APLIKASI PENGAMANAN DATA DENGAN ALGORITMA KRIPTOGRAFI AES 256 BERBASIS *REST API*

Bayu Mahdhani[1)], Siswanto[2)]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1.2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : bayumadhani@rocketmail.com[1)], siswanto@budiluhur.ac.id[2)]

ABSTRAK

Application Programming Interface (API) merupakan antarmuka yang dibangun oleh pengembang sistem supaya sebagian atau keseluruhan fungsi sistem dapat diakses secara programmatis. Sementara Representational State Transfer (REST) merupakan salah satu gaya arsitektur dari pengembangan API yang menggunakan Hypertext Transfer Protocol (HTTP) dalam melakukan komunikasi data. Penelitian ini mengimplementasikan gaya arsitektur REST dalam pengembangan API sebagai, back-end sistem informasi PT Balticindo Jaya Food. dikembangkan menggunakan Javascript Object Notation (JSON) sebagai standar format dalam komunikasi data serta JSON Web Token (JWT) sebagai kode otentikasi.Untuk menjaga kemanan pertukaran data agar data yang di request hanya dapat dibaca oleh user yang mempunyai hak , maka data yang diminta user akan dienkripsi sesuai access token user dengan menggunakan metode kriptografi AES 256 (Advance Encryption System).). Penggunaan sistem kriptografi ini dimaksudkan agar data tersebut tidak mudah disadap. Hasil dari pengujian kriptografi ini, data dapat diamankan untuk menghindari serangan cryptanalysis. Hanya saja Aplikasi Client harus melakukan dua kali request untuk melakukan enkripsi dan dekripsi data sebelum data tersebut disajikan.

Kata Kunci : *REST API*, *Android*, Kriptografi,*AES*

1. PENDAHULUAN

PT. Balticindo Jaya Food adalah perusahaan yang bergerak di bidang food delivery yang dimana pemasaran nya dilakukan oleh telemarketing , dengan cara menghubungi kustomer yang ada di *database*.Data yang ada di *database* tidak langsung dapat diolah oleh telemarketing karna data tersebut harus dipilih sesuai kepemilikan telemarketing ,kemudian hasil data yang bisa dipilih baru bisa bisa di print untuk diserahkan terhadap telemarketing yang bersangkutan.

Dikarenakan sulitnya proses yang ada bagi marketing untuk mendapatkan data kustomer , maka semua data marketing harus dipindahkan ke penyimpanan online yang dapat diakses secara *realtime* dan dapat diakses melalu aplikasi yang dipasang di setiap *handphone* telemarketing agar dapat memudahkan telemarketing mengakses data.

Demi keamanan data setiap telemarketing di PT.Balticindo Jaya Food dan untuk memastikan data yang telah ditentukan hanya dapat diakses oleh telemarketing yang memiliki hak nya, maka salah satu cara yang harus dilakukan adalah dengan melakukan *encrypt* pada data yang akan diakses sehingga hanya pihak yang berhak atas data tersebut yang memiliki kunci untuk membuka data. Salah satu alternatif yang dapat digunakan untuk menjaga kerahasiaan informasi tersebut adalah dengan menyamarkannya menjadi bentuk tersandi yang tidak bermakna.

Arsitektur *REST* yang decoupled (terpisah) serta beban komunikasi yang ringan antara produsen dan konsumen membuatnya populer di dunia *cloud-based API*. layanan berbasis *web* yang menggunakan arsitektur *REST* semacam itu dinamakan *REST ful APIs*..

Keamanan *database* tidak hanya berkenaan dengan data yang ada pada *database* saja, tetapi juga meliputi bagian lain dari *system database*, yang tentunya dapat mempengaruhi *database* tersebut. Hal ini berarti keamanan *database* mencakup perangkat keras, perangkat lunak, orang dan data.

Agar memiliki suatu keamanan yang efektif dibutuhkan kontrol yang tepat. Seseorang yang mempunyai hak untuk mengontrol dan mengatur *database* biasanya disebut *Administrator database*. Seorang *Administrator* lah yang memegang peranan penting pada suatu *system database*, oleh karena itu *Administrator* harus mempunyai kemampuan dan pengetahuan yang cukup agar dapat mengatur suatu

system database Keamanan merupakan suatu proteksi terhadap pengrusakan data dan pemakaian data oleh pemakai yang tidak punya kewenangan.
Menurut Data Security Handbook (2008), ancaman keamanan data dapat dibagi menjadi 2 yaitu *Technical Threat* dan *Administrative* and *Physical Threat*.Yang termasuk *technical threat* adalah : serangan virus, *worm, trojan horses, botnets.*
Pada 2006, AES 256 merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik.

2. METODE PENELITIAN

Metode penellitian yang digunakan dalam penelitian ini, langkah-langkah sebagai berikut::

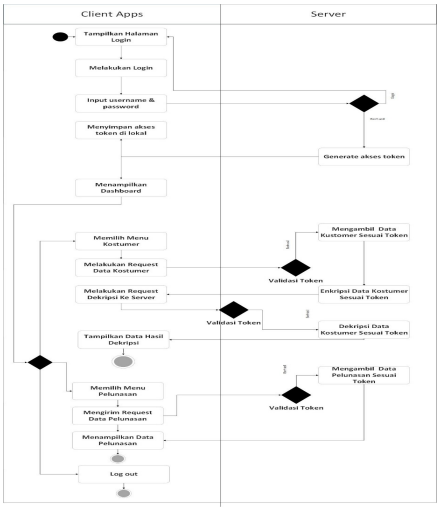
a. Analisa Kebutuhan dilakukan dengan penelitian langsung ke *PT Balticindo Jaya Food.* yang diteliti untuk mendapatkan data dan informasi yang harus diamankan serta masalah yang sering terjadi selam proses transfer file yang berisikan data penting.
b. Mempelajari cara kerja algoritma AES-256 dan Base64.
c. Mendesain serta memodelkan algoritma dan user interface aplikasi pengamanan data yang akan digunakan untuk mengamankan data.
d. Membuat program dengan bahasa pemrograman *Javascript Object Notation (JSON).*
e. Ujicoba Program dengan mencoba panjang pesan chat yang kecil dan yang besar ukuran pesannya.

3.HASIL DAN PEMBAHASAN

3.1 Skema Proses Aplikasi

Aplikasi ini dibuat oleh penulis, dan pada Penelitian ini adalah aplikasi yang telah dibuat berbasis *client server*, yang telah dikembangkan oleh bahasa pemrograman *php* untuk *server* dan *android* sebagai *client*. Berikut adalah langkah-langkah proses aplikasi:

a. *Login* ke dalam aplikasi melalui halaman *login*
b. *Server* akan mengembalikan nilai berupa *token* bila *login* berhasil.
c. *User* menyimpan *token* dari *server* ke dalam *local storage*.
d. *User* melakukan *request* ke server *REST API* dengan menyertakan token.
e. Server REST API melakukan enkripsi dengan metode *AES 256* data *respon* data dari *request* user dengan *user token* sebagai *key*.
f. User melakukan *request* ke *endpoint* dekripsi untuk mendekripsikan hasil enkripsi sesuai dengan *access token user.*
g. Mengembalikan nilai hasil deksripsi.
h. Menampilkan nilai hasil deskripsi



Gambar 1.:Activity Diagram Proses Keseluruhan Aplikasi

3.2 Perangkat Yang Digunakan

Perangak keras yang dibutuhkan dalam membangun perangkat lunak ini memiliki spesifikasi:

a. Perangkat Keras *Server* (*Hardware*)

Perangkat keras *server* yang digunakan untuk menjalankan sistem ini terdiri dari satu buah *PC* dengan spesifikasi sebagai berikut :

1) CPU : Xeon Quad-core E5440
2) Hardisk : 50 GB.
3) RAM : 4.00 GB.

b. Perangkat Keras *Client* (*Hardware*)

Perangkat keras *client* yang digunakan untuk menjalankan sistem ini terdiri dari satu buah *Handphone Android* dengan spesifikasi sebagai berikut :

4) CPU : Quad-core 1.3 GHz Cortex-A7
5) Hardisk : 8 GB.
6) RAM : 2.00 GB.

c. Perangkat Lunak *Server* (*Software*)

Perangkat lunak yang digunakan untuk menunjang kelancaran dalam menjalankan aplikasi ini memiliki spesifikasi:

1) Sistem Operasi : Windows Server 2012
2) *Local Server* : XAMPP v1.8.3, PHP v5.5.15

d. Perangkat Lunak *Client* (*Software*)

Perangkat lunak yang digunakan untuk menunjang kelancaran dalam menjalankan aplikasi ini memiliki spesifikasi:

1) Sistem Operasi : Android Lolipop

3.3 Spesifikasi *Resource API*

a. Tabel Data Keseluruhan *User*

Table *Resource API* menggambarkan *endpoint uri* dan setiap *request* yang terjadi antara aplikasi *client* dengan *server* ,disertai *response server* yang akan di kembalikan apabila *request* berhasil.:

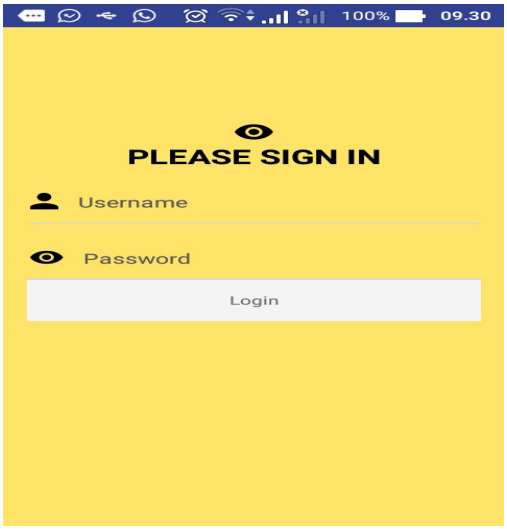
Tabel 1 : Table *Resource API*

Table Resource API				
No	URI	Dekripsi	Parameter	Response
1	*/login*	authentikasi pengguna	email,password	*access token, refresh token*
2	/client	mengambil dan melakukan enkripsi data kustomer	*access token*,phone,nama,alamat	id_kustomer, nama_kustomer,alamat ,wilayah,kelurahan,kecamatan,phone
3	/decrypt	melakukan dekripsi data kustomer yang telah di enkripsi	*access token*,data kustomer yang tersandi dengan format json	id_kustomer, nama_kustomer,alamat ,wilayah,kelurahan,kecamatan,phone
4	/sales	mengambil dan menampilkan data penjualan	*access token*,bulan,tahun,status penjualan	id_kustomer, nama_kustomer, jumlah_tagihan,pic,id_transaksi
5	/rekap_sales	mengambil rekap penjualan dalam satu tahun	access_token	bulan,total_penjualan

4.Implementasi Dan Uji Coba Program

a. Tampilan Form Layar *Login*

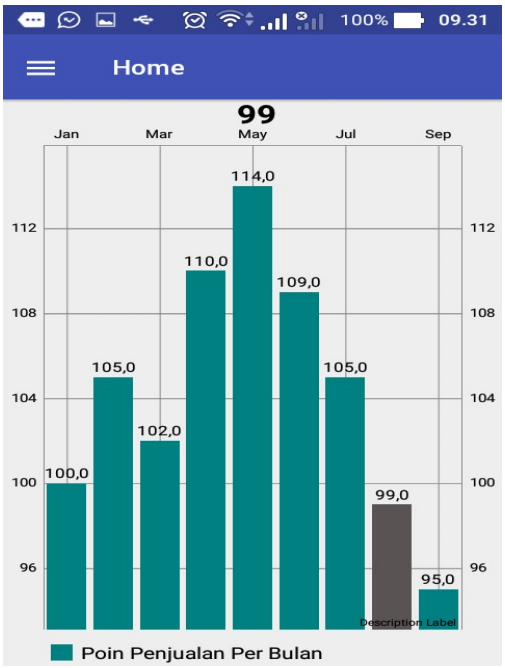
Tampilan layar halaman *login* merupakan layar yang akan tampil pertama kali ketika Aplikasi dijalankan yang menjadi penghubung ke halaman home. Berikut adalah gambar tampilan layar halaman *login* .



Gambar 2. Tampilan Form Layar Login

b. Tampilan Layar Halaman *Home*

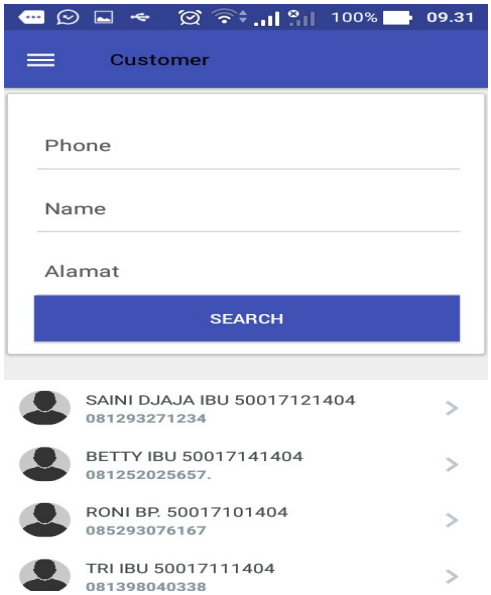
Halaman *home* android seperti pada Gambar 3 ini merupakan halaman home yang menampilkan statistik penjualan marketing per bulan dalama satu tahun. Statistik yang ditampilkan adalah total penjualan.



Gambar 3. Tampilan Home

c. Tampilan Layar Halaman *Customer*

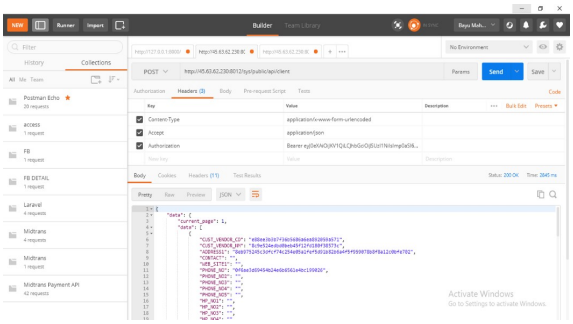
Berikut ini pada gambar 4 adalah tampilan layar halaman *customer* yang berfungsi untuk mengambil data *customer* yang ada di *database* yang sudah melalui proses enkripsi dan dekripsi



Gambar 4. Tampilan **Halaman *Customer***

d. Tampilan *Request* Enkripsi Di *Background*

Request Enkripsi pada Gambar 5 merupakan proses *request database* dari aplikasi android ke *server* dan proses enkripsi hasil *request database*.



Gambar 5. Tampilan Request **Di Background Aplikasi**

e. Tampilan Table Hasil Uji Coba

Pada tabel ini dapat dilihat hasil kecepatan enkripsi dan deskripsi pesan teks bedasarkan koneksi di tiap negara, Letak *server* yang berlokasi di *Los Angles* mengurangi waktu eksekusi ketika menggunakan ip address lokasi negara Amerika..

Tabel 2 : Table Hasil Ujicoba

Nama Negara	*Request & Encrypt*	*Decrypt*	Satuan
Jepang	2310	1788	*ms*
Australia	4387	1223	*ms*
Swedia	2126	1210	*ms*
Kanada	1651	2235	*ms*
Jerman	5576	1274	*ms*
Prancis	2295	1793	*ms*
Amerika	2732	981	*ms*
Inggris	3074	2165	*ms*

5. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan serta uji coba sistem dapat disimpulkan sebagai berikut :

1) Pegamanan *REST API* dapat diamankan dengan algortima kriptografi AES 256
2) Data tidak dapat dibaca oleh pihak yang tidak berhak yang tidak memiliki *access token*.
3) Proses *REST API* tergantung dengan koneksi *internet* yang digunakan, sehingga proses pengiriman dan *request* bisa cepat atau lama

Pengembangan yang perlu dilakukan untuk penelitian berikutnya adalah Membuat berbagai variasi *client application* selain *mobile application*. dapat berupa *Single Page Applicatio*

5. DAFTAR PUSTAKA

[1] Sadikin, Rifki. (2012). Kriptografi untuk kemanan dan jaringan.

[2] More, Sharddha. (2015), *Implementation of AES 256 with Time Complexity Measurement forVarious Output, ISSN :* 0975 – 4172*Vol. 15 Issue*

[3] Aggarwal Abhinandan (2016), *Implementation of AES 256 algorithm* ISSN : 2395 6992

[4] Pitchaiah M. (2012) *Implementation of Advance Encryption Standart Algorithm ISSN : 2278-9723. Vol. 01 No 38*

[4] Paddhan Sagar. (2014) *AES 256-256 Encryption in Communication using LabVIEW ISSN :* 2278- 8875. *Vol. 04 Issue 6*