BAB I

PENDAHULUAN

1.1 Latar Belakang

Sangat pentingnya nilai sebuah informasi yang menyebabkan adanya pembatasan akses terhadap orang-orang tertentu.Sebagai contoh tersebarnya informasi ke pihak yang tidak seharusnya (misalnya data sensitif kependudukan) yang dapat menimbulkan penyalahgunaan terhadap data dan juga kerugian bagi pemilik data tersebut. Menurut G. K. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan disebuah sistem yang berbasis informasi, dimana informasi sendiri tidak memiliki arti fisik.

Inti dari permasalahan ini adalah sangat penting nya suatu informasi sensitive untuk di jaga atau di rahasiakan jika tidak di rahasiakan maka akan bias di salah gunakan oleh pihak-pihak yang tidak bertanggung jawab.

Solusi yang bias penulis berikan adalah dengan cara pengamanan data sensitive menggunakan metode rinjdeal ,tetapi bias juga dengan metode lain nya.

Beberapa hal yang sangat penting diperhatikan pada keamanan *web* dan menjadi masalah yang penuh dengan kerentanan adalah *API ENDPOINT. API ENDPOINT sistem* yang menggunakan database sebagai autentikasi pada *user* dan *password* sangat rentan untuk diretas. *SQL injection* merupakan salah satu teknik serangan yang sering

digunakan untuk mengekploitasi sebuah sebuah aplikasi *web*, sebagai akibatnya penyerang bisa mendapatkan akses ilegal (tidak sah) ke sebuah *database* dan juga dapat menyalahgunakan informasi yang didapat [2].

Keamanan informasi sangatlah penting dan dibutukan agar dapat melindungi kerahasiaan. Sering kali kejadian tentang peretasan terhadap sistem informasi berbasis web, karena kurang nya perhatian akan keamanan sistem yang dibangun. Keamanan harus diperhatikan oleh para pengelola atau pun pengembang *web* supaya mempunyai keamanan yang baik dan susah untuk diretas oleh orang-orang yang tidak berkepentingan.

Salah satu teknik pengamanan sistem informasi berbasis *web* adalah dengan menggunakan teknik enkripsi dan dekripsi yang mana kedua nya masuk kedalam bidang ilmu kriptografi. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, tanpa ada gangguan dari pihak ketiga [3]. Pengamanan ini dilakukan dengan cara mengenkripsi data atau informasi menggunakan sebuah kunci khusus. Informasi ini sebelum dienkrip dinamakan *plaintext*. Setelah dienkrip menggunakan sebuah kunci dinamakan *ciphertext* [4].

Rijndael merupakan algoritma kriptografi yang dapat melindungi informasi dengan baik dan juga efisien dalam implementasinya dan juga telah dinobatkan sebagai AES (Advanced Encryption Standard), termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan blok-sandi. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan juga dekripsi serta masukan dan keluaranya berupa

blok dengan jumlah bit tertentu. Rijndael mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun *Rijndael* mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit.

Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Berbagai penelitian telah dilakukan terhadap algoritma *Rijndael* dan serang *SQL Injection*. (Soyjaudah et al., 2004) melakukan penelitian tentang enkripsi yang dilakukan dalam sistem komunikasi untuk melindungi informasi yang dikirim lewat saluran komukasi agar tidak ditangkap dan dibaca oleh pihak yang tidak berwenang . (Majumder dan Saha, 2009) melakukan penelitian tentang *Analysis SQL Injection Attack* . Oleh karena itu penulis mencoba merancang sebuah perlindungan *API ENDPOINT* sistem sebuah *web* menggunakan algoritma Rijndael. Dan melindungi web dari serangan *SQL Injection*.

1.2 Rumusan Masalah

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

1. Bagaimana merancang sebuah enkripsi data menggunakan algoritma Rijndael pada sebuah sistem *API ENDPOINT*.
2. Bagaimana mengimplementasikan algoritma *Rijndael* pada bahasa pemrograman PHP.

1.3 Batasan Masalah

Dari rumusan masalah yang diuraikan diatas agar hasil pembahasan tidak melebar dan lebih terperinci. Adapun ruang lingkup permasalahanya sebagai berikut:

1. Aplikasi ini dirancang menggunakan bahasa pemrograman PHP native.
2. Informasi login di enkripsi menggunakan algoritma Rijndael dengan memanfaatkan library yang ada pada PHP.
3. Perancangan keamanan *API ENDPOINT* menggunakan algoritma *Rijndael.*

1.4 Maksud dan Tujuan Penelitian

Adapun Tujuan dari penelitian ini adalah sebagai berikut:

1. Sebagai salah satu syarat untuk menyelesaikan pendidikan program Strata 1 Teknik Informatika pada Universitas AMIKOM Yogyakarta.
2. Menambah wawasan dalam hal keamanan dalam sebuah informasi.
3. memberi sinyal kepada pihak-pihak yang ingin membuat suatu web informasi, supaya dapat memperhatikan ke amanan sistemnya.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian adalah untuk menjawab berbagai masalah yang telah dirumuskan diantaranya:

1. Merancang *API ENDPOINT* sistem yang dapat mencegah adanya peretasan terhadap data.

2. Membantu mengamankan *API ENDPOINT* sistem dari serangan pihak yang tidak berwenang.

1.6 Metode Penelitian

Metode penelitian yang dilakukan pada penelitian ini sebagai berikut :

1.6.1 Metode Pengumpulan Data

Metode yang digunakan dalam menyusun skripsi ini adalah metode studi pustaka, dengan membaca buku-buku literatur, dokumen, jurnal ilmiah, video tutorial dan informasi lain dari internet yang berkaitan dengan penelitian.

1.6.2 Metode Analisis

Metode analisis yang digunakan dalam menggembangkan aplikasi ini adalah menggunakan metode *SDLC (System Development Life Cycle)*. Pada tahap ini penulis akan melakukan pengamatan, mempelajari, dan memahami sistem kerja pada aplikasi *API ENDPOINT* yang akan diimplementasikan dengan Algoritma *Rijndael*.

1.6.3 Evaluasi Sistem

Evaluasi sistem dilakukan untuk mengetahui apakaha aplikasi yang telah dirancangan dan diimplementasikan sudah berjalan dengan baik atau benar.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penelitian ini terbagi dalam beberapa pokok bahasan, yaitu :

BAB I : PENDAHULUAN

Pada bab ini akan diuraikan mengenai latar belakang masalah, rumusan masalah, batasan masalah, manfaat dan tujuan penelitian, metode penelitian , sistematika penulisan dan rencana kegiatan.

BAB II : LANDASAN TEORI

Bab ini merupakan tinjauan pustaka, mengurai teori-teori yang mendukung judul dan mendasari pembahasan secara detail.

BAB III : ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi tentang tinjauan umum yang menguraikan tentang analisa kebutuhan pada aplikasi dan juga perancangan algoritma Rijndael pada *API ENDPOINT* sistem.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Berisi tentang implementasi serta pengujian terhadap *API ENDPOINT* sistem yang telah dibuat beserta analisisnya.

BAB V : PENUTUP

Bab ini berisi kesimpulan dari pembahasan secara menyeluruh dari perancangan sistem ini dan saran-saran yang ditujukan pada para pengelola ataupun perancang web.