan masalah ”

BAB 3. METODOLOGI PENELITIAN

Pada bab ini akan membahas jenis penelitian, dan alur penelitian yang digunakan dalam pembangunan aplikasi validasi tiket pada perusahaan travel pt. bumindo jaya cemerlang dan implementasi algoritma aes-128 dan *qr code*pada aplikasi tersebut untuk menjaga keaslian tiket travel.

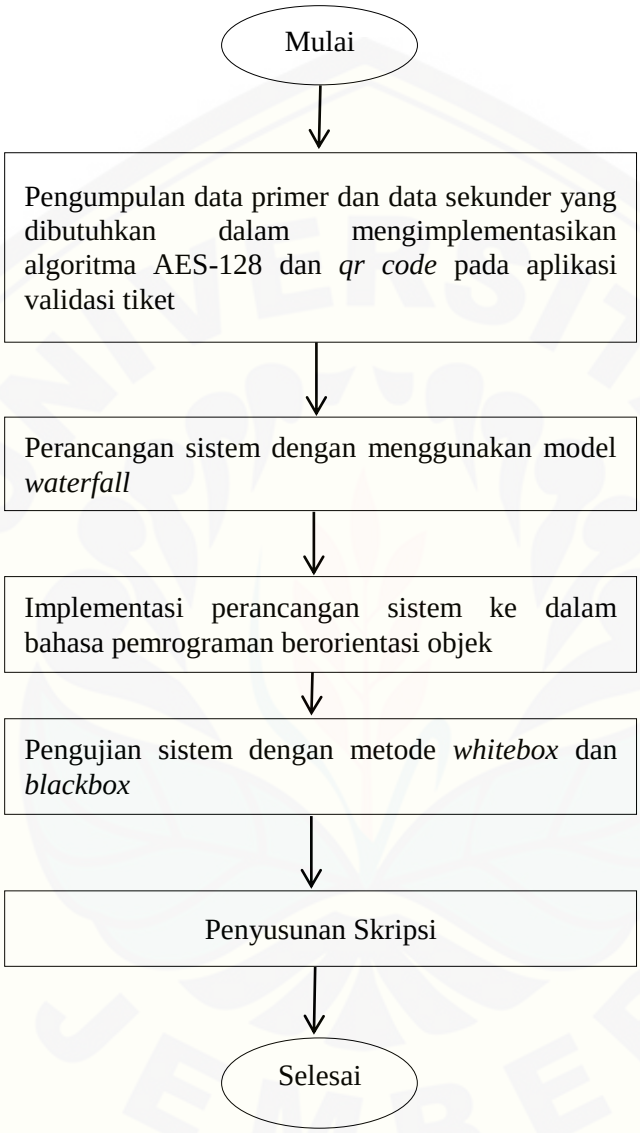
3.1 Jenis Penelitian

Jenis penelitian yang digunakan merupakan jenis penelitian kualitatif. Sehingga data yang diperoleh bukan berupa angka-angka, tetapi data hasil wawancara. Tujuan dari penelitian kulitatif yaitu untuk menggambarkan fakta yang ada. Masalah yang ditemukan pada fakta yang ada, akan dicocokkan dengan teori yang berlaku menggunakan metode deskriptif.

3.2 Alur Penelitian

Alur Penelitian menjelaskan urutan penelitian yang akan dilakukan yaitu tahap pengumpulan data, tahap perancangan, tahap implementasi, tahap pengujian dan tahap penyusunan skripsi.

Diagram alir tahapan yang akan dilakukan dalam penelitian pengimplementasian algoritma AES-128 dan *qr code* pada aplikasi validasi tiket pt. Bumindo Jaya Cemerlang dapat dilihat pada Gambar 3.1.



Gambar 3.1 Diagram alir penelitian

3.3 Tahap Pengumpulan Data

Tahap pengumpulan data dilakukan dengan cara mencari data primer dan data sekunder yang dibutuhkan dalam mengimplementasikan algoritma AES-128 dan *qr code* pada aplikasi validasi tiket travel.

Data primer diperoleh langsung pada objek penelitian dengan cara wawancara pada Pt. Bumindo Jaya Cemerlang. Wawancara ini dilakukan untuk mendapatkan data-data yang dibutuhkan dalam pembuatan aplikasi validasi tiket menggunakn *qr code*. Data tersebut yaitu sebagai berikut:

a. Data spesifikasi Pt. Bumindo Jaya Cemerlang

   Data tentang spesifikasi dari administrasi yang ada di Pt. Bumindo Jaya Cemerlang.

b. Data fasilitas Pt. Bumindo Jaya Cemerlang

   Data mengenai fasilitas-fasilitas yang ada di Pt. Bumindo Jaya Cemerlang dan fasilitas yang perlu diterapkan kedalam aplikasi validasi tiket Pt. Bumindo Jaya Cemernlang.

Data sekunder diperoleh dengan carastudi literatur pada penelitian-penelitian terdahulu di berbagai jurnal, buku, skripsi, dan *e-book*. Studi literatur dibutuhkan untuk menunjang pemahaman dan pengetahuan penulis tentang materi, konsep, teori, dan metode apa yang diperlukan dalam proses pengerjaan tugas akhir ini.

3.4 Tahap Perancangan

Tahap perancangan merupakan tahapan yang dilakukan setelah tahapan pengumpulan data selesai dilakukan. Pada tahapan ini peneliti akan mulai membuat rancang bangun aplikasi validasi tiket dengan menggunakan metode kriptografi AES. Pada proses perancangan aplikasi ini, akan digunakan model perancangan *waterfall*.

Perancangan sistem yang digunakan menggunakan konsep berbasis objek dengan pemodelan *Unified Modelling Language* (UML). Pemodelan UML yang digunakan pada penelitian ini antara lain, *Business Process*, *Usecase Diagram*, *Usecase Scenario*, *Sequence Diagram*, *Activity Diagram*, *Class diagram* dan *Entity*

Relationship Diagram (ERD). Perangkat lunak yang akan dibangun ini menggunakan bahasa pemrograman PHP pada server dan bahasa pemrograman Java XML pada perangkat *mobileandroid*. Dengan database yang digunakan adalah database model menggunakan mySql pada server, dan database SQLite pada perangkat *mobileandroid*.

3.5 Tahap Implementasi

Pada tahap implementasi ini, dilakukan dengan cara mentransformasikan desain sistem yang telah dibuat ke dalam sebuah bahasa pemrograman berorientasi objek sehingga dapat dihasilkan suatu aplikasi validasi tiket. Algoritma AES-128 dan *qr code* diimplementasikan pada aplikasi validasi tiket untuk menjaga keaslian dari tiket.

3.6 Tahap Pengujian

Tahap pengujian dilakukan apabila aplikasi yang dibuat telah selesai dan siap untuk digunakan pengguna. Pengujian yang dilakukan berguna untuk mengetahui sejauh mana pengimplementasian algoritma AES-128 dan *qr code* pada aplikasi validasi tiket Pt. Bumindo Jaya Cemerlang. Tahapan pengujian dilakukan dengan mencari kesalahan-kesalahan yang mungkin terjadi, serta melakukan perbaikan untuk menyempurnakan aplikasi validasi tiket Pt. Bumindo Jaya Cemerlang dalam mengimplementasikan algoritma AES-128 dan *qr code*. Proses pengujian dilakukan dengan metode *whitebox* oleh pengembang dan *blackbox* oleh pengguna. Pengujian whitebox dilakukan untuk mengetahui apakah aplikasi yang dibangun dari segi desain dan program sesuai dengan kebutuhan. Sedangkan untuk pengujian *blackbox* dilakukan hanya dengan memperhatikan masukan/keluaran (I/O) yang dihasilkan oleh aplikasi. Apakah I/O sudah sesuai dengan yang diinginkan atau tidak melalui kuesioner yang diisi pengguna.

3.7 Tahap Penyusunan Skripsi

Tahap penyusunan skripsi merupakan langkah akhir pada penelitian ini. Pada tahap ini akan dilakukan penyusunan laporan yang menjelaskan dasar teori dan metode yang digunakan dalam skripsi ini serta hasil dari implementasi algoritma AES-128 dan *qr code* pada validasi tiket Pt. Bumindo Jaya Cemerlang.

BAB 5 HASIL DAN PEMBAHASAN

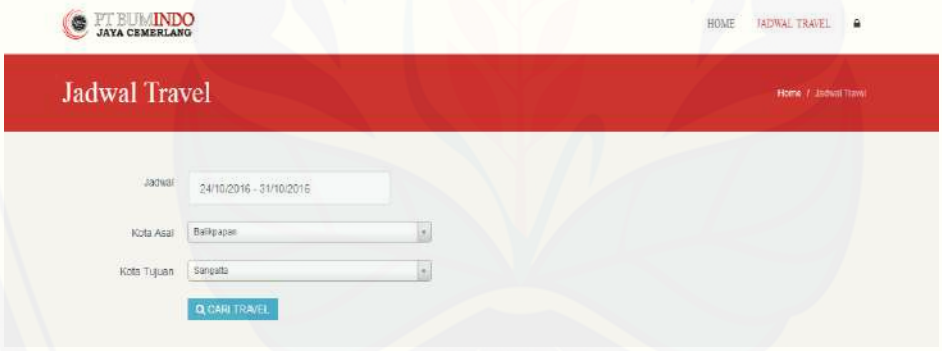
Bab ini menjabarkan tentang hasil implementasi implementasi AES-128 dan *Qr Code* pada system di travel Pt. Bumindo Jaya Cemerlang. Pembahasan yang akan dijabarkan diutamakan dalam hal keamanan aplikasi dengan menggunakan AES-128.

5.1 Implementasi Sistem

Tahap implementasi ini merutahap pengkodean dari perancangan yang telah dibuat ke dalam bahasa pemrograman. Tahap pengkodean ini akan menghasilkan beberapa *interface* atau tampilan sistem sesuai dengan hak akses *user*. Berikut ini adalah beberapa tampilan fitur yang ada dalam sistem.

5.1.1 Tampilan Jadwal Travel

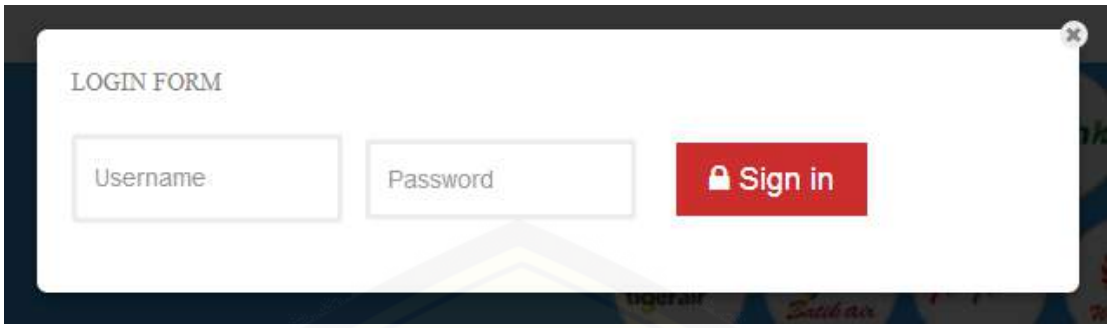
Tampilan menu jadwal travel merupakan menu untuk melihat jadwal travel yang tersedia, seperti yang ditunjukkan pada gambar 5.1.



Gambar 5.1 Tampilan Jadwal Travel

5.1.2 Tampilan *Login*

Tampilan menu *login* merupakan tampilan ketika *user* belum *login* ke system. *User* harus mengisi *username* dan *password* untuk bisa mengakses sistem sesuai hak akses user, seperti yang ditunjukkan pada gambar 5.2

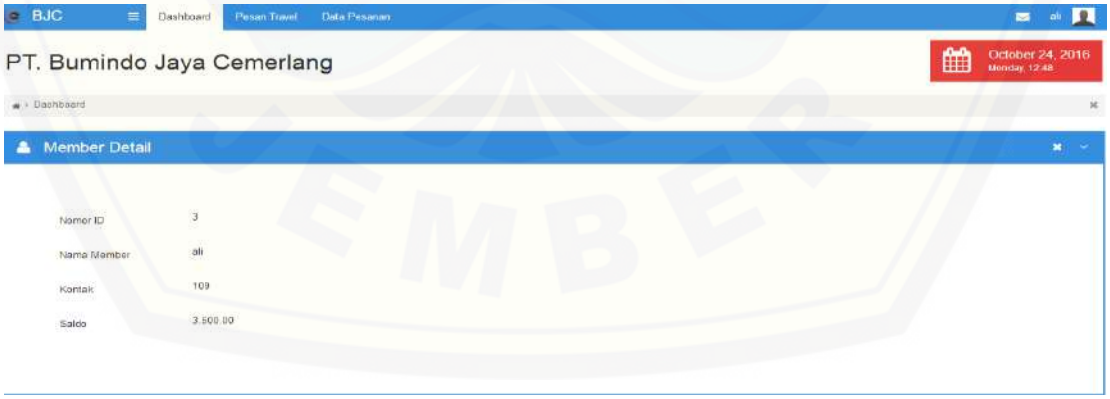


Gambar 5.2 Tampilan *Form Login*

Sistem akan menampilkan tampilan atau *interface* yang berbeda setelah *user* berhasil *login*, dalam kasus ini ada dua *user* berbeda yaitu admin dengan tampilan utama seperti yang ada pada gambar 5.3

Gambar 5.3 Tampilan *dashboard* Admin

User member dengan tampilan utama seperti yang ada pada gambar 5.4.



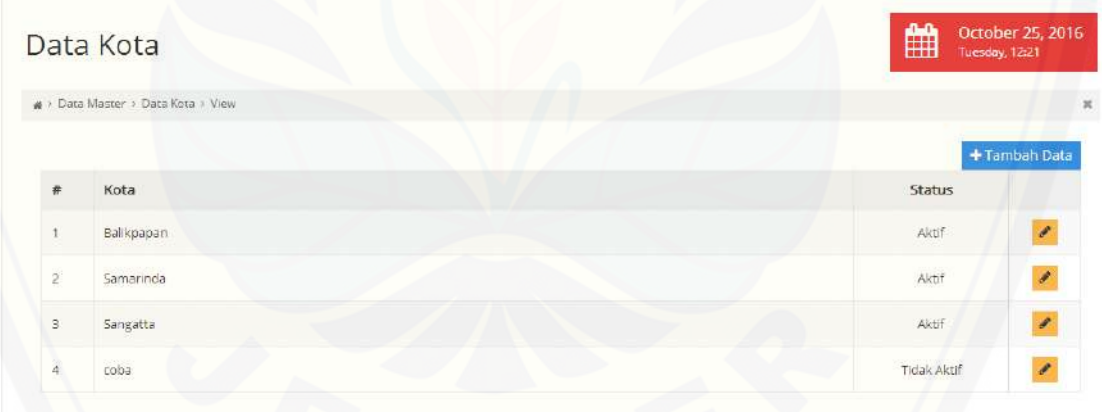
Gambar 5.4 Tampilan *dashboard Member*

Jika *user* salah memasukkan *username* atau *password* sistem akan menampilkan tampilan seperti yang ada pada gambar 5.5

Gambar 5.5 Tampilan login salah *password* atau *username*

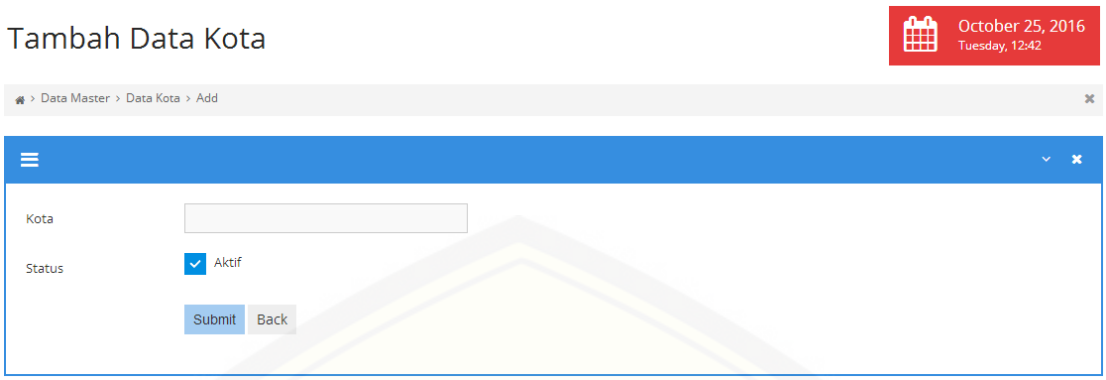
5.1.3 Tampilan Data Kota

Menu data kota memiliki sub menu tambah dan *edit* data kota. Tampilan utama menu data kota bisa dilihat pada gambar 5. 6.



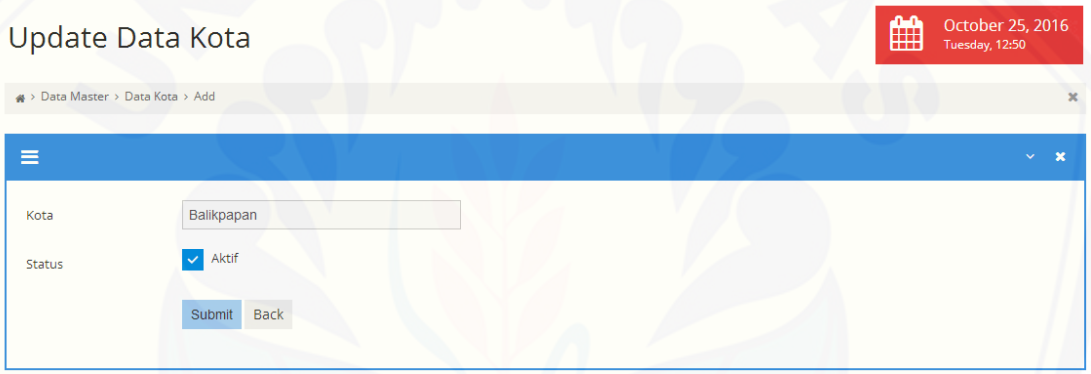
Gambar 5. 6 Tampilan utama menu data kota

Untuk menambah data kota, pada menu ini menyediakan *form* tambah data setelah klik tombol tambah data. *Form* tambah data bisa dilihat pada gambar 5.7.



Gambar 5.7 Tampilan tambah data kota

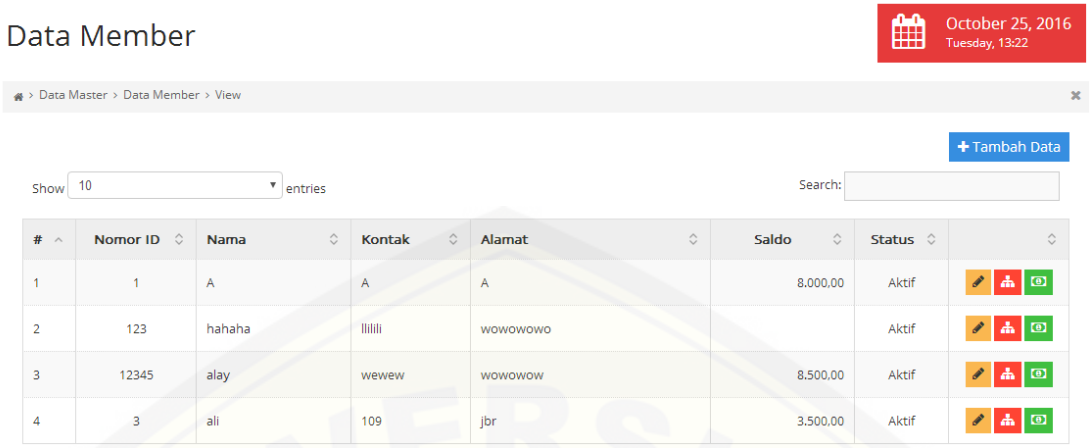
Sub menu *edit* juga disediakan di menu data kota dengan cara klik ikon *edit.* Tampilan *form edit* bisa dilihat pada gambar 5.8.



Gambar 5.8 Tampilan *Edit* data kota

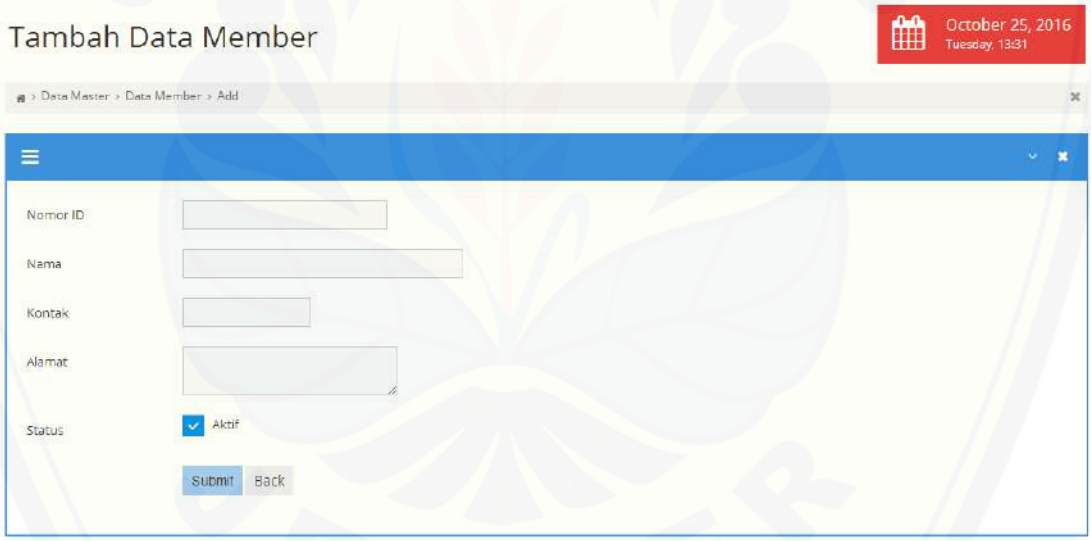
5.1.4 Tampilan Data *Member*

Menu data *member* memiliki sub menu tambah data, *edit*, tambah *user*, tambah saldo. Tampilan utama data *member* bisa dilihat pada gambar 5.9.



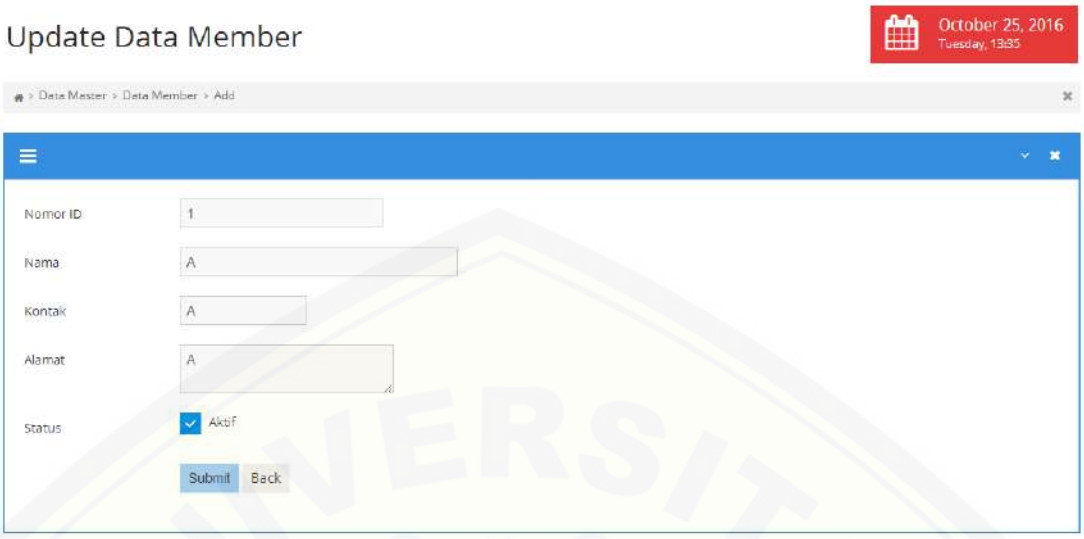
Gambar 5.9 Tampilan utama menu data *member*

Untuk menambah data *member*, pada menu ini menyediakan *form* tambah data setelah klik tombol tambah data. *Form* tambah data bisa dilihat pada gambar 5.10.



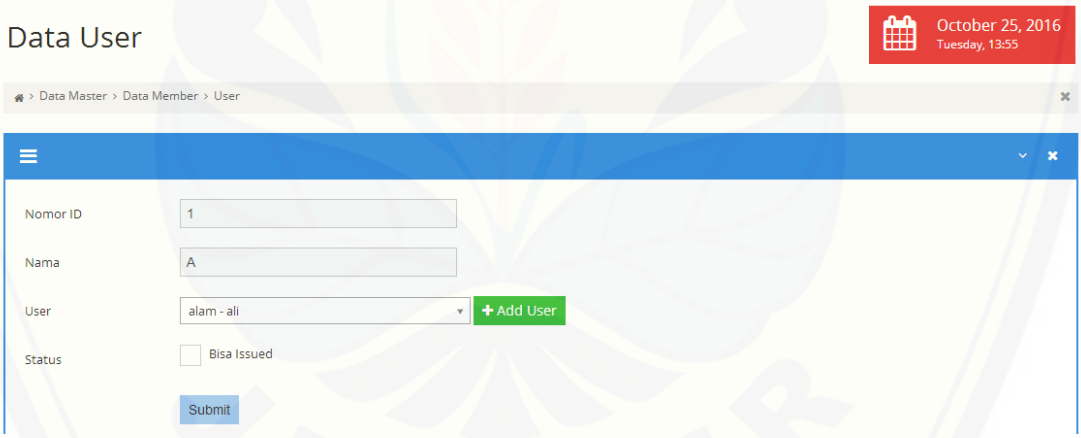
Gambar 5.10 Tampilan tambah data *member*

Sub menu *edit* juga disediakan di menu data *member* dengan cara klik ikon *edit.* Tampilan *form edit* bisa dilihat pada gambar 5.11.



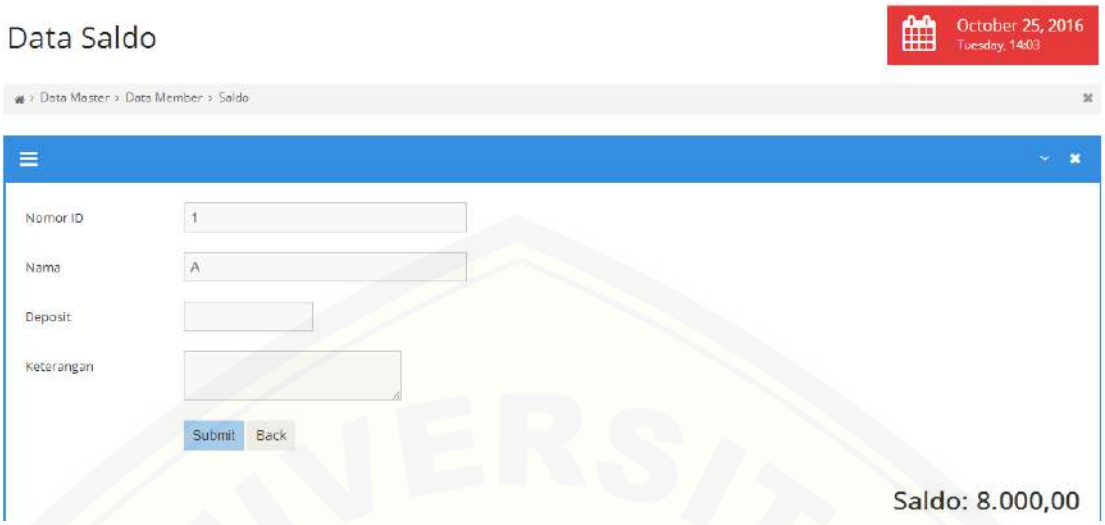
Gambar 5.11 Tampilan *edit* data *member*

Menu data *member* juga menyediakan tambah data *user*, *form* tambah data *user* bisa ditampilkan setelah klik ikon tambah data *user* seperti yang ditampilkan dalam gambar 5.12.



Gambar 5.12 Tampilan tambah data *user*

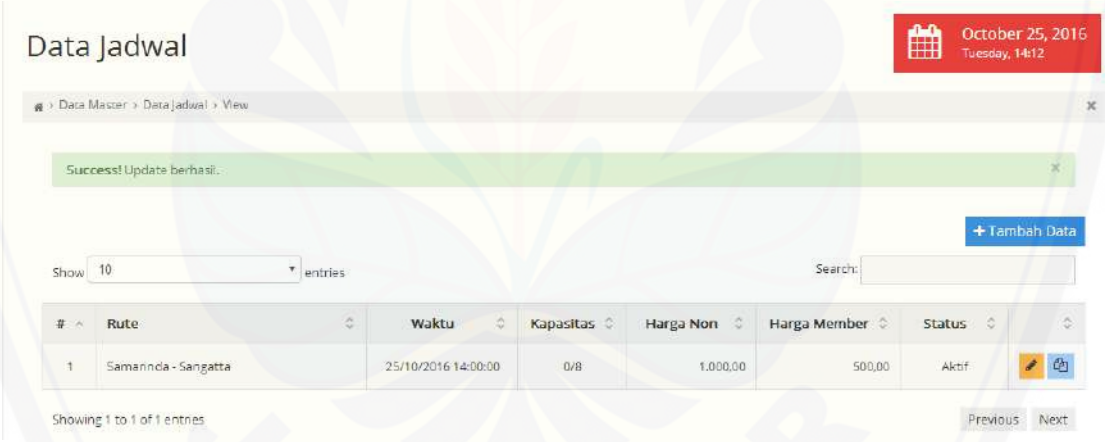
Sub menu tambah saldo juga disediakan di menu data *member* dengan cara klik ikon tambah saldo. Tampilan *form* tambah saldo bisa dilihat pada gambar 5.13.



Gambar 5.13 Tampilan tambah saldo

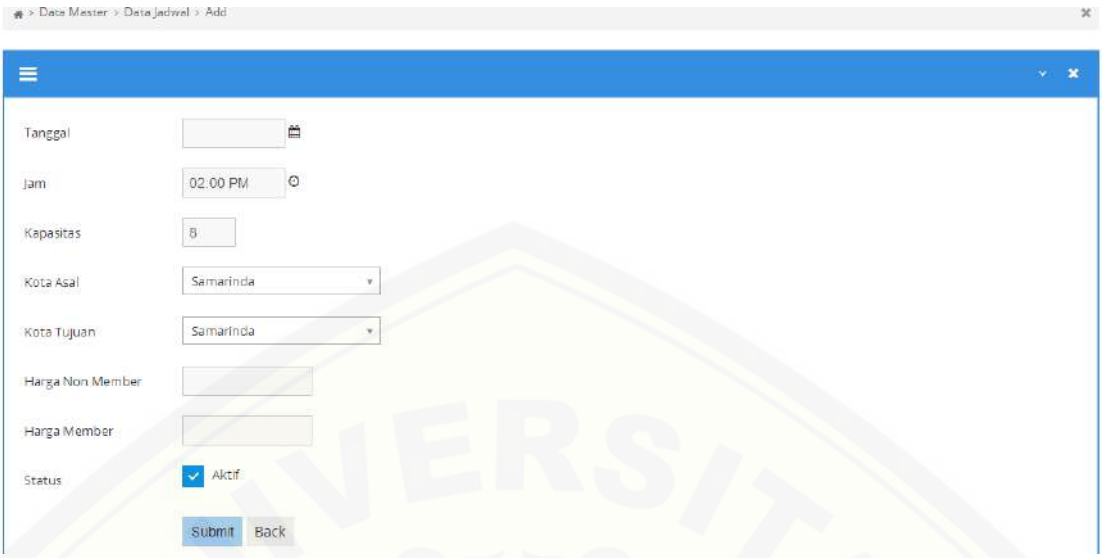
5.1.5 Tampilan Data Jadwal

Menu data jadwal memiliki sub menu tambah data, *edit*, *copy*. Tampilan utama data *member* bisa dilihat pada gambar 5.14.



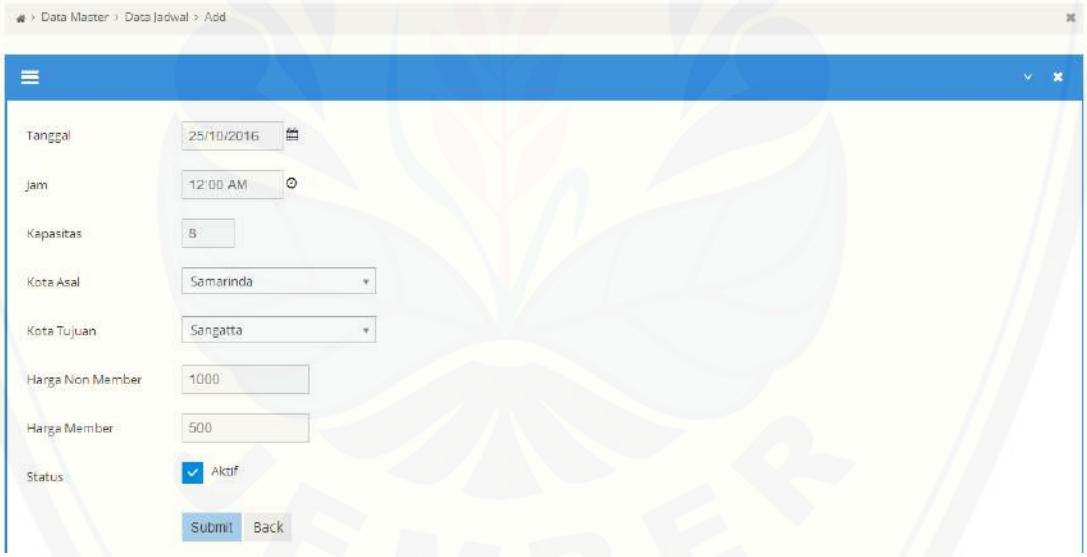
Gambar 5.14 Tampilan utama data jadwal

Untuk menambah data jadwal, pada menu ini menyediakan *form* tambah data setelah klik tombol tambah data. *Form* tambah data bisa dilihat pada gambar 5.15.



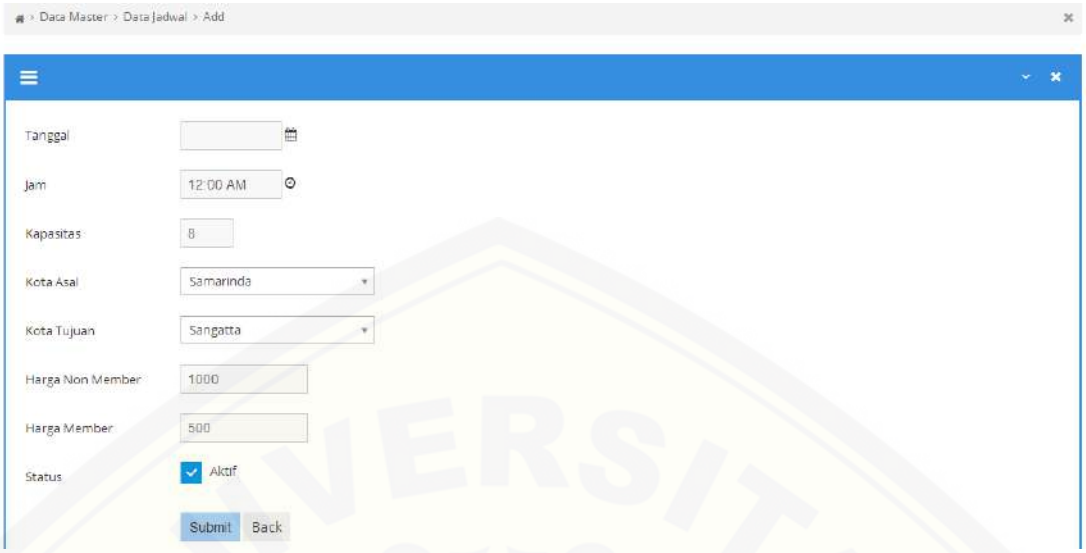
Gambar 5.15 Tampilan tambah data jadwal

Sub menu *edit* juga disediakan di menu data jadwal dengan cara klik ikon *edit.* Tampilan *form edit* bisa dilihat pada gambar 5.16.



Gambar 5.16 Tampilan *edit* data jadwal

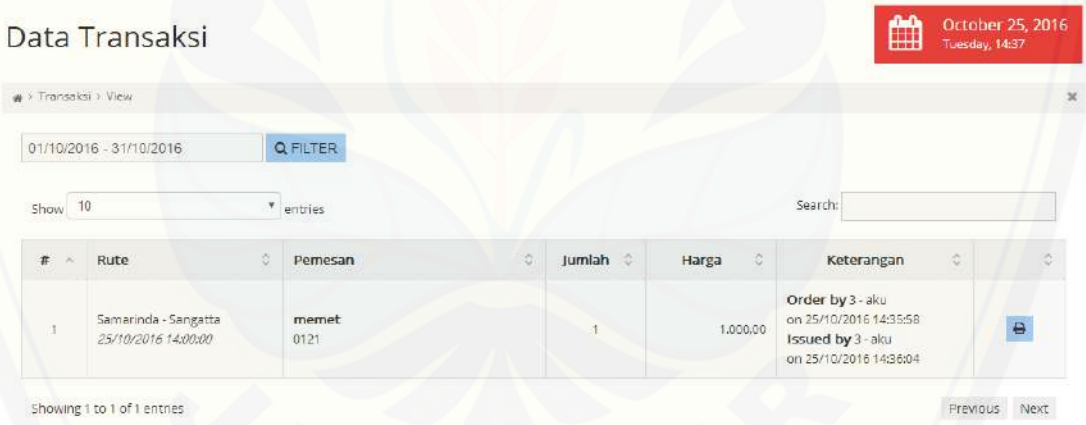
Sub menu *copy* juga disediakan di menu data jadwal dengan cara klik ikon *copy.* Tampilan *form copy* bisa dilihat pada gambar 5.17.



Gambar 5.17 Tampilan *copy* data jadwal

5.1.6 Tampilan Data Transaksi

Menu data transaksi memiliki sub menu cetak tiket. Tampilan utama data *member* bisa dilihat pada gambar 5.18.



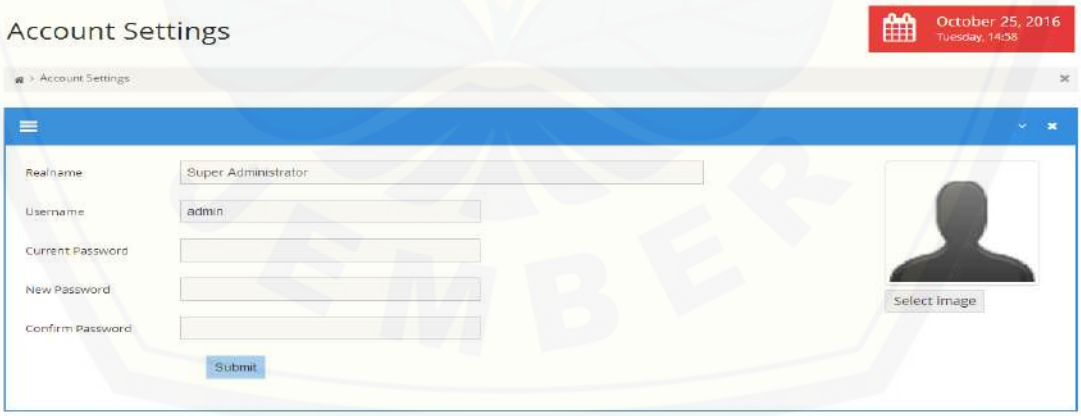
Gambar 5.18 Tampilan utama data transaksi

Sub menu cetak tiket disediakan di menu data transaksi dengan cara klik ikon cetak. Tampilan halaman cetak bisa dilihat pada gambar 5.19.

Gambar 5.19 Tampilan tiket setelah dicetak

5.1.7 Tampilan *Account Settings*

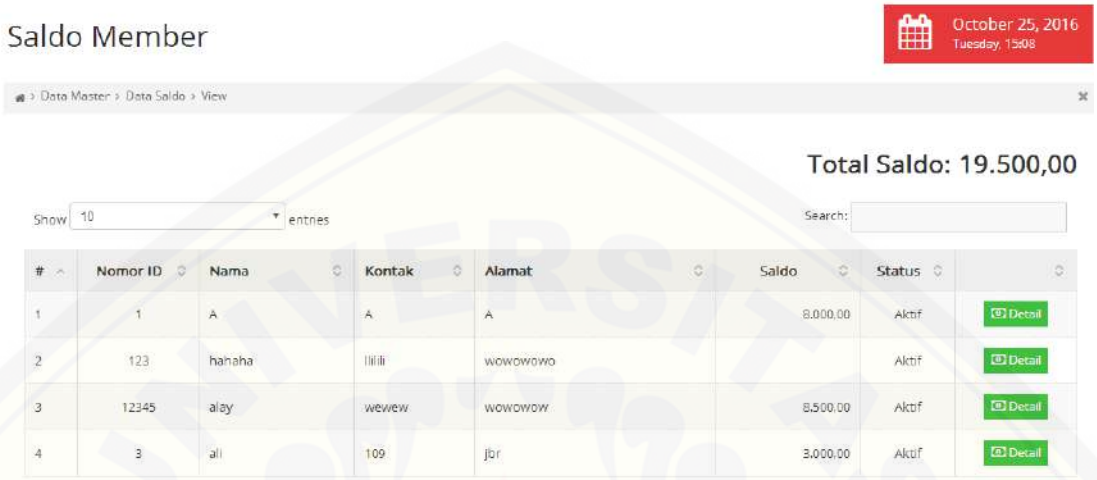
Tampilan *account setting* merupakan menu untuk mengubah data akun. Menu ini berisi *form* untuk mengubah data akun seperti yang terlihat di gambar 5.20.



Gambar 5.20 Tampilan *account setting*

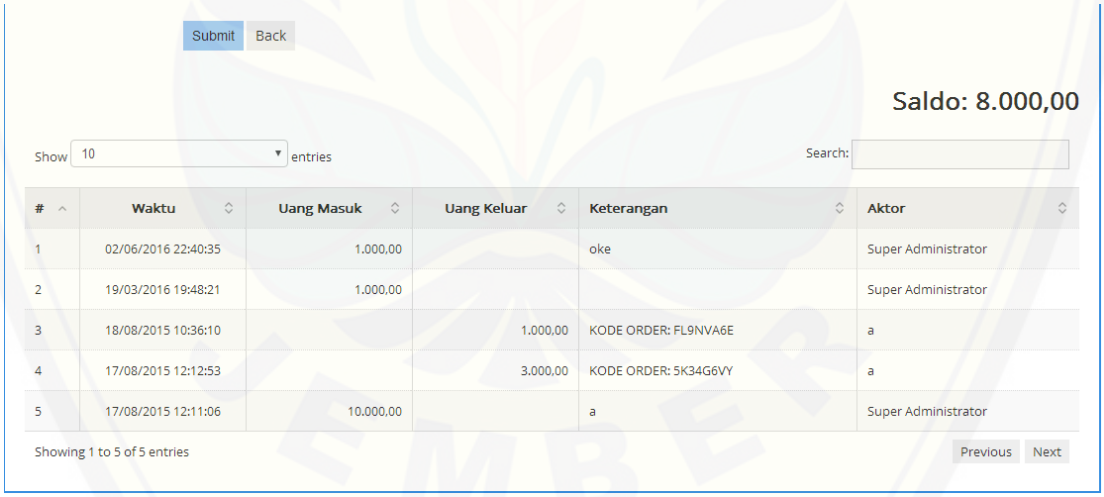
5.1.8 Tampilan Data Saldo

Menu data saldo memiliki sub menu *detail*. Tampilan utama data saldo bisa dilihat pada gambar 5.21.



Gambar 5.21 Tampilan utama data saldo

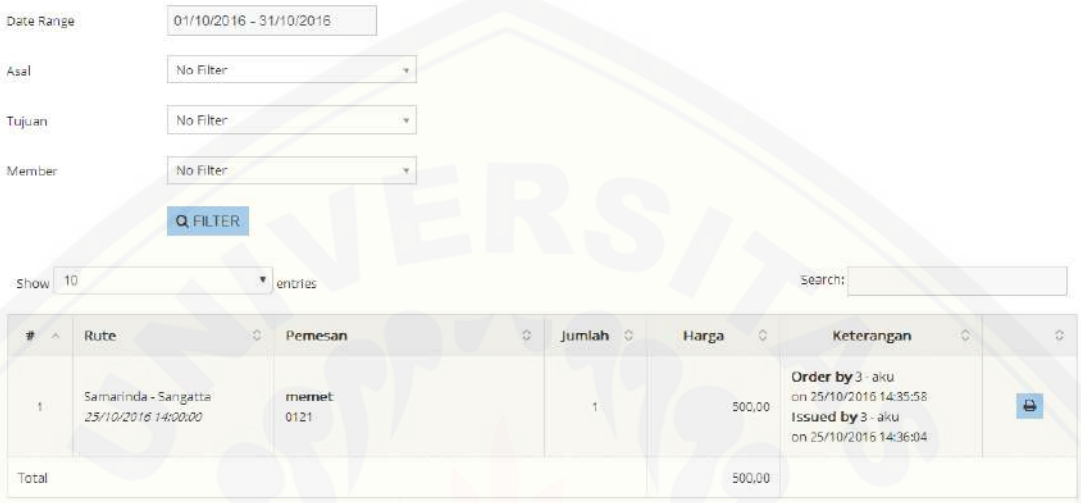
Sub menu *detail* disediakan di menu data saldo dengan cara klik ikon *detail.* Tampilan halaman *detail* bisa dilihat pada gambar 5.22.



Gambar 5.22 Tampilan *detail* data saldo

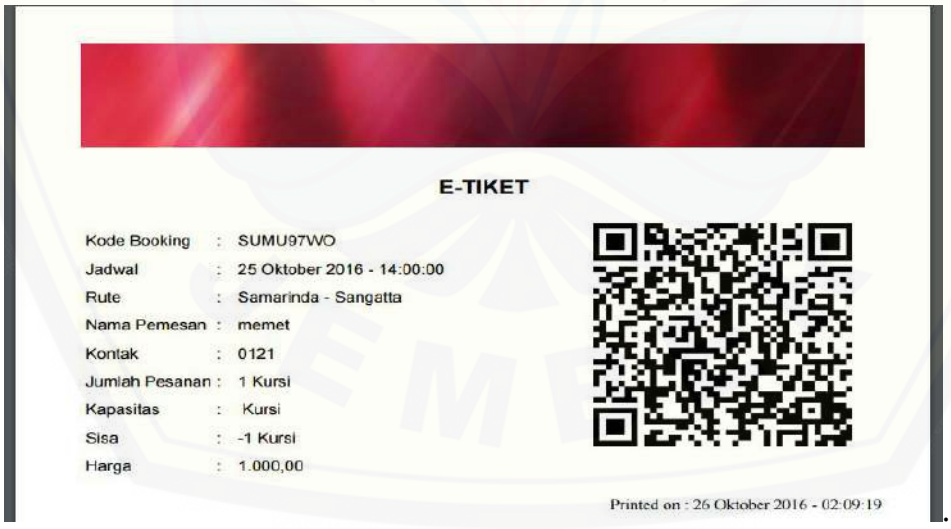
5.1.9 Tampilan Data Laporan

Menu data laporan memiliki sub menu cetak. Tampilan utama data saldo bisa dilihat pada gambar 5.23.



Gambar 5.23 Tampilan utama data laporan

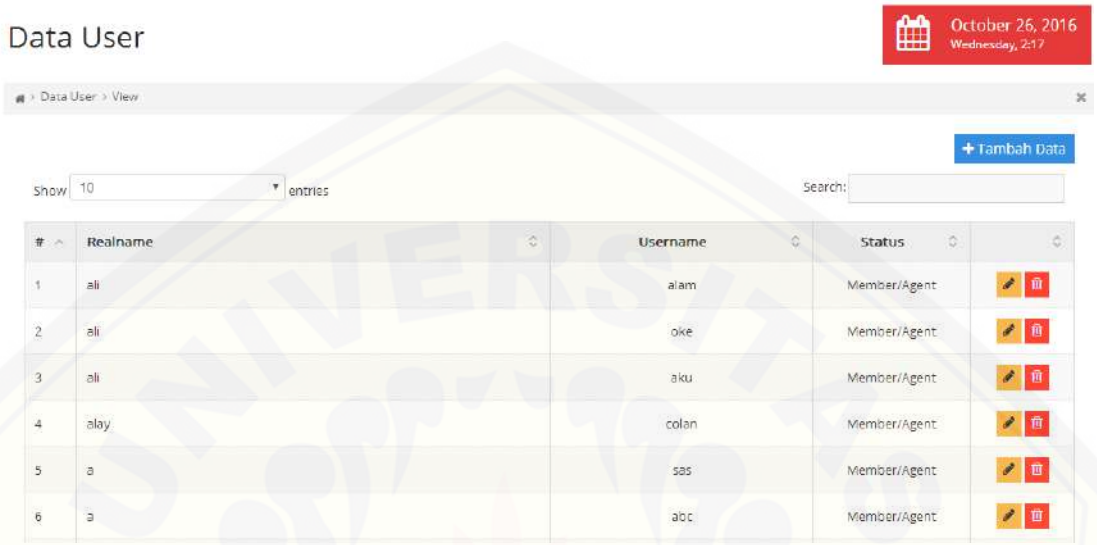
Sub menu cetak tiket disediakan di menu data laporan dengan cara klik ikon cetak. Tampilan halaman cetak bisa dilihat pada gambar 5.24.



Gambar 5.24 Tampilan tiket setelah dicetak

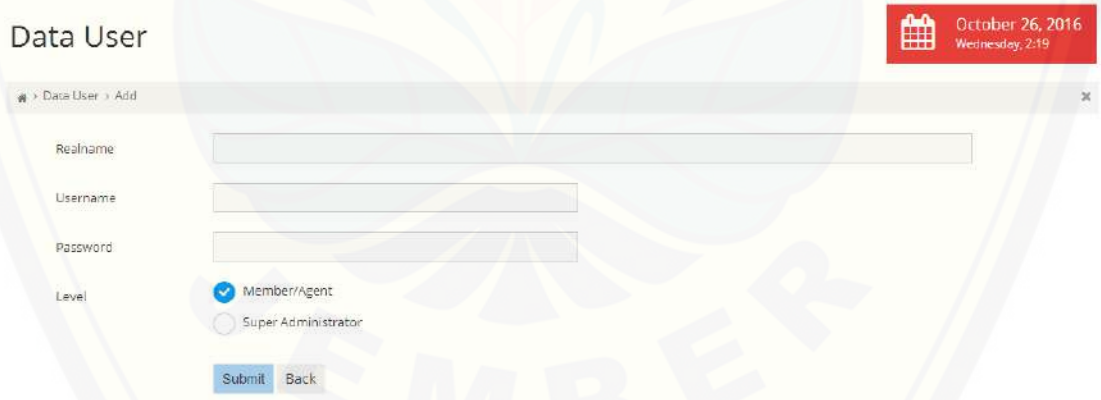
5.1.10 Tampilan Data *User*

Menu data laporan memiliki sub menu tambah data, *edit*, hapus. Tampilan utama data saldo bisa dilihat pada gambar 5.25.



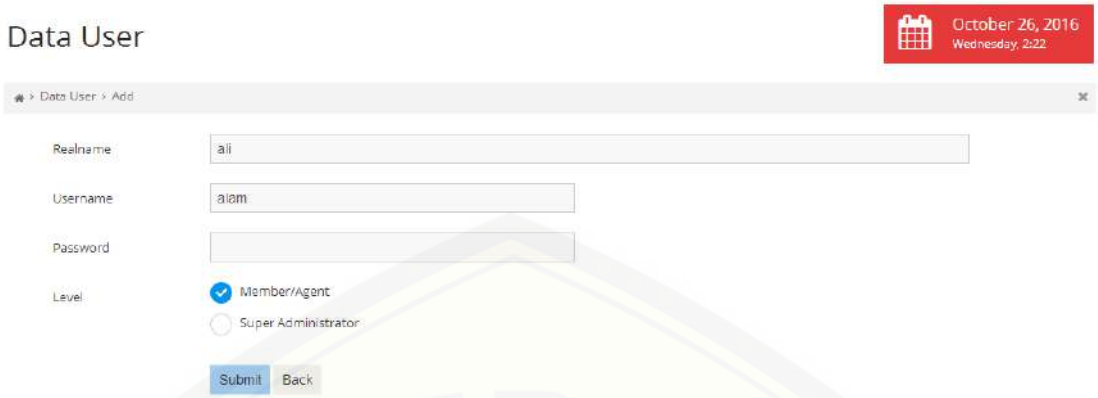
Gambar 5.25 Tampilan utama data *user*

Untuk menambah data *user*, pada menu ini menyediakan *form* tambah data setelah klik tombol tambah data. *Form* tambah data bisa dilihat pada gambar 5.26.



Gambar 5.26 Tampilan tambah data *user*

Sub menu *edit* disediakan di menu data *user* dengan cara klik ikon *edit*. Tampilan halaman *edit* bisa dilihat pada gambar 5.27.



Gambar 5.27 Tampilan *edit* data *user*

Sub menu hapus disediakan di menu data *user* dengan cara klik ikon hapus. Tampilan halaman hapus bisa dilihat pada gambar 5.28.

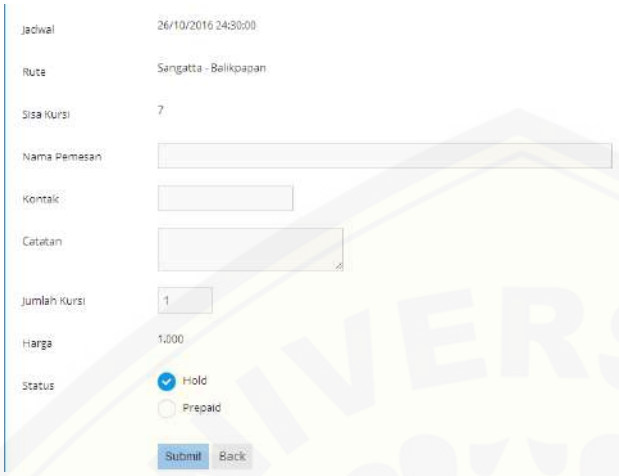
Gambar 5.28 Tampilan hapus data *user*

5.1.11 Tampilan Pesan Travel

Menu data pesan travelmemiliki sub menu pesan dan info. Tampilan utama data saldo bisa dilihat pada gambar 5.29.

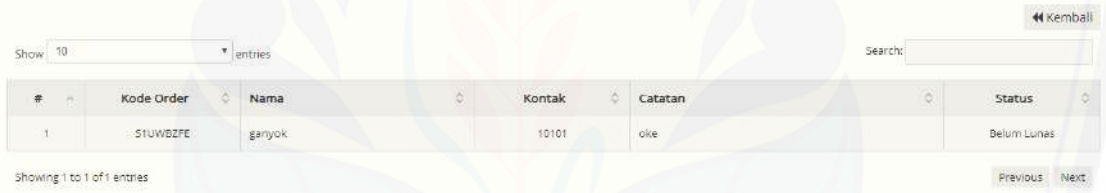
Gambar 5.29 Tampilan utama pesan travel

Sub menu pesan tiket disediakan di menu pesan travel dengan cara klik ikon pesan. Tampilan halaman pesan bisa dilihat pada gambar 5.30.



Gambar 5.30 Tampilan pesan di menu pesan travel

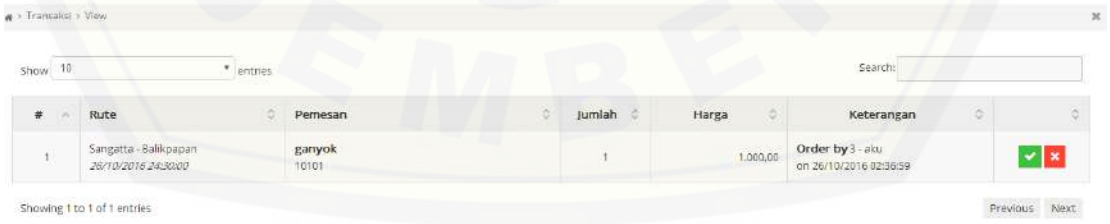
Sub menu info disediakan di menu pesan travel dengan cara klik ikon info. Tampilan halaman pesan bisa dilihat pada gambar 5.31.



Gambar 5.31 Tampilan info di menu pesan travel

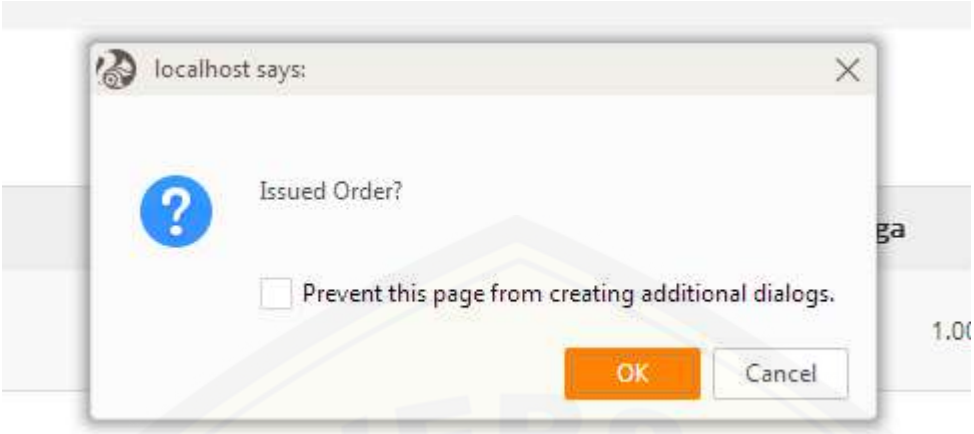
5.1.12 Tampilan Data Pesanan

Menu data pesanan memiliki dua fungsi didalamnya yaitu menyetujui atau membatalkan pesanan. Tampilan utama data pesanan bisa dilihat pada gambar 5.32.



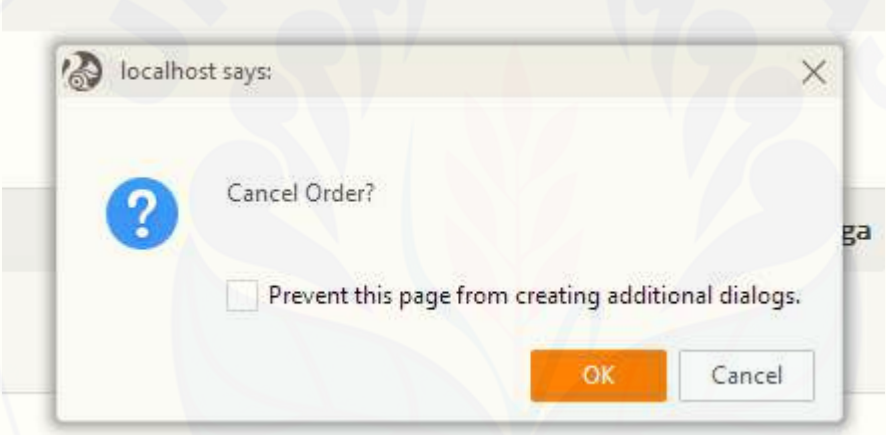
Gambar 5.32 Tampilan utama data pesanan

Fungsi menyetujui pesanan dapat dilihat pada gambar 5.33.



Gambar 5.33 Tampilan fungsi menyetujui pesanan

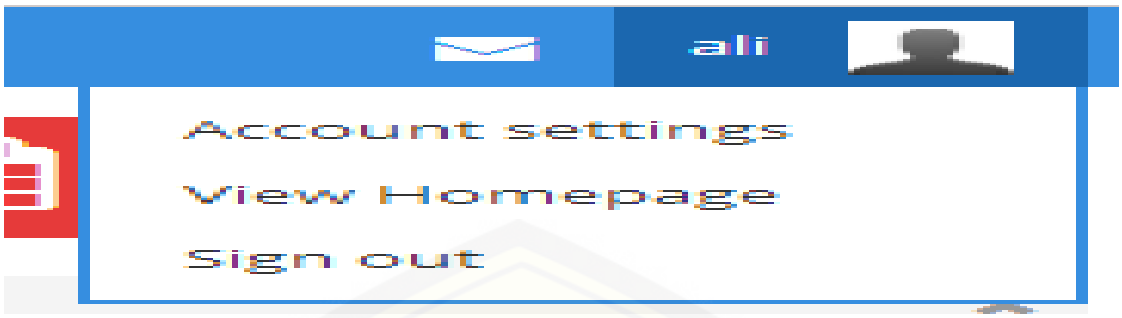
Fungsi menyetujui pesanan dapat dilihat pada gambar 5.34.



Gambar 5.34 Tampilan fungsi membatalkan pesanan

5.1.13 Tampilan *Logout*

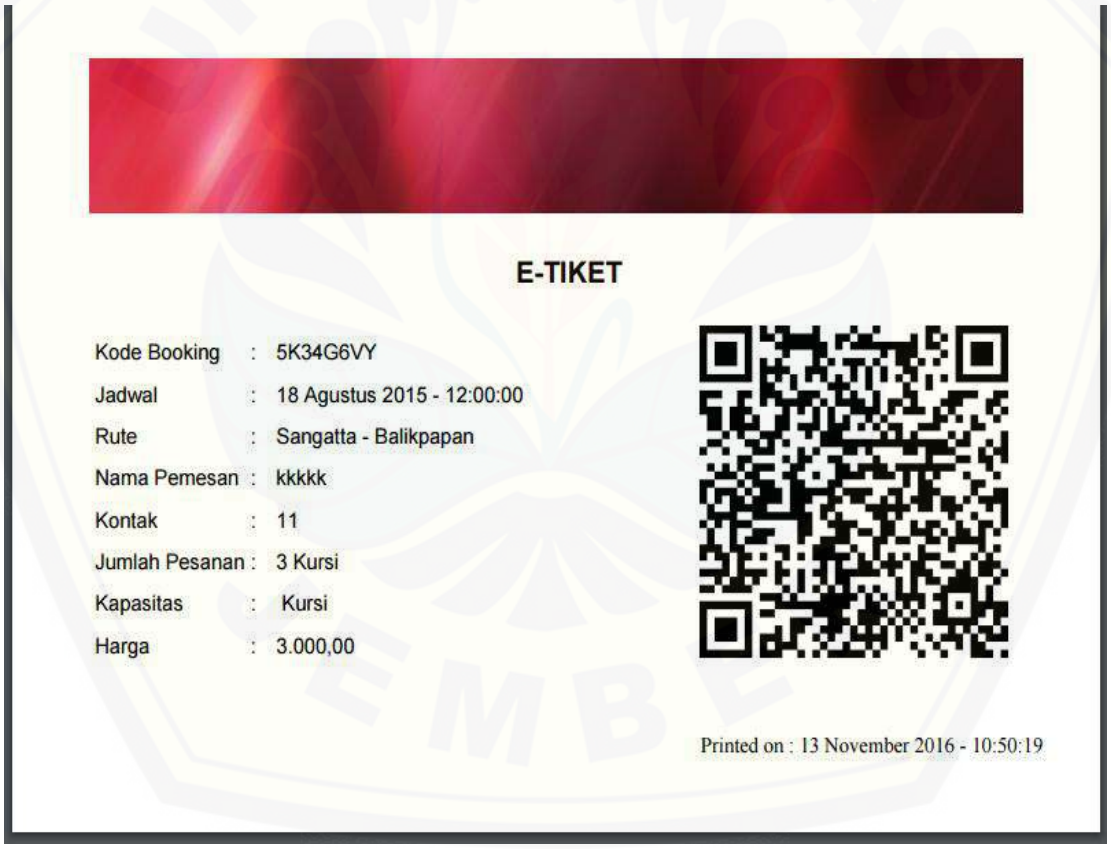
Menu *logout*ketika *user* ingin keluar dari system, tampilan menu *logout* bisa dilihat pada gambar 5.35.



Gambar 5.35 Tampilan menu *logout*

5.2 Hasil Implementasi AES-128 pada Validasi Tiket Pt. Bumindo Jaya Cemerlang

Implementasi AES-128 pada validasi tiket bisa dilihat pada gambar 5.36, yang menampilkan cetak halaman tiket



Gambar 5.36 halaman tiket

Halaman ini akan dihasilkan sebuah kode yang hanya akan bisa dibaca oleh *qr code scanner* berbasis android yang sudah dibuat oleh peneliti. Kode ini berdasarkan pada proses enkripsi yang telah dilakukan oleh sistem. Proses tersebut dapat dilihat pada gambar 5.37

Gambar 5.37 Data telah dienkripsi

Proses enkripsi sendiri terjadi setelah system mencetak tiket, data yang dienkripsi merupakan data yang dicetak menjadi *qr code*. Proses mencetak *qr code* menggunakan *qr code generator*. Berikut akan diberikan gambaran tentang perbedaan antara data yang sudah dienkripsidan yang belum dienkripsi. Gambar 5.38 memperlihatkan *qr code* yang belum di enkripsi

Gambar 5.38 *Qr Code* tidak dienkripsi

Hasil scan dari *qr code* diatas menggunakan aplikasi *packet data sniffer* hasilnya seperti ini :

5K34G6VY;S;Sangatta - Balikpapan;S;18/08/2015 12:00:00;S;kkkkk;S;3;S;3000;S;Lunas

Gambar 5.39 Hasil scan data menggunakan *packet data sniffer* tanpa enkripsi

Perbedaan antara *qr code* yang sudah dienkripsi bisa dilihat pada gambar 5.40.

Gambar 5.40 *Qr Code* dienkripsi

Hasil scan dari *qr code* diatas hasilnya seperti ini menggunakan aplikasi *packet data sniffer*:

```
Vwi+vXvPz+5QgDqQwUAa89bUaKxlxpqM2wRHu0Ua
zxQAuGlVQYDpyZDMcpZ6S9aNql7B5E40u9mlksGmoCxarP6j17seyOa0PiUQ
EyAExe09NKHG8l2ROBfUQ2+Gxpzq
```

Gambar 5.41 Hasil scan menggunakan *packet data sniffer*

Untuk hasil scan dari *qr code* diatas hasilnya seperti ini menggunakan aplikasi *wired shark:*

Gambar 5.42 Hasil scan menggunakan *wired shark*

Peneliti menggunakan aplikasi *qr code reader* dari platform android yang lain untuk membedakan hasil scan dari aplikasi *qr code reader* yang dirancang peneliti.

Hasil scan dari *qr code reader* yang sudah dirancang oleh peneliti bisa dilihat pada gambar 5.43.

Gambar 5.43 Hasil scan tiket

BAB 6 PENUTUP

Bab ini merupakan bagian akhir di dalam penulisan skripsi, berisi tentang kesimpulan dan saran. Kesimpulan yang ditulis merupakan kesimpulan dari hasil penelitian yang telah dilakukan dan saran lanjutan untuk dilakukan pada penelitian selanjutnya.

6.1 Kesimpulan

Kesimpulan dari penelitian yang telah dilakukan adalah sebagai berikut:

1. Aplikasi *qr code reader* yang dibuat mampu menampilkan dan menjaga keaslian data yang dicetak menjadi *qr code* dan hanya bias dibaca oleh *qr code reader* yang dibuat oleh peneliti.
2. Pemanfaatan algoritma AES-128 padaValidasi Tiket Travel Pt. Bumindo Jaya Cemerlang mampu menjaga keaslian tiket travel dengan data tiket tidak bias dibaca oleh *qr code reader* lain.
3. Hasil scan dari data yang belum dienkripsi seperti berikut:

   5K34G6VY;S;Sangatta - Balikpapan;S;18/08/2015 12:00:00;S;kkkkk;S;3;S;3000;S;Lunas

4. Hasil scan dari data yang sudah dienkripsi seperti berikut:

   Vwi+vXvPz+5QgDqQwUAa89bUaKxlxpqM2wRHu0Ua
   zxQAuGlVQYDpyZDMcpZ6S9aNqI7B5E40u9mlksGmoCxarP6j17seyOa0PiUQ
   EyAExe09NKHG8I2ROBfUQ2+Gxpzq

6.2 Saran

Pengembangan lebih lanjut untuk penelitian ini dapat dilakukan dengan membangun *interface* program yang lebih menarik dandisarankan menggunakan metode kriptografi lainnya untuk menciptakan perbandingan antar metode yang satu dengan yang lain.

DAFTAR PUSTAKA

Bokhari, M., Alam, S., & Masoodi, F. S. (2012). Cryptanalysis Techniques for Stream Cipher: A Survey. *International Journal of Computer Applications*.

Firmansyah, M. N., & Kadarsetia, E. (2010). PENYELIDIKAN POTENSI BANJIR BANDANG DI KABUPATEN JEMBER. 1-9.

Lusiana, V. (2011). Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma AES-128. *Jurnal Dinamika Informatika Vol.3 No.2*.

Mangiwa, S., & Wicaksana, I. W. (2008). Membandingkan Model-Model Pengembangan Database. *Seminar Ilmiah Nasional Komputer dan Sistem Intelijen*.

Meimaharani, R., & Laily, D. (2014). E-Commerce Goody Bag Spunbond Menggunakan QR Code Berbasis Web Responsif. *Jurnal SIMETRIS, Vol 5 No 2*.

Novandi, R. A. (2007). Perbandingan Algortima Dijkstra dan Algoritma Floyd-warshall dalam Penentuan LIntasan Terpendek (Single Pair Shortest Path) . *MAKALAH IF2251 STRATEGI ALGORITMIK*, 3.

Nurdiansyah, Y., Istiyadi, D., & I, R. E. (2014). Implementasi Algoritma AES-128 pada Mobile Learning Universitas Jember. *Konferensi Nasional Ilmu Komputer*, 400-403.

Nuur, S., & Rahman, F. (2013). *Analisis dan Perancangan Program Apliksai Music Player dengan Menggunakan Metode Kriptografi 3DES.* 2013: Universitas Bina Nusantara.

Pasca Nugraha, M., & Munir, R. (2011). Pengembangan Aplikasi QR Code Generator dan QR Code Reader dari Data Berbentuk Image. *Konferensi Nasional Informatika*.

R12K4. (2008). R12K4. Retrieved February 20, 2016,http://r12k4.wordpress.com/

Raharjo, B. (1999). *Keamanan Sistem Infomrasi Berbasis Internet.* Bandung: Pt. Insan Komunikasi.

Rahayu, Y. D., Nana Ramadijanti, S. M., & Yuliana Setiowati, S. M. (2010). Pembuatan Aplikasi Pembacaan Quick Response Code Menggunakan Perangkat Mobile Berbasis J2ME untuk identifikasi Barang.

Scheiner, B. (1996). *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C.* New York: Wiley Computer Publishing, John Wiley & Sons, Inc.

Surian, Didi (2006) ALGORITMA KRIPTOGRAFI AES RIJNDAEL