Volume 10 Number 2 November 2020 Page. 43-52
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i2

Article DOI : 10.36350/jbs.v10i2.87
Received: October; Accepted : October; Published : November

Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket

Adiat Pariddudin[1*], Fatih Syauqi[2]
[1]STIKOM Binaniaga/Sistem Informasi
Email: adiat@stikombinaniaga.ac.id
[2] STIKOM Binaniaga/Teknik Informatika
Email: fatih.blogger@yahoo.com

ABSTRAK

Tiket merupakan suatu dokumen yang sangat penting dalam suatu acara (event travel) karena tiket menentukan apakah seseorang memiliki akses untuk memasuki acara tersebut atau tidak. Kesederhanaan sistem verifikasi tiket online ini, banyak disalahgunakan untuk mendapatkan akses masuk ke dalam acara dengan bebas. Tidak adanya proses identifikasi dan validasi tiket pada data yang dimiliki oleh penyelengara acara membuat kecurangan dapat terjadi setiap saat. Dari permasalahan yang ada, maka dilakukan penelitian dengan memanfaatkan QR code dan menggunakan Algoritma Kriptografi AES (Advanced Encryption Standard) sebagai tiket masuk event dengan memperhitungkan tingkat koreksi kesalahan. Dan memperbaharui sistem verifikasi tiket dengan sistem komputerisasi dengan mengganti bentuk fisik tiket menjadi QR code dan menerapkan Algoritma AES. Dengan menggunakan Aplikasi Verifikasi Pemesanan Tiket yang mengamankan data tiket, untuk mengurangi resiko penggandaan tiket karena tiket di enkripsi oleh algoritma AES dan setiap waktu yang sudah ditentukan kode tiket selalu berubah setiap 60 detik menjadikan duplikasi tiket tidak dapat dilakukan.

Kata kunci*: QR code; Algoritma; Kriptografi; AES; Advanced Encryption Standard.*

A. PENDAHULUAN

PT. Wisata Murah Indonesia merupakan salah satu perusahaan yang bergerak di bidang layanan travel di Jakarta Timur. Sesuai dengan namanya PT. Wisata Murah Indonesia yang menyediakan pilihan paket wisata yaitu wisata domestik dan wisata internasional. Dalam kegiatan travel tentu saja tidak asing dengan yang nama nya tiket. Tiket merupakan sebuah alat bukti apakah seseorang dapat mengikuti kegiatan travel atau tidak.

Saat ini tiket hanya dapat di pesan melalui website atau datang ke kantor dengan cara mengisi data diri serta melengkapi dokumen penting yang di perlukan, lalu calon pemesan memilih paket yang telah di sediakan oleh PT. Wisata Murah Indonesia dan memilih tanggal keberangkatan yang diinginkan, setelah itu pihak kantor akan mengirimkan invoice kepada email calon pemesan, kemudian calon pemesan tiket melakukan transfer dengan jumlah yang telah tercantum pada invoice, setelah pembayaran diterima dan diverifikasi maka calon pemesan akan mendapatkan sebuah tiket yang akan dikirim ke email calon pemesan.

Volume 10 Number 2 November 2020 Page. 43-52
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i2

Namun dalam kondisi tersebut, tiket yang telah dibuat, masih belum memiliki penyimpanan pada basis data sebagai alat penyimpan seluruh berkas tiket, hal ini dapat menyebabkan kerugian dalam segi keamanan data maupun proses verifikasi tiket yang belum dapat mengetahui apakah tiket tersebut (asli) sah atau (palsu) tidak sah, sehingga pihak yang tidak berwenang dapat membuat ulang secara bebas.

Tidak adanya keamanan pada identitas tiket dapat berpengaruh terhadap penjualan tiket, dengan cara menggandakan atau menduplikasi tiket, hal ini dapat menyebabkan kerugian dari penjualan tiket.

Penerapan Algoritma Kriptografi AES (Advanced Encryption Standard) pada QR-Code sebagai tiket, dapat digunakan untuk menyelesaikan masalah tersebut. Sehingga petugas dapat melakukan proses verifikasi tiket lebih cepat dan lebih mudah. Dengan adanya data yang telah terenkripsi oleh Algoritma AES pada QR-Code. Tiket wisata yang sekarang menggunakan kertas maupun hologram, dapat diganti dengan tiket yang berbentuk QR-Code. Hal ini dapat mengurangi biaya produksi dalam pembuatan tiket, sebagai keuntungan lebih untuk PT. Wisata Murah Indonesia.

1. Latar Belakang

Dalam verifikasi dan pembuatan tiket dengan Algoritma AES dan QR-CODE Hal ini membuat peneliti berpikir untuk melakukan penelitian untuk membuat aplikasi dengan menggunakan metode Algoritma AES pada QR-CODE. Aplikasi Mobile akan mempermudah petugas tiket untuk memverifikasi tiket.

2. Permasalahan

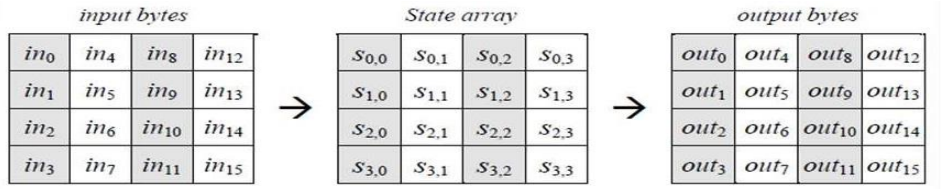
Proses pembuatan dan verifikasi tiket di PT. Wisata Murah Indonesia belum memiliki sistem. Sehingga Terjadinya ketidak sesuaian informasi tiket antara data tiket yang telah di pesan oleh pelanggan dengan data yang di miliki PT. Wisata Murah Indonesia, dan pelanggan tidak memiliki layanan untuk melihat informasi secara berkala terhadap data tiket yang telah di pesan secara langsung.

3. Tujuan

Menerapkan Algoritma Advanced Encryption Standard (AES) pada QR Code untuk keamanan identitas tiket yang telah terjual dan memudahkan petugas tiket dalam memverifikasi tiket.

4. Tinjauan Pustaka / Landasan Teori

Operasi AES dilakukan terhadap array of byte dua dimensi yang disebut dengan state. State mempunyai ukuran NROWS X NCOLS. Pada awal enkripsi, data masukan yang berupa in0, in2, in3, in4, in5, in6, in7, in8, in9, in10, in11, in12, in13, in14, in15 disalin ke dalam array state. State inilah yang nantinya dilakukan operasi enkripsi / dekripsi. Kemudian keluarannya akan ditampung ke dalam array out. Proses disajikan pada Gambar 1. Proses Input Bytes, State Array, dan Output Bytes.



Gambar 1. Proses Input Bytes, State Array, dan Output Bytes

Gambar 1. Proses Input Bytes, State Array, dan Output Bytes mendefinisikan pada saat permulaan, input bit pertama kali akan disusun menjadi suatu array byte dimana panjang dari array byte yang digunakan pada AES adalah sepanjang 8 bit data. Array byte inilah yang nantinya akan dimasukkan atau dicopy ke dalam state dengan urutan dimana r (row / baris)

Volume 10 Number 2 November 2020 Page. 43-52
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i2

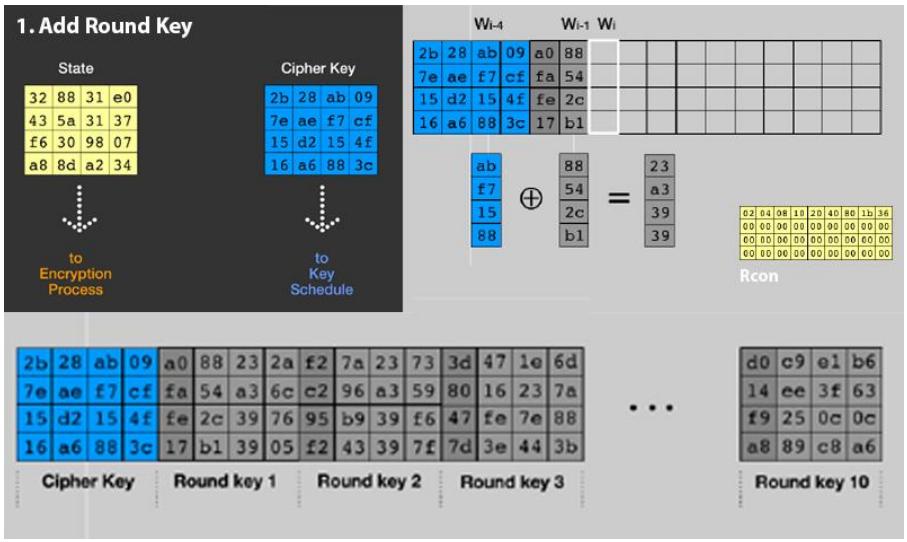
dan c (column/kolom) : s[r,c] = in[r+4c] untuk $0 \leq r < 4$ dan $0 \leq c < Nb$ sedangkan dari state akan dicopy ke output dengan urutan : out[r+4c] = s[r,c] untuk $0 \leq r < 4$ dan $0 \leq c < Nb$..

B. METODE

Enkripsi algoritma AES di mulai dengan memasukan XOR plainteks/state yang akan di enkripsi dengan roundkey, setelah selesai melakukan XOR plainteks dengan roundkey. Kita lakukan subtitusi dengan s-Box, Setelah itu hasil dari subtitusi dengan s-Box selesai. Kita lakukan siftrow. Setelah hasil shiftrow didapat, maka langkah selanjutnya yaitu melakukan Mix Columns dengan mengalikan matrik Setelah perhitungan Mix Column selesai maka kita melakukan addround key. Yaitu melakukan XOR state dengan round key. Lakukan sampai literasi 10, namun pada saat putaran/literasi yang ke 10, setelah step shiftrow lompati step Mix Colums dan langsung lanjut melakukan XOR hasil state saat shift row dengan round key.

1. Proses Enkripsi - Input State Dan Chiper Key

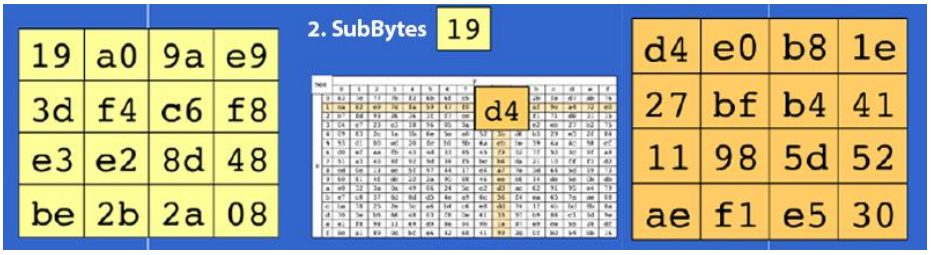
Gambar 2. Proses Enkripsi Algoritma AES – Input mendefinisikan Round key ditambahkan pada state dengan operasi XOR. Setiap round key terdiri dari Nb word dimana tiap word tersebut akan dijumlahkan dengan word atau kolom yang bersesuaian dari state.



Gambar 2. Proses Enkripsi Algoritma AES – Input

2. Proses Enkripsi – Subbytes

Gambar 3. Ilustrasi Proses Enkripsi Algoritma AES – SubBytes mendefinikan Prinsip dari Sub Bytes adalah menukar isi matriks atau tabel yang ada dengan matriks atau tabel lain yang disebut dengan Rijndael S-Box.

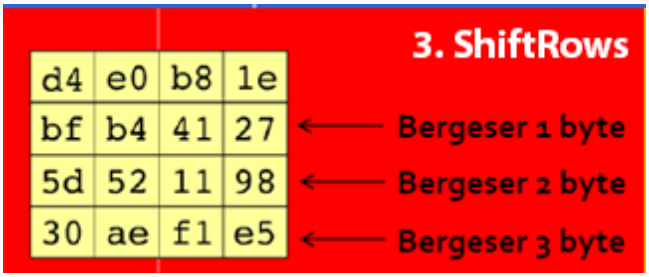


Gambar 3. Ilustrasi Proses Enkripsi Algoritma AES – SubBytes

3. Proses Enkripsi – Shiftrows

Gambar 4. Ilustrasi Proses Enkripsi Algoritma AES – ShiftRows mendefinisikan tentang Shift Rows seperti namanya adalah sebuah proses yang melakukan shift atau pergeseran pada setiap elemen blok/tabel yang dilakukan per barisnya.

Volume 10 Number 2 November 2020 Page. 43-52
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i2



Gambar 4. Ilustrasi Proses Enkripsi Algoritma AES – ShiftRows

4. Proses Enkripsi – Mixcolumns

Gambar 5. Ilustrasi Proses Enkripsi Algoritma AES – MixColumns mendefinisikan tentang Mix Column adalah mengalikan tiap elemen dari blok chiper dengan matriks. Pengalian dilakukan seperti perkalian matriks biasa yaitu menggunakan dot product lalu perkalian keduanya dimasukkan ke dalam sebuah blok chiper baru.

Gambar 5. Ilustrasi Proses Enkripsi Algoritma AES – MixColumns

5. Proses Enkripsi – Mixcolumns

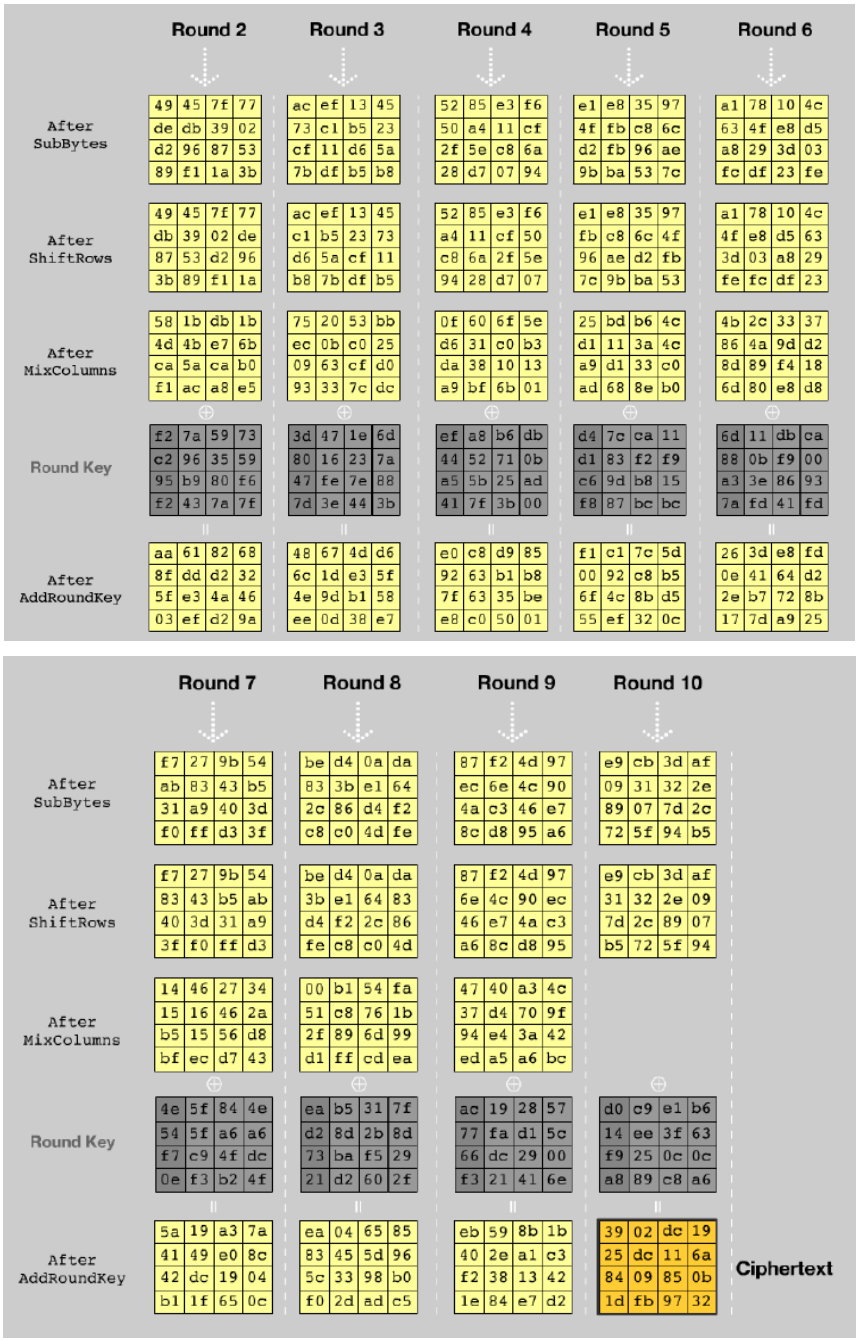
Gambar 6. Ilustrasi Proses Enkripsi Algoritma AES – Add RoundKey mendefinisikan Add Round Key pada dasarnya adalah mengkombinasikan chiper teks yang sudah ada dengan chiper key yang chiper key dengan hubungan XOR.

Gambar 6. Ilustrasi Proses Enkripsi Algoritma AES – Add RoundKey

6. Hasil Enkripsi Algoritma Aes

Gambar 7. Hasil Enkripsi Algoritma AES mendefinisikan proses enskripsi dari tahap awal sampai akhir yang menggunakan byte sebagai gambaran ilustrasi.

Volume 10 Number 2 November 2020 Page. 43-52
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i2

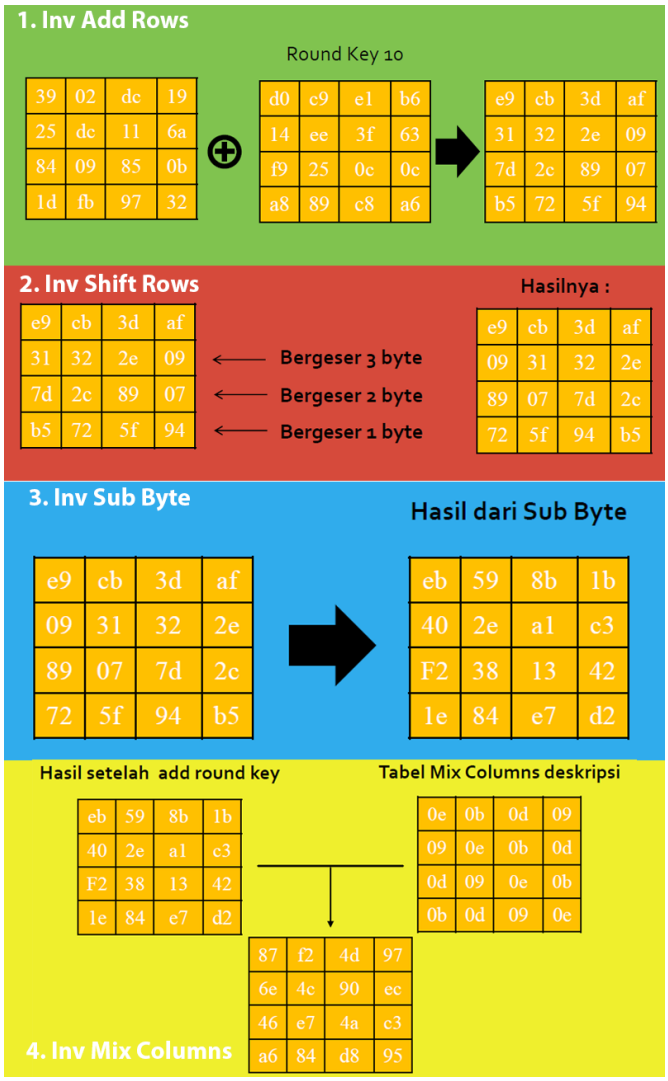


Gambar 7. Hasil Enkripsi Algoritma AES

7. Proses Dekripsi Algoritma AES

Gambar 8. Proses Dekripsi Algoritma AES mendefinisikan proses dekripsi algoritma AES di mulai dengan melakukan XOR chipertext dengan Add Rows setelah itu lakukan Inv ShiftRows dan Inv SubByte kemudian Tranformasi InvMixColumns sama dengan MixColumns, dimana perbedaannya adalah a(x) yang digunakan adalah inversnya (a-1).

Volume 10 Number 2 November 2020 Page. 43-52
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i2



Gambar 8. Proses Dekripsi Algoritma AES

C. HASIL DAN PEMBAHASAN

1. HASIL

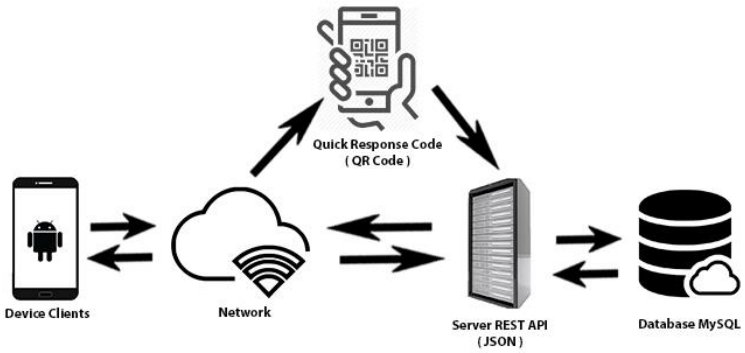
Hasil dari penerepan QR-CODE dan algoritma Advanced Encryption Standard (AES) pada sistem pemesanan tiket yaitu detil informasi tiket dari kode tiket, halaman detil informasi tiket yang berisi informasi kode tiket, nama paket yang telah di pesan, tanggal tour, durasi paket, nama pelanggan, status verifikasi tiket dan QR Code. Data tersebut telah di enkripsi dengan Algoritma AES 256bit dan QR Code yang akan berubah setiap menit sekali, disajikan pada Gambar 9. Tampilan Detil Informasi Tiket.

Volume 10 Number 2 November 2020 Page. 43-52
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i2

Gambar 9. Tampilan Detil Informasi Tiket

2. PEMBAHASAN

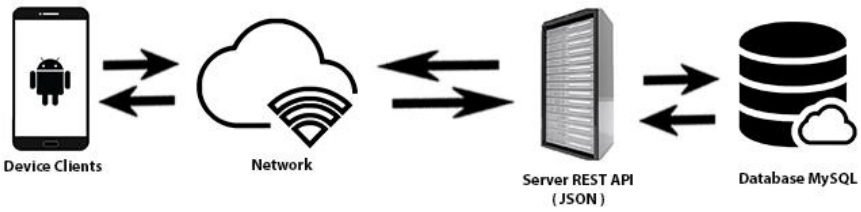
Metode Algoritma AES pada QR CODE diterapkan pada smartphone. Dengan penerapan algoritma AES pada QR Code, proses awal di lakukan oleh petugas dengan mengakses sistem menggunakan aplikasi yang telah ter-instal pada smartphone, sebelum menjalankan aplikasi petugas harus meng-aktifkan koneksi internet terlebih dahulu agar dapat terhubung dengan server rest api (json), setelah mengaktifkan koneksi internet petugas dapat melakukan verifikasi tiket dengan cara memindai / scanning QR Code pada tiket yang berisi kombinasi kode tiket dan waktu yang telah di enkripsi dengan menggunakan Algoritma AES, jika QR Code terbaca oleh sistem, maka sistem akan otomatis melakukan pengecekan pada database melalui layanan web service atau rest api, jika kode tiket dan waktu yang di kirim melalui web service cocok dengan data pada database, maka sistem akan memberikan respon balik untuk melakukan update status tiket pelanggan menjadi telah ter-verifikasi. Proses Arsitektur disajikan pada Gambar 10. Arsitektur Proses Verifikasi Tiket.



Gambar 10. Arsitektur Proses Verifikasi Tiket

Volume 10 Number 2 November 2020 Page. 43-52
Journal Homepage : http://teknois.stikombinaniaga.ac.id/index.php/JBS
DOI Link : http://doi.org/10.36350/jbs.v10i2

Gambar 11. Arsitektur Proses Pembuatan Tiket mendefinisikan pelanggan dapat diketahui bahwa proses awal di lakukan dengan mengakses sistem menggunakan aplikasi yang telah ter-instal pada smartphone, sebelum menjalankan aplikasi pengguna dan pelanggan harus meng-aktifkan koneksi internet terlebih dahulu agar dapat terhubung dengan server rest api (json), setelah mengaktifkan koneksi internet pengguna akan di minta untuk login atau daftar terlebih dahulu untuk dapat melakukan pemesanan paket dan tiket.



Gambar 11. Arsitektur Proses Pembuatan Tiket

Gambar 12. Pengkodean Proses Enkripsi AES 256bit merupakan pengkodean proses enkripsi aes dengan berisi kombinasi tanggal, jam dan no urut tiket di mulai dari plaintext identitas tiket selanjut nya plaintext akan di enkripsi menggunakan algoritma aes 256bit dengan metode aes-256-cbc dan password yang telah di hash sha256 setelah itu di enkripsi kembali dengan enkripsi base64 dan hasilnya menjadi chipertext yang tidak dapat dibaca.

```php
<?php
  $IdTicket =  $dateticket.$timeticket.$no_urut_now;
  $plaintext = $IdTicket;
  $password = 'WISATAMURAHINDONESIA';
  $method = 'aes-256-cbc';
  $key = substr(hash('sha256', $password, true), 0, 32);
  $iv = chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) .
chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0);
  $encrypted = base64_encode(openssl_encrypt($plaintext, $method, $key, OPENSSL_RAW_DATA, $iv));
?>
```

Gambar 12. Pengkodean Proses Enkripsi AES 256bit

Hasil dari proses enkripsi algoritma AES dan base 64 pada Gambar 5 yaitu:

Plaintext: 2019122309545401

Chipertext: dG7ThqT8rHWJ764y+iYIGQ==

Gambar 13. Pengkodean Proses Dekripsi AES mendefinikan tentang pengkodean proses dekripsi aes dari chipertext dan akan dapat dibaca dengan proses dekripsi dari chipertext menjadi plaintext dengan proses dimulai dari dekripsi base64 dan selanjutnya dekripsi menggunakan algoritma aes 256 dengan metode aes-256-cbc dan password yang telah di hash sha256 dan hasil nya menjadi plaintext yang dapat dibaca kembali.

```php
<?php
  $KodeReferensi = $_REQUEST['kode_referensi'];
  $password = 'WISATAMURAHINDONESIA';
  $method = 'aes-256-cbc';
  $key = substr(hash('sha256', $password, true), 0, 32);
  $iv = chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) .
chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0);
  $decrypted = openssl_decrypt(base64_decode($KodeReferensi), $method, $key, OPENSSL_RAW_DATA, $iv);
?>
```

Gambar 13. Pengkodean Proses Dekripsi AES

D. KESIMPULAN

Berdasarkan hasil penelitian yang telah diuraikan, maka kesimpulan yaitu:

1. Dengan menerapkan Algoritma Andvanced Encryption Standard (AES) pada Quick Response Code (QR Code), sistem dapat mengamankan identitas tiket dari penjualan ulang tiket dan manipulasi data tiket dari pihak yang tidak berwenang.

2. Tersedianya sistem untuk melihat informasi tiket yang dapat di akses langsung oleh pelanggan dengan menggunakan teknologi QR Code secara real time.

E. DAFTAR RUJUKAN

[1] Aditia Rahmat Tulloh(1), Yurika Permanasari(2), Erwin Harahap(3), Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen, Jurnal Matematika UNISBA, Vol 15 No 1, Mei 2016.

[2] Agus, Sutarom, 2016. Enkripsi dan Dekripsi Gambar Menggunakan Algoritma Advanced Encription Standard (AES) Pada Pemrograman PHP, Jurnal Ilmiah Mahasiswa, (1): 1-11

[3] Arikunto Suharsimi. 2005. Manajemen Penelitian, edisi Revisi. Jakarta : Rineka Cipta.

[4] Edwin Fajar Nurdiansyah (1), Irawan Afrianto (2), Implementasi QR CODE Sebagai Tiket Masuk Event Dengan Memperhitungkan Tingkat Koreksi Kesalahan, Teknik Informatika, Universitas Komputer Indonesia

[5] Febrianto Rama Anji, Saiful Bukhori, Yanuar Nurdiansyah, 2015. Rancang Bangun Aplikasi Verifikasi Pemesanan Tiket Dengan QR-Code Berbasis Android Menggunakan Algoritma Kriptografi Asimetris RSA, Jurnal Ilmiah Mahasiswa, (1): 1-6

[6] Ghaniy, Rajib. "Analisis Penerimaan User terhadap Penerapan Sistem Reservasi Tiketing Bus Antar Kota Antar Provinsi dengan Menggunakan SMS." *Teknois*, vol. 6, no. 1, May. 2016, pp. 38-50, doi:10.36350/jbs.v6i1.46.

[7] Mita Pramihapsari, Perancangan Labelling pada Dokumen Menggunakan QR Code, 1-7

[8] Munir, R. 2004. Advanced Encryption Standard (AES). Bandung: Institut Teknologi Bandung

[9] Munir, R. 2004. Sistem Kriptografi Kunci-Publik. Bandung: Institut Teknologi Bandung

[10] Riduwan (2005). Belajar Mudah Penelitian Untuk Guru, Karyawan dan Peneliti Pemula, Bandung :alfabeta.

[11] Risnita (2012). Pengembangan Model Skala Likert.

[12] Rizal Loa Wanda “Pengertian Prototyping Model”. http://rizalloa.ilearning.me/?p=132#

[13] Roger S. Pressman 2005. Software Engineering Fifth Edition.

[14] Sadikin, Rifki. Kriptografi Untuk Keamanan Jaringan. Yogyakarta: Penerbit Andi. 2012.

[15] Spengetahuan (2015) “Pengertian Instrumen Penelitian Menurut Para Ahli”. https://www.spengetahuan.com/2015/11/pengertian-instrumen-penelitian-menurut-para-ahli-jenisnya.html.

[16] Sugiyono (2010). Statistika untuk Penelitian, Bandung: Alfabeta.

[17] Tulach, Jaroslav. 2008. Practical API Design: Confessions of a Java™ Framework Architect. Apress, United States of America

[18] Voni Yuaniati(1), Gani Indriyanta(2), Antonius Rachmat C(3), Enkripsi dan Dekripsi Dengan Algoritma AES 256 Untuk Semua Jenis File, Jurnal Informatika,Volume 5 Nomor 1, April 2009

[19] Wicaksana, Binanda, and Ma'mun Setiawan. "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Pengamanan Berkas Soal Ujian" Teknois, vol. 10, no. 1, May. 2020, pp. 25-34, doi:10.36350/jbs.v10i1.74.

[20] Yusaindera (2017) "Pengertian Application Programming". http://www.yusaindera.com/2017/03/pengertian-application-programming.html#.