BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada saat ini telah mengalami kemajuan yang sangat pesat dan sudah menjadi salah satu kebutuhan baik dalam lingkup individu maupun industri. Terutama dalam hal pertukaran informasi antara dua atau lebih aplikasi di perangkat lunak menggunakan teknologi API (*Application Programming Interface*) [1].

Konsep REST pertama kali diperkenalkan oleh Roy Fielding pada tahun 2000. REST merupakan standar arsitektur komunikasi berbasis web yang selalu digunakan terhadap pengembangan layanan berbasis web. Pada umumnya, *Hypertext Transfer Protoco*l (HTTP) berperan sebagai protokol untuk melakukan komunikasi data. Sistem yang menggunakan prinsip-prinsip dari REST dapat disebut dengan "RESTful" [2].

API tidak hanya mudah diterapkan di berbagai platform seperti situs web, aplikasi *desktop*, perangkat seluler, dan integrasi antar server, namun karena kemudahannya itu menyebabkan layanan API menjadi sangat rentan dalam keamanannya. Contohnya terjadi pada PT. Bakti Indonesia Mengaji, PT. Bakti Indonesia Mengaji adalah sebuah perusahaan yang bergerak di bidang Teknologi Informasi yang fokus di bidang pembelajaran baca Qur'an. Perusahaan tersebut memiliki sebuah produk aplikasi yang bernama gurungaji.com.

Berdasarkan wawancara dengan Bapak Laurensius selaku CTO gurungaji.com, terjadi serangan yang dilakukan secara berulang kali pada server dengan tujuan mencari celah untuk berlangganan pada fitur yang berbayar, tetapi pelaku tidak ingin melakukan pembayaran pada fitur yang sudah dipilih. Kemudian pelaku melakukan serangan dengan metode *SQL Injection* bertujuan untuk mengubah status pada data transaksi yang berawal status menunggu pembayaran menjadi status selesai pembayaran. Ini dibuktikan oleh *log* peretasan pada bagian data transaksi yang dimana peretasan tersebut menggunakan metode *SQL Injection*. Tidak hanya itu, peretasan terjadi akibat dari autentikasi pada *header request* yang tidak memiliki metode enkripsi khusus. Hal ini mengakibatkan kerentanan dalam keamanan sistem, karena berpotensi bagi pelaku untuk mengakses dan memanipulasi data yang dikirimkan dalam *header request* tanpa ada lapisan perlindungan yang memadai.

Metode *SQL Injection* banyak digunakan sebagai memasukan perintah atau kode khusus *SQL* sebagai masukkan pada suatu website untuk mendapatkan informasi server maupun akses ke dalam basis data [3]. *SQL Injection* menyerang pada bagian *key-value pairs* yang belum terenkripsi. *Key-value pairs* adalah dua nilai yang biasanya dihubungkan sedemikian rupa sehingga nilainya diakses menggunakan kunci tersebut. *Key-value pairs* terdapat pada autentikasi *header* REST API.

Atas terjadinya peretasan tersebut tentu sangat merugikan perusahaan, terutama pada akses fitur yang berbayar. Peretasan ini juga memungkinkan

pelaku untuk mengakses, mengubah, atau menghapus data sisi server. Tidak hanya itu, data pengguna yang sifatnya rahasia dapat menjadi sasaran untuk diambil, sehingga dapat merugikan perusahaan dan pengguna.

Dengan uraian latar belakang diatas, maka dalam penelitian ini peneliti akan mengimplementasikan algoritma *Advanced Encryption Standard* pada proses enkripsi dan dekripsi pada *key-value pairs* yang terdapat di autentikasi *header* REST API. Adapun judul penelitian yang berjudul **"Implementasi Keamanan Komunikasi Data Berbasis Rest Api Web Service Dengan Penerapan Kriptografi Advanced Encryption Standard (Studi Kasus : Aplikasi Android gurungaji.com PT. Bakti Indonesia Mengaji)".**

1.2 Identifikasi Masalah

Berdasarkan latar belakang masalah diatas, dengan ini peneliti dapat mengidentifikasikan permasalahan yang ada, yaitu:

1. Terjadi serangan yang dilakukan secara berulang kali pada server dengan tujuan mencari celah untuk berlangganan pada fitur yang berbayar.
2. Pelaku melakukan serangan dengan metode *SQL Injection* bertujuan untuk mengubah status pada data transaksi yang berawal status menunggu pembayaran menjadi status selesai pembayaran.
3. Peretasan terjadi akibat dari autentikasi pada *header request* yang tidak memiliki metode enkripsi khusus.

1.3 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka dapat dirumuskan masalah sebagai berikut:

1. Bagaimana mengimplementasikan algoritma *Advanced Encyption Standard* pada proses enkripsi pada *key value pairs* yang terdapat di autentikasi *header* REST API dari sisi server ?
2. Bagaimana proses dekripsi dari hasil *enkripsi key value pairs* dari sisi *client* ?

1.4 Batasan Masalah

Dalam pembahasan dan permasalahan yang terjadi, diperlukan beberapa batasan masalah atau ruang lingkup kajian sehingga penyajian lebih terarah dan terkait satu sama lain. Adapun batasan masalahnya adalah sebagai berikut:

1. Metode yang digunakan untuk mengamankan dari serangan *SQL Injection*, yaitu metode algoritma *Advanced Encryption Standard* 128 untuk keamanan komunikasi data pada autentikasi *header* REST API.
2. Data yang dienkripsi merupakan *key value pairs* pada header REST API.
3. Sistem diuji coba menggunakan Postman (*Software testing*), postman adalah sebuah *platform* API untuk membangun dan mengunakan sebuah API [4].

4. Sistem dibuat menggunakan bahasa pemrograman PHP dengan *framework* nya adalah CodeIgniter 4 dan MySQL.
5. Data yang diamankan merupakan URL pada data transaksi (*dummy*).

1.5 Tujuan Penelitian

Berdasarkan perumusan masalah yang telah diuraikan diatas, maka didapat tujuan sebagai berikut:

1. Mengamankan *key value pairs* pada autentikasi *header* REST API untuk pengaksesan data.
2. Mengamankan *key value pairs* dari serangan *SQL Injection*.

1.6 Manfaat Penelitian

Adapun manfat dalam penelitian ini adalah sebagai berikut:

1. Bagi peneliti

   Penelitian tentang teknologi memberikan manfaat besar bagi para peneliti dengan memberikan kesempatan untuk mendalami dan menggali wawasan mendalam mengenai perkembangan terkini dalam bidang teknologi. Melalui penelitian ini, peneliti dapat menjadi sumber informasi yang berharga bagi pembaca, memberikan pandangan yang mendalam tentang tren, isu-isu terkini, dan potensi dampak teknologi pada masyarakat dan industri. Selain itu, penelitian teknologi juga membuka pintu bagi peneliti untuk berkontribusi dalam merumuskan solusi dan ide- ide baru yang dapat membentuk arah perkembangan teknologi di masa depan.

Dengan terus berinovasi dan menggali pengetahuan lebih dalam, peneliti dapat menciptakan karya-karya yang informatif, inspiratif, dan relevan dengan tuntutan zaman.

2. Bagi perusahaan

   Meningkatkan keamanan dalam komunikasi data, agar dapat membatasi siapapun mengakses, merubah, maupun menghapus data dari sisi server.

1.7 Pertanyaan Penelitian

Adapun pertanyaan penelitian yang ditanyakan dalam penulisan skripsi ini adalah sebagai berikut:

1. Apakah algoritma *Advanced Encryption Standard* dapat mengenkripsi *key value pairs* di *header* autentikasi REST API pada sisi server ?
2. Apakah algoritma *Advanced Encryption Standard* dapat mendekripsi dari hasil enkripsi pada sisi *client* ?

1.8 Hipotesis Penelitian

Berdasarkan pemaparan diatas, maka dapat dikemukakan hipotesis "Dengan penggunaan algoritma AES dalam mengenkripsi dan mendekripsi *key value pairs* pada REST API akan secara signifikan meningkatkan tingkat keamanan data yang dikirim dan disimpan, dengan mengurangi risiko akses yang tidak sah atau pencurian informasi."

1.9 Metodologi Penelitian

Metodologi penelitian adalah pendekatan sistematis dan terstruktur yang digunakan oleh peneliti untuk merencanakan, melaksanakan, mengumpulkan data, menganalisis, dan menyajikan hasil penelitian. Metodologi ini bertujuan untuk memastikan bahwa penelitian dilakukan secara objektif, akurat, dan dapat diandalkan, serta memungkinkan peneliti untuk menjawab pertanyaan penelitian dengan cara yang valid dan obyektif. Adapun metode penelitian yang digunakan adalah:

1.9.1 Metode Pengumpulan Data

Pada metode ini membahas mengenai cara memperoleh data yang dibutuhkan untuk melakukan penelitian, metode yang digunakan yaitu:

1. Observasi

   Observasi dilakukan secara langsung ke kediaman bapak Laurensius Dede Suhardiman selaku CTO di tim IT gurungaji.com yang beralamat di Blok Lumbu Desa Cigugur, Kelurahan Cigugur, Kecamatan Cigugur, Kabupaten Kuningan, Jawa Barat 45552. Pada tanggal 20 Februari 2023. Kedatangan ke lokasi tersebut untuk mengetahui secara langsung bagaimana permintaan HTTP di inisiasi

dan diproses oleh REST API, serta untuk mengamati interaksi antara pengguna dan sistem dalam situasi praktis.

2. Wawancara

   Setelah melakukan observasi di tempat tersebut, saya melakukan wawancara dan meminta izin untuk melakukan penelitian kepada CTO dari gurungaji.com yaitu bapak Laurensius Dede Suhardiman yang bertempat di kediamannya, beralamat Blok Lumbu Desa Cigugur, Kelurahan Cigugur, Kecamatan Cigugur, Kabupaten Kuningan, Jawa Barat 45552. Hasil wawancara yang didapatkan adalah terjadinya serangan yang dilakukan oleh *user* yang sudah terdaftar dan ingin berlangganan pada fitur yang berbayar, tetapi pelaku tidak ingin melakukan pembayaran pada fitur yang sudah dipilih. Kemudian pelaku melakukan serangan dengan metode *SQL Injection* bertujuan untuk mengubah status pada data transaksi yang berawal status menunggu pembayaran menjadi status selesai pembayaran. Ini dibuktikan oleh *log* peretasan pada bagian data transaksi yang dimana peretasan tersebut menggunakan metode *SQL Injection*.

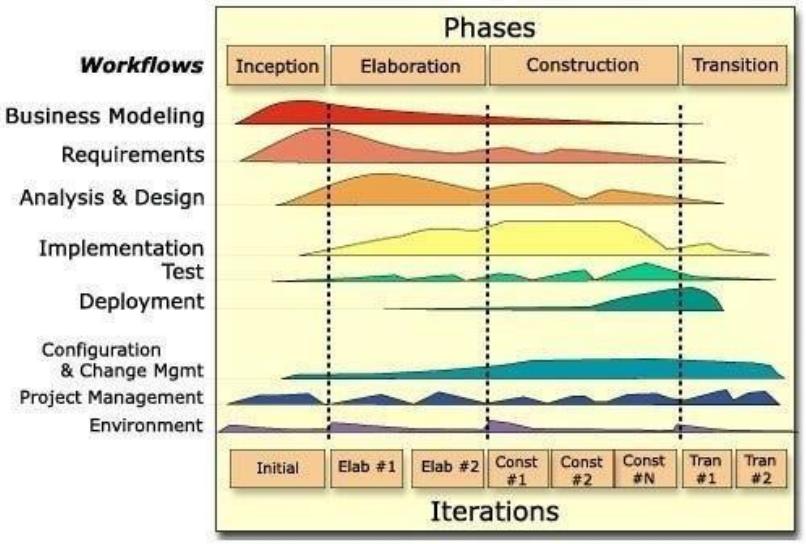
3. Studi Pustaka

   Studi pustaka ini dilakukan dengan menggunakan sumber-sumber seperti jurnal, buku, dan internet. Studi pustaka ini berguna untuk mengetahui landasan teori pengetahuan dan informasi pada penelitian ini, seperti jurnal referensi yang sesuai dengan judul

penelitian yang diambil, jurnal Implementasi Web Service Restful Dengan Autentikasi Json Web Token Dan Algoritma Kriptografi Aes-256 Untuk Aplikasi Peminjaman Laboratorium Berbasis Mobile Pada Universitas Budi Luhur, jurnal Implementasi Algoritma AES-256 Untuk Pengamanan Layanan API Pada Restful Dengan Autentikasi Json Web Tokens, dan jurnal Penerapan Kriptografi AES Class Untuk Pengamanan URL WEBSITE Dari Serangan SQL INJECTION. Jurnal tersebut yang berhubungan dengan permasalahan yang ada. Sumber-sumber ini digunakan untuk melengkapi informasi yang diperlukan dalam mendukung pelaksanaan penelitian ini.

1.9.2 Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah dengan metode *Rational Unified Process* (RUP). Metode RUP merupakan metode pembangunan perangkat lunak yang *iterative* dan *incremental* serta berfokus pada aristektur. RUP memiliki empat tahap yaitu *inception*, *elaboration*, *contruction*, dan *transition*. Metode RUP tergambarkan pada gambar dibawah ini:



Gambar 1. 1 Metode RUP

1. *Inception*

   Tahap ini lebih pada memodelkan proses bisnis yang dibutuhkan (*business modeling*), mendefinisikan kebutuhan akan sistem yang akan dibuat (*requirement*) serta analisis dan desain.

2. *Elaboration*

   Tahap ini lebih pada analisis dan desain sistem serta implementasi sistem yang fokus pada purwarupa sistem (*prototype*).

3. *Construction*

   Tahap ini lebih pada implementasi dan pengujian sistem yang fokus pada implementasi perangkat lunak pada kode program.

4. *Transition*

   Tahap ini lebih pada deployment atau instalasi sistem agar dapat dimengerti oleh user.

1.9.3 Metode Penyelesaian Masalah

Metode yang digunakan oleh penulis yaitu menggunakan algoritma AES-128. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. AES memiliki kecepatan enkripsi dan deskripsi tertinggi, berikutnya *Blowfish*, DES dan IDEA [2]. Algoritma AES juga merupakan sebuah algoritma simetris, yakni menggunakan kunci yang sama saat melakukan proses enkripsi dan dekripsi pada setiap bit[6].

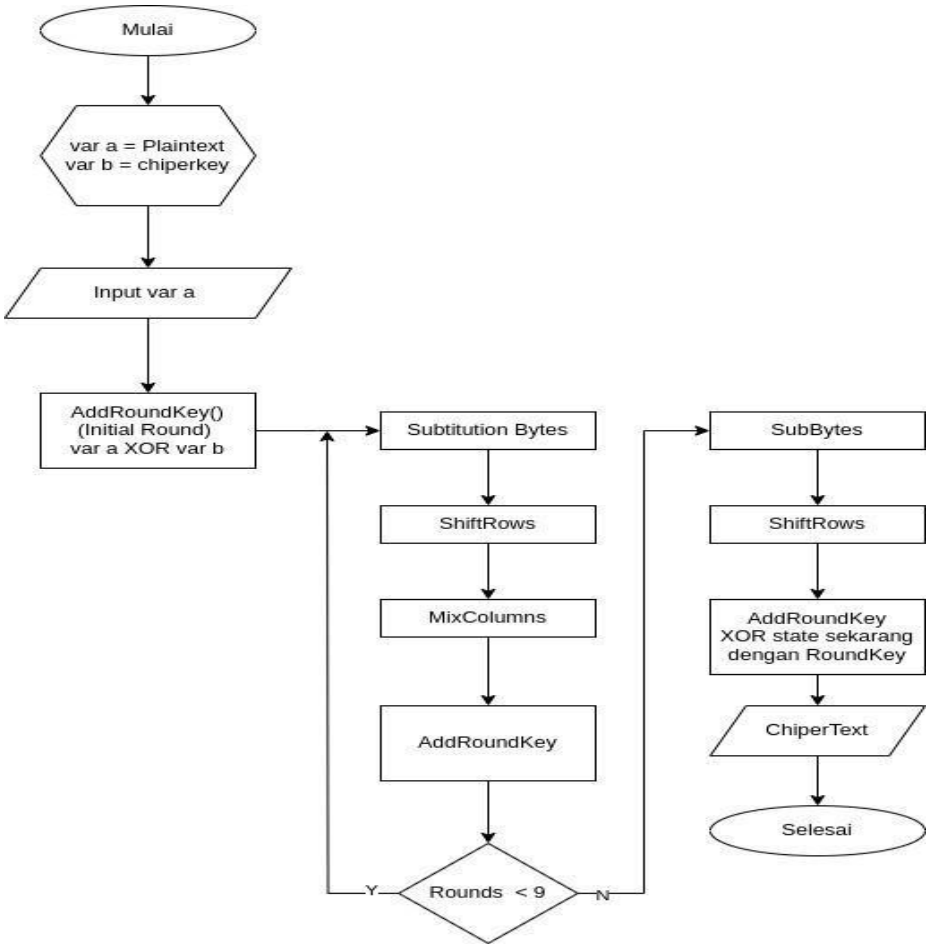
Perbedaan panjang kunci akan mempengaruhi jumlah *round* (putaran) yang akan diimplementasikan pada algoritma AES. Ada 10, 12, atau 14 putaran dalam AES yang sesuai dengan ukuran kunci yang digunakan [1]. Algoritma AES mempunyai tiga parameter yaitu :

a. *Plaintext*, array yang berukuran 16 *byte* yang berisi data masukan.
b. *Ciphertext*, array yang berukuran 16 *byte* yang berisi hasil enkripsi.
c. Kunci, array yang berukuran 16 *byte* yang berisi kunci chiper.

1. Proses Enkripsi

Proses enkripsi algoritma AES-128 terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Pada Awal proses enkripsi, *state* akan mengalami transformasi *byte AddRoundKey*. Setelah itu, *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang

sebanyak Nr (nilai *round*). Proses ini disebut sebagai *round function*. Pada *round* terakhir proses yang dilakukan berbeda dari sebelumnya dimana *state* tidak mengalami transformasi *MixColumns*. Adapun *flow chart* proses enkripsi algoritma AES-128 dapat dilihat pada gambar berikut.

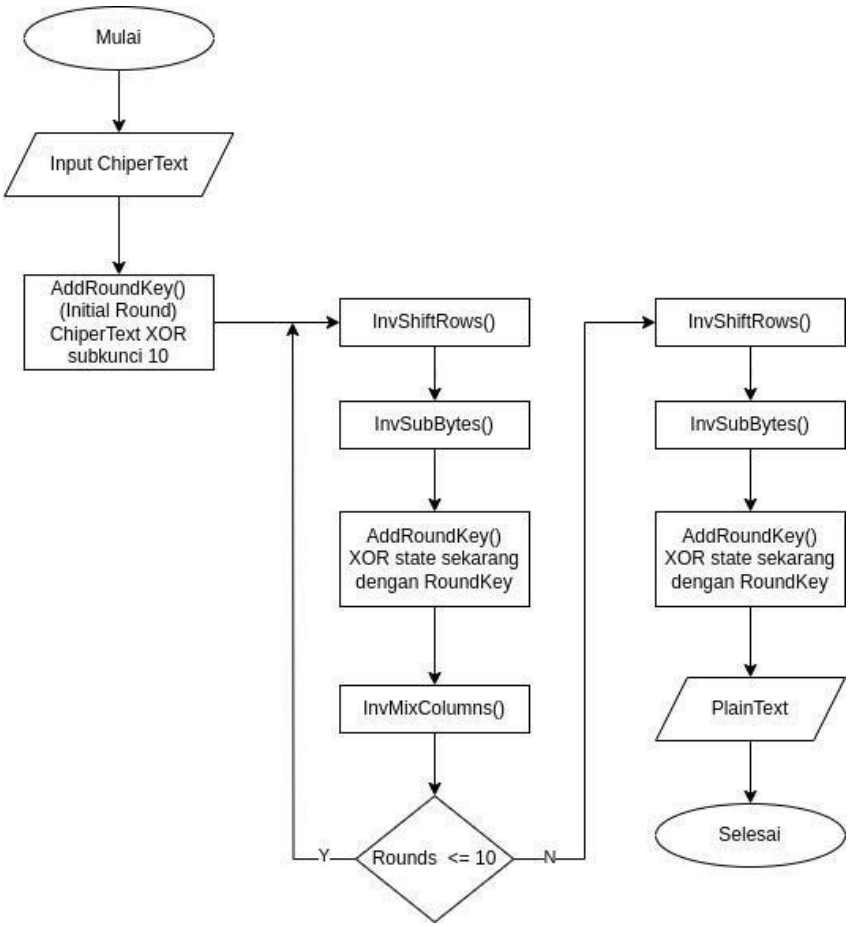


Gambar 1. 2 FlowChart Enkripsi AES

2. Proses Dekripsi

Untuk proses Dekripsi pada AES-128 diperlukan transformasi *cipher* dengan cara dibalik sehingga menghasilkan *inverse cipher*

dengan tahapan yaitu: *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey* [7]. Adapun *flow chart* dekripsi sebagai berikut:



Gambar 1. 3 FlowChart Dekripsi AES

1.10 Jadwal Penelitian

Jadwal pelaksanaan penelitian dibuat dengan tahapan yang jelas dalam bentuk *bar chart*.

Tabel 1. 1 Jadwal Kegiatan

No	Kegiatan		Bulan 2023															
			September				Oktober				November				Desember			
1.	Penyusunan Proposal																	
2.	*Inception* (permulaan)																	
	2.1	Identifikasi Tujuan dan cakupan penelitian.																
	2.2	Identifikasi Kebutuhan dari perusahaan.																
3.	*Elaboration* (Perencanaan)																	
	3.1	Analisis Kebutuhan Arsitektur																

4.	*Construction* (Konstruksi)		
	4.1	Implementasi kode berdasarkan desain	
5.	*Transition* (Transisi)		
	5.1	Menerapkan sistem ke lingkungan produksi.	
6.	Laporan Akhir		

1.11 Sistematika Penelitian

Sistematika penulisan skripsi ini disusun untuk memberikan gambaran umum tentang penelitian yang dilaksanakan. Sistematika penulisan skripsi ini adalah sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini dibahas tentang latar belakang masalah, identifikasi masalah, rumusan masalah, batasan masalah, tujuan

penelitian, manfaat penelitian, pertanyaan penelitian, hipotesis penelitian, metode penelitian, dan sistematika penulisan yang digunakan.

BAB II : LANDASAN TEORITIS

Pada bab ini menjelaskan tentang teori-teori yang berkaitan dengan bahasan penelitian, penelitian sebelumnya, dan kerangka teoritis.

BAB III : ANALISA DAN PERANCANGAN

Pada bab ini menjelaskan tentang analisis sistem, perancangan sistem, dan perancangan antar muka dari perangkat lunak yang dibangun.

BAB IV : IMPLEMENTASI DAN PENGUJIAN

Pada bab ini berisi tentang pengujian sistem untuk mengukur keselarasan fungsi logika, mekanisme operasional perangkat lunak yang dibangun dan implementasi sistem untuk mengukur tingkat efisiensi dan efektifitas penerapan perangkat lunak yang dibangun.

BAB V : KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari keseluruhan uraian bab-bab sebelumnya dan saran-saran yang diharapkan dapat bermanfaat dalam pengembangan sistem selanjutnya