Implementasi Algoritma AES-256 Untuk Pengamanan Layanan API Pada Restful Dengan Autentikasi *Json Web Tokens*

Achmad Ardiansyah[1], Mepa Kurniasih[2]
[1,2]Fakultas Teknologi Informasi, Universitas Budi Luhur Jakarta
[1]ahd.ardiansyah@gmail.com,[2]mepa.kurnia@gmail.com

Abstrak

Perkembangan teknologi informasi pada saat ini telah mengalami kemajuan yang sangat pesat dan sudah menjadi salah satu kebutuhan baik dalam lingkup individu maupun organisasi. Perusahaan Bintang Cemerlang Abadi adalah sebuah perusahaan yang bergerak dibidang *general supplier, productivity cleaning,* dan *workplace safety distributor*. Masing – masing unit memiliki sistem yang berbeda *platform* dan bahasa pemrograman di lingkungan perusahaan. Penerapan *REST API* merupakan alternatif terbaik yang digunakan dalam mengatasi kondisi integrasi sistem dan distribusi data yang dialami oleh pihak perusahaan. Untuk mengatasi kekurangan dari keamanan dan kebijakan hak akses tersebut *REST API* diperlukan sistem authentikasi untuk memberikan hak akses data. *JSON Web Tokens* atau *JWT* merupakan sebuah token berbentuk string yang digunakan untuk melakukan otentikasi dan menjamin integritas pesan yang dikirim oleh salah satu pihak. Dibutuhkan keamanan data terhadap pertukaran data, maka perlu adanya metode kriptografi. Metode tersebut yang diimplementasikan menggunakan algoritma AES-256. Dengan adanya algoritma AES-256 supaya tidak disalahgunakan oleh orang yang tidak berhak mengetahui isi data yang telah dienkripsi tersebut, dan mengembalikan data yang dienkripsi tanpa mengalami perubahan data yang sesuai dengan data asli. Metode pengujian menggunakan *black box testing, black box* merupakan metode yang digunakan untuk menemukan kesalahan dan mendemonstrasikan fungsional aplikasi saat dioperasikan. Setelah melalui tahap pengujian pada implementasi *REST API*, maka di dapatkan kesimpulan bahwa telah berhasil dibangun dan diimplementasikan dalam pengamanan data menggunakan algoritma AES-256 dan *JSON Web Tokens*.

Kata Kunci : algortima AES-256, API, JWT, REST, keamanan, pertukaran data

Abstract

The development of information technology at this time has experienced very rapid progress and has become one of the needs of both individuals and organizations. Bintang Cemerlang Abadi Company is a company engaged in general suppliers, productivity cleaning, and workplace safety distributors. Each unit has a different system platform and programming language in the corporate environment. The application of REST API is the best alternative used in overcoming the conditions of system integration and data distribution experienced by the company. To overcome the shortcomings of security and the access rights policy, the Rest API is required for an authentication system to provide data access rights. JSON Web Tokens or JWT is a string-shaped token that is used to authenticate and guarantee the integrity of messages sent by one party. Data security is needed for data exchange, so there is a need for cryptographic methods. The method is implemented using the AES 256 algorithm. With the AES 256 algorithm so that it is not misused by unauthorized people know the contents of the data that has been encrypted, and return the encrypted data without experiencing data changes that match the original data. The test method uses black box testing, black box is a method used to find errors and demonstrate functional applications when operated. After going through the testing phase of the implementation of the Rest API, then get the conclusion that it has been successfully built and implemented in data security using the AES-256 algorithm and JSON web tokens.

***Keywords** : AES-256 algorithm, API, JWT, REST, security, data exchange*

I. PENDAHULUAN

Perkembangan teknologi informasi pada saat ini telah mengalami kemajuan yang sangat pesat dan sudah menjadi salah satu kebutuhan baik dalam lingkup individu maupun organisasi. Untuk memfasilitasi pertukaran informasi atau data antara dua atau lebih aplikasi perangkat lunak menggunakan teknologi API (Application Programming

Interface). Salah satu teknologi API yang populer yaitu Restful, namun komunikasi Restful memiliki beberapa kekurangan yaitu tidak ada dukungan standar untuk keamanan dan kebijakan pengaksesan data pada sisi *server*, hal ini menyebabkan siapapun bisa mengakses, merubah, maupun menghapus data yang terdapat pada sisi *server*. Untuk mengatasi kekurangan dari keamanan dan kebijakan hak akses tersebut Restful diperlukan sistem autentikasi untuk memberikan hak akses data pada Restful *Server*. JSON *Web Token* atau JWT merupakan sebuah *token* berbentuk *string* yang digunakan untuk melakukan autentikasi dan menjamin integritas pesan yang dikirim oleh salah satu pihak. Dengan menggunakan JWT pada komunikasi API maka dapat memberikan keamanan dan kebijakan hak akses data dari restful.

Pada implementasi JWT dibutuhkan suatu metode yang dapat menjaga kerahasiaan data, dan metode yang dimaksud adalah kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Algoritma yang digunakan dalam metode kriptografi yaitu algoritma AES (Advanced Encryption Standard). Untuk tingkat keamanan yang lebih baik, algoritma AES menggunakan kunci 256bit. Maka dari itu penulis membuat "Implementasi Algoritma AES-256 Untuk Pengamanan Layanan API Pada RESTFul dengan Autentikasi JSON Web Token".

II. TINJAUAN PUSTAKA

A. Representational State Transfer (REST)

REST merupakan salah satu teknologi Web Service yang terbilang cukup populer di masa sekarang ini. Teknologi ini bekerja berdasarkan resource untuk membuat sistem terdistribusi. REST (disebut juga RESTful services) adalah perangkat lunak yang didesain dengan penekanan pada kesederhanaan, skalabilitas, serta kegunaan. REST mulai berkembang pesat karena sistemnya yang lebih sederhana daripada SOAP dan WSDL. Sisi sederhana dari REST yang membuat menarik adalah REST dapat dibangun dengan sedikit tools. Selain itu untuk melakukan testing terhadap REST service dapat dilakukan secara sederhana pada web browser tanpa harus melakukan simulasi client – server.

Metode REST didasari oleh empat prinsip utama teknologi yaitu:

a. Resource identifiier melalui Uniform Resource Identifier (URI), REST Web Service mencari sekumpulan sumber daya yang mengidentifikasi interaksi antar client.

b. Uniform Interface, sumber daya yang dimanupulasi CRUD (Create, Read, Update, Delete) menggunakan operasi PUT, GET, POST, DELETE.

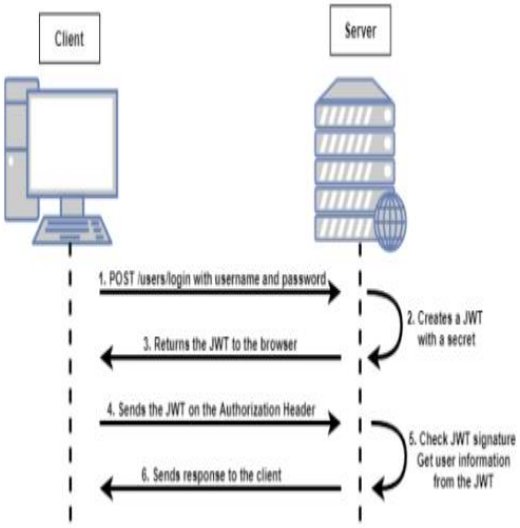
c. Self-descriptive messages, sumber daya informasi tidak terikat, sehingga dapat mengakses berbagai format konten (HTML, XML, PDF, JPEG, Plain Text dan lainnya). Metadata pun dapat digunakan.

d. Stateful intercations melalui hyperlinks, setiap interaksi dengan suatu sumber daya bersifat stateless, yaitu request messages tergantung jenis kontennya.

B. JSON Web Tokens (JWT)

JWT adalah sebuah token berbentuk string JSON yang sangat padat (ukurannya), informasi mandiri yang gunanya sendiri untuk melakukan sistem autentikasi dan pertukaran informasi. Karena bentuknya kecil, token JWT dapat dikirim melalui URL, parameter HTTP POST atau di dalam Header HTTP, dan juga karena ukurannya yang kecil maka dapat ditransmisikan dengan lebih cepat. Disebut informasi mandiri karena isi dari token yang dihasilkan memiliki informasi dari pengguna yang dibutuhkan, sehingga

tidak perlu query ke basis data lebih dari satu kali. Token tersebut dapat diverifikasi dan dipercaya karena sudah di-sign secara digital. JWT tidak bergantung pada bahasa program tertentu. JWT tersusun atas 3 bagian yaitu header, payload dan signature.



GAMBAR 1 : MEKANISME AUTENTIKASI DENGAN JWT

C. Algoritma Advanced Encryption Standard (AES)

AES menggunakan algoritma Rijndael yang telah memenangkan sayembara terbuka yang dilakukan oleh NIST (National 9 Institute of Standard and Technology). Jenis algoritma kriptografi AES (atau Rijndael) ini bersifat simetri dan cipher blok. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi, serta masukkan dan keluaran berupa blok dengan urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut sebagai blok data atau plaintext yang nantinya akan di-enkripsi menjadi chipertext. Cipher key dari AES terdiri dari key dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round (putaran) yang akan diimplementasikan pada algoritma AES ini. Ada 10, 12, atau 14 putaran dalam AES yang sesuai dengan ukuran kunci yang digunakan.

	Jumlah Key (Nk)	Ukuran Blok (Nb)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

TABEL 1 : PERBANDINGAN JUMLAH ROUND DAN KEY

Algoritma Rijndael (AES) mempunyai tiga parameter yaitu :
a. Plaintext, array yang berukuran 16 byte, yang berisi data masukkan.
b. Ciphertext, array yang berukuran 16 byte, yang berisi hasil enkripsi
c. Kunci, array yang berukuran 16 byte, yang berisi kunci chiper

III. METODOLOGI PENELITIAN.

Dalam penelitian ini, beberapa metode digunakan untuk memperoleh informasi yang diperlukan dan menyelesaikan masalah yang ditemui. Adapun metode – metode ini sebagai berikut:

A. Mengumpulkan Data

Tahapan ini dilakukan untuk mengumpulkan data dengan mencari informasi pembahasan yang sudah pernah dibahas di internet, wawancara narasumber, meminta data yang akan dibutuhkan dalam pembangunan aplikasi ke instansi dan membaca buku-buku referensi.

B. Analisa Data

Menganalisa algoritma kriptografi AES dan JWT serta teknik-teknik yang digunakan.

C. Perancangan

Merancang API untuk menentukan spesifikasi dari sistem sesuai hasil analisa yang dilakukan.

D. Implementasi

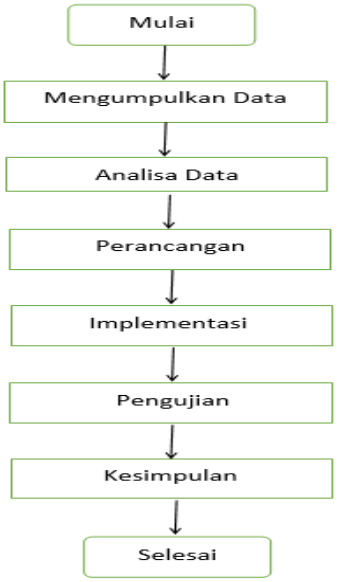
Melakukan tahapan untuk mengembangkan perangkat lunak dengan pengkodean program, pengujian, dan menerapkan berdasarkan hasil analisa kedalam bentuk program dengan bahasa pemrograman Java.

E. Pengujian

Melakukan pengujian terhadap program yang telah dirancang serta menyimpulkan hasil pengujian.

F. Kesimpulan

Pada tahap akhir dilakukan pengambilan kesimpulan dari hasil pengujian terhadap aplikasi yang dibangun.



GAMBAR 2 : METODOLOGI PENELITIAN

IV. HASIL DAN PEMBAHASAN

A.`Definisi Masalah

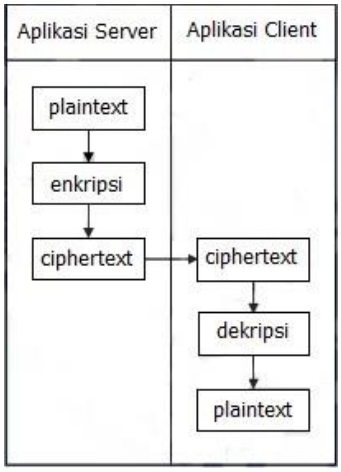
Perusahaan Bintang Cemerlang Abadi adalah sebuah perusahaan yang bergerak dibidang General Supplier, Productivity Cleaning, dan Workplace Safety Distributor yang beroperasi di daerah Karang Tengah. Terdapat beberapa unit dalam lingkungan perusahaan. Masing – masing unit memiliki sistem yang berbeda platform dan bahasa pemrograman. Kondisi seperti ini memberikan pengaruh besar dalam penurunan kinerja dari masing-masing unit. Dalam kesehariannya, terdapat transaksi-transaksi yang mempengaruhi jumlah stok barang, pencatatan dan laporan transaksi yang dilakukan. Proses tersebut berdampak pada penyesuaian data antara data pergudangan dan data pencatatan transaksi, dikarenakan terdapat beberapa database yang digunakan secara terpisah dan aplikasi-aplikasi yang berbeda – beda.

B. Pemecahan Masalah

Penerapan REST API merupakan alternatif terbaik yang digunakan dalam mengatasi kondisi integrasi sistem dan distribusi data yang dialami oleh pihak perusahaan. Namun komunikasi REST API memiliki beberapa kekurangan yaitu tidak ada dukungan standar untuk keamanan dan kebijakan pengaksesan data pada sisi server, untuk mengatasi kekurangan tersebut REST API diperlukan sistem autentikasi untuk memberikan hak akses data pada REST Server. JSON Web Token atau JWT merupakan sebuah token berbentuk string yang digunakan untuk melakukan autentikasi dan menjamin integritas pesan yang dikirim oleh salah satu pihak. Pada implementasi JWT dibutuhkan suatu metode yang mendefinisikan cara yang simpel dan independen dari transmisi informasi yang aman antar setiap pihak dengan menggunakan format data objek JSON. Untuk keamanan data terhadap pertukaran data perlu adanya metode kriptografi yang diimplementasikan menggunakan algoritma AES 256.

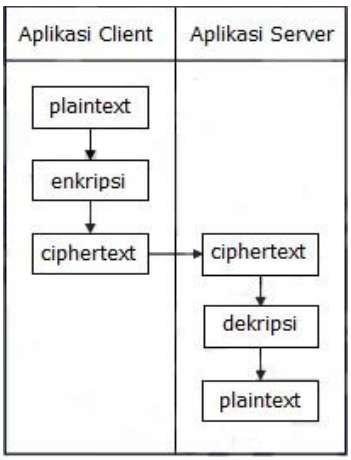
C. Program Aplikasi Usulan

Sesuai dengan analisis sistem, maka didapatkan gambaran bahwa client mengirimkan sebuah request message yang mencakup HTTP method yang akan diinvokasi, lokasi resource dalam format URL, serta pilihan format pesan (pada dasarnya dapat berupa format seperti HTML, plaintext, JSON), kemudian server akan mengirimkan respon sesuai dengan spesifikasi yang diminta oleh client. Selama ini, yang berfungsi sebagai client adalah sebuah web browser yang memfasilitasi komunikasi antara mesin dengan manusia. Dengan adanya REST, aplikasi client dapat berupa aplikasi apa saja dengan memanfaatkan HTTP. Rancangan proses komunikasi pada aplikasi client dan aplikasi serverdapat ditunjukkan pada Gambar 2 dan Gambar 3.



GAMBAR 2 : KOMUNIKASI CLIENT KE SERVER

Pada Gambar 2 menjelaskan tentang rancangan proses komunikasi antara aplikasi client dengan aplikasi server dalam hal ini REST API *Client* bermaksud mengirimkan data ke *server* dalam bentuk *plaintext*. Sebelum dikirimkan, data yang berupa *plaintext* dienkripsi dahulu dengan algoritma AES-256, kemudian hasil enkripsi berupa *ciphertext*, dikirimkan ke *server*. *Server* menerima data dalam bentuk *ciphertext*, kemudian didekripsi dengan algoritma AES-256, sehingga diperoleh data *plaintext*. Selanjutnya data *plaintext* tersebut diteruskan akan diolah.



Gambar 3 : Komunikasi Server Ke Client

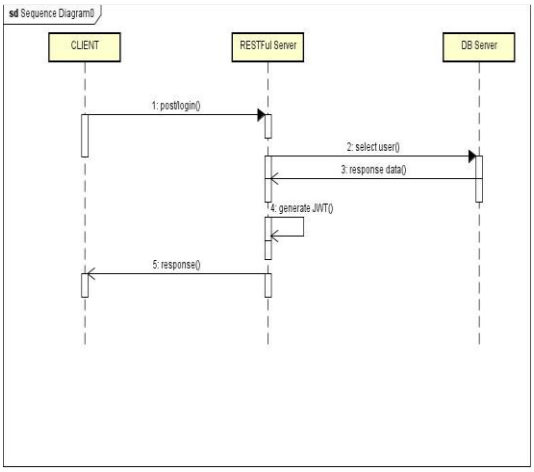
Sebaliknya, pada Gambar 3 menjelaskan tentang rancangan komunikasi dari server ke client. Server mengirimkan data yang telah terenkripsi dengan algoritma AES-256 sebelumnya (ciphertext) ke aplikasi client. Kemudian oleh client, data ciphertext didekripsi dengan algoritma AES, untuk mendapatkan data plaintext. Selanjutnya data plaintext tersebut diolah atau ditampilkan di aplikasi client.

D. Alur Kerja API

Dalam menggambarkan beberapa urutan – urutan proses yang harus dilalui, digambarkan dalam bentuk alur kerja sebagai penjelasan. Dibawah ini akan diberikan beberapa alur kerja untuk masing – masing proses.

1) Token

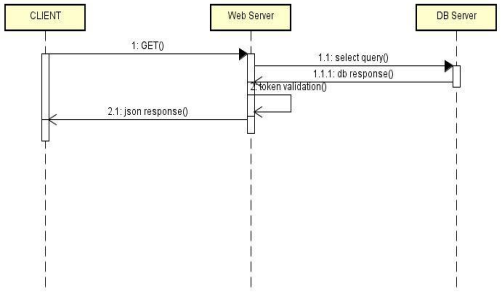
Sebelum client melakukan akses kepada setiap sumberdaya yang dimiliki, client harus melakukan login terlebih dahulu. Respon dari proses login yaitu token yang akan digunakan pada HTTP Header untuk mengakses sumberdaya. Alur kerja dari API yang dibangun, dapat dijelaskan pada Gambar 4 berikut ini :



GAMBAR 4 : TOKEN

2) Method GET

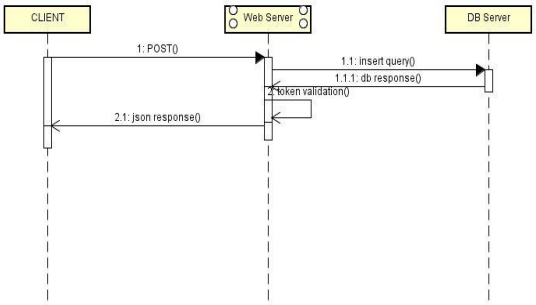
Merupakan operasi read only yang digunakan untuk meminta informasi spesifik pada server dalam bentuk query, karakteristik dari operasi GET adalah idempotent dan safe sebanyak-banyaknya apapun operasi ini dilakukan, hasilnya akan tetap sama. Sedangkan, safe berarti ketika operasi ini diinvokasi tetap tidak mengubah state di server.



GAMBAR 5 : METHOD GET

3) Method POST

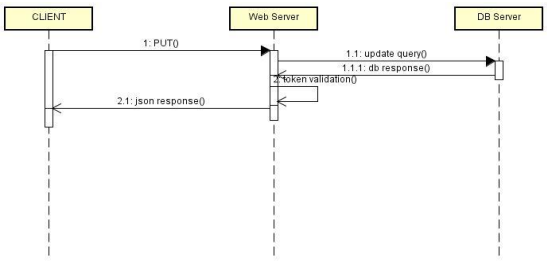
POST merupakan operasi untuk membuat resource baru. Method tersebut digunakan untuk proses simpan data.



Gambar 6 : Method POST

4) Method PUT

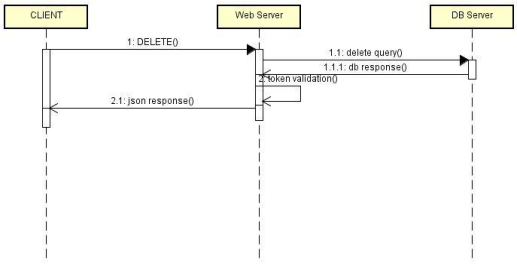
PUT merupakan operasi untuk meminta kepada server agar mengubah sebuah *resource* yang sudah ada.



GAMBAR 7 : METHOD PUT

5) Method DELETE

DELETE digunakan untuk menghapus resource tertentu.



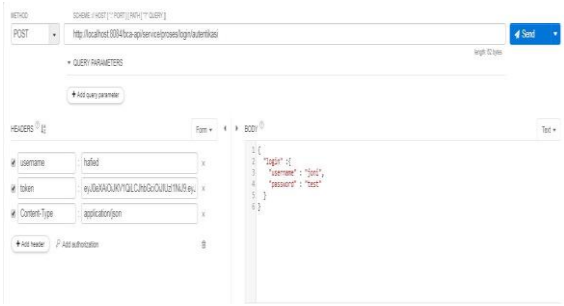
GAMBAR 8 : METHOD DELETE

E. Cara Pengoperasian *API*

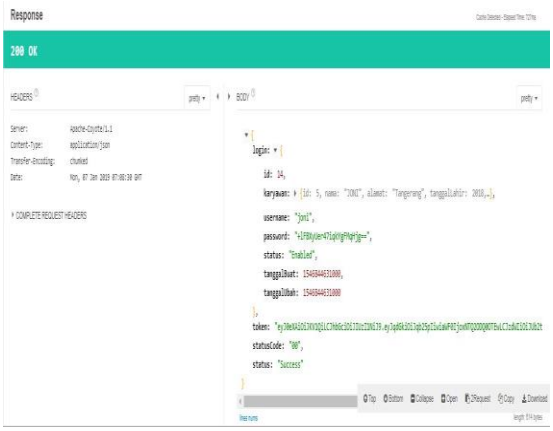
Pada bagian ini, akan diuraikan mengenai pengoperasioan aplikasi ini mulai dari pertama kali dijalankan sampai diimplementasikan. Berikut ini akan diberikan penjelasan dari gambar mengenai pengoperasian yang ada pada aplikasi ini.

6) Login Autentikasi

Berikut ini *request* dan *response login* autentikasi dengan memasukan username dan password yang telah terdaftar pada table login lalu akan mendapatkan *response* berupa token. Token ini nantinya dapat digunakan untuk mengakses sumber daya yang dimiliki.

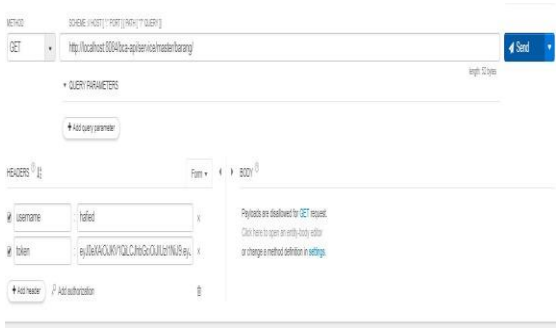


GAMBAR 9 : *REQUEST LOGIN* AUTENTIKASI



GAMBAR 10 : *RESPONSE LOGIN* AUTENTIKASI

7) Menampilkan Data Barang



Berikut ini *request* dan *response* untuk menampilkan barang:

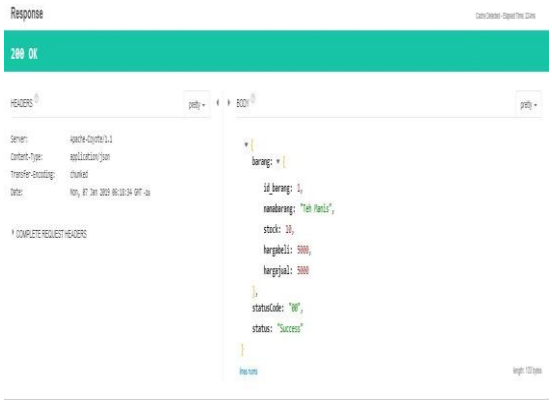
GAMBAR 11 : *REQUEST* DATA BARANG

Gambar 12 : *Response* Data Barang

8) Menampilkan Data Barang Berdasarkan Id

Berikut ini *request* dan *response* untuk menampilkan data barang berdasarkan Id barang:

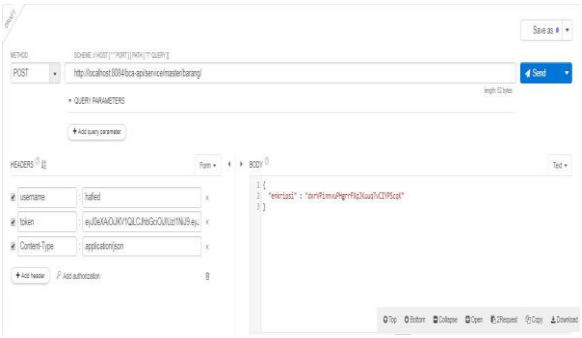
GAMBAR 13 : *REQUEST* DATA BARANG BERDASARAKAN ID



GAMBAR 14 : *RESPONSE* DATA BARANG BERDASARAKAN ID

9) Menyimpan Data Barang

Berikut ini *request* dan *response* untuk menyimpan barang berhasil ditambahkan dengan status *success*.

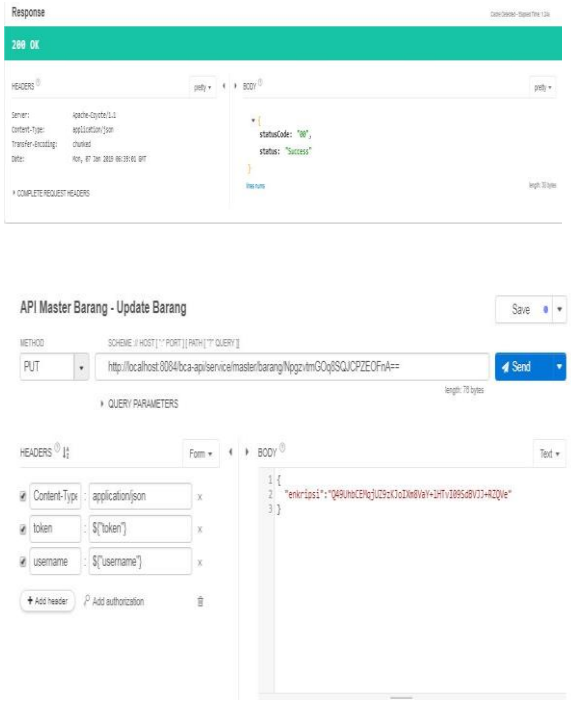


GAMBAR 15 : *REQUEST* MENYIMPAN DATA BARANG

10) Mengubah Data Barang

Berikut ini *request* dan *response* untuk mengubah barang berhasil ditambahkan dengan status *success*.

GAMBAR 17 : *REQUEST* MENGUBAH BARANG



GAMBAR 18 : *RESPONSE* MENGUBAH BARANG

11) Menghapus Data Barang

Berikut ini *request* dan *response* untuk menghapus barang berdasarakan id barang.

GAMBAR 19 : *REQUEST* MENGHAPUS DATA BARANG

GAMBAR 20 : *RESPONSE* MENGHAPUS DATA BARANG

F. Pengujian Program

Pada bagian ini penulis menggunakan metode pengujian *black box testing*, *black box* merupakan metode yang digunakan untuk menemukan kesalahan dan mendemonstrasikan fungsional aplikasi saat dioperasikan, apakah input diterima dengan benar dan output yang dihasilkan telah sesuai yang diharapkan. Pada *black box testing* meliputi *security* dan *performance* sistem dapat ditunjukan:

a) Pengujian Login Autentikasi

Pada pengujian ini untuk memasukan *username* dan *password* dengan method post.

No	Skenario Pengujian	*Test Case*	Hasil Pengujian
1	Menginput *username* dan *password* pada *request body* dengan metode *POST.*	*Username* : hafied *Password* : joni	Sesuai Harapan

TABEL 2 : PENGUJIAN LOGIN AUTENTIKASI

b) Pengujian Data Barang

Pada pengujian ini untuk menampilkan, menyimpan, mengubah dan menghapus data barang.

No	Skenario Pengujian	*Test Case*	Hasil Pengujian
1	Menampilkan data barang dengan metode *GET*	Input URL dan klik tombol Send pada *Restlet Client*	Sesuai Harapan
2	Menampilkan data barang berdasarkan id_barang dengan metode *GET*	Input URL beserta id_barang dan klik tombol *Send* pada *Restlet Client*	Sesuai Harapan
3	Menambah data barang dengan metode *POST*	Input URL dan input data barang pada *request body Restlet Client* lalu klik tombol *Send*	Sesuai Harapan
4	Mengubah data barang berdasarkan id_barang dengan metode *PUT*	Input URL beserta id_barang dan input data barang pada *request body Restlet Client* lalu klik tombol *Send*	Sesuai Harapan
5	Menghapus data barang berdasarkan id_barang dengan metode *DELETE*	Input URL beserta id_barang dan klik tombol *Send* pada *Restlet Client*	Sesuai Harapan
6	Mengosongkan *token* dan *username* pada *request header Restlet Client*	Input *token* dan *username* pada *request header Restlet Client*	Sesuai Harapan

TABEL 3 : PENGUJIAN DATA BARANG

V. PENUTUP

Berdasarkan hasil penelitian dan pembahasan penerapan implementasi API Restful menggunakan algoritma AES-256 dengan autentikasi *json web tokens*, maka didapatkan kesimpulan bahwa dari hasil pengujian menggunakan *black box testing* secara fungsional telah berhasil dibangun dan diimplementasikan dengan baik. Kecepatan enkripsi yang dilakukan sesuai terhadap panjang yang digunakan, semakin panjang kunci maka semakin lama waktu yang dibutuhkan..Untuk penelitian selanjutnya bisa membandingkan antara algoritma yang akan digunakan untuk proses enkripsi dan dekripsi, supaya dari segi kecepatan dan keamanan dalam enkripsi dan dekripsi .

VI. REFERENSI

Rahmatulloh, Alam., Sulastri, H., Nugroho, R.(2018). “Keamanan RESTful Web Service menggunakan JSON Web Token (JWT).” Yogyakarta.

Satria, Bagus., Kusyanti, A., Yahya., W. (2018). "Implementasi Algoritma Blake2s pada Json Web Token Untuk Mekanisme Autentikasi Layanan REST-API.” Malang.

Tanaem, F., Penidas., Manongga., D., Iriani, Adi. (2016). “RESTFul Web Service Untuk Sistem Pencatatan Studi Kasus PT. XYZ” Salatiga.

Fauziah, Yuli. (2007). “Aplikasi Iklan Baris Online Menggunakan Arsitektur Web Service ” Yogyakarta.

Perkasa, Iqbal., M., Setiawan., Budi., E. (2018). “Pembangunan Web Service Data Masyarakat Menggunakan REST API dengan Access Token.” Bogor.

Subekti, Dwi. (2017). “Kriptografi Pesan Suara Menggunakan Algoritma AES (ADVANCED ENCRYPTION STANDARD).” Jakarta.

Sugiyanto, Hapsari., Kembang, R. (2016). ”Pengembangan Algoritma Advanced Encryption Standard Pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere”Surabaya.

Abidin, Muazim., A., Hardianti, F., Setiani, Nur., I. (2016). “Analisa Dan Implementasi Proses Kriptografi Encryption-Decryption Dengan Algoritma ADVANCED ENCRYPTION STANDARD (AES-128).” Tuban.

Yuniati, Voni., Indriyanta, Gani., C, Rachmat, A. (2015). “Enkripsi Dan Dekripsi Dengan ALGORITMA AES 256 UNTUK SEMUA JENIS FILE.” Universitas Kristen Duta Wacana