

BAB I

PENDAHULUAN

Pada bab ini akan dibahas tentang latar belakang masalah yang berisi deskripsi latar belakang masalah dari aplikasi yang dibuat kemudian perumusan masalah yang menjelaskan tentang rumusan permasalahan yang ada kemudian tujuan dari dibuatnya tugas akhir ini. Kemudian terdapat juga hipotesa penelitian ini dan yang terakhir terdapat metodologi penelitian yang berisi metodologi penelitian yang digunakan.

1.1. Latar Belakang Masalah

Perkembangan teknologi informasi saat ini telah menjadikan teknologi *cloud computing* yang dahulu masih jarang untuk digunakan menjadi suatu hal yang telah banyak diimplementasikan oleh banyak perangkat lunak yang ada saat ini. *Webservice* menjadi sarana untuk pertukaran informasi yang berpusat pada *cloud server* dari penyedia jasa dari *webservice* kemudian didistribusikan kepada perangkat lunak yang telah melakukan *request* sesuai dengan aturan masing-masing *webservice* yang ada. Proteksi terhadap aplikasi yang menjadikan *webservice* sebagai *core* bisnis dari suatu perusahaan yang menggunakannya juga diperlukan agar *sourcecode* programnya aman dan tidak dapat ditiru oleh perusahaan kompetitor sejenis [7]. Pada saat yang bersamaan, javascript sebagai bahasa pemrograman web yang dipakai oleh kebanyakan website modern saat ini telah digunakan juga untuk pengembangan aplikasi *console game*, tablet, maupun *smartphone*. Javascript juga merupakan *core* dari teknologi *webservice* yang saat ini banyak digunakan oleh *cloud server* penyedia layanannya. Perkembangan dari aplikasi *mobile* saat ini telah berkembang dengan cepat dibandingkan dengan aplikasi berbasis *web* karena kemudahan untuk menggunakan aplikasi yang semakin mudah dan ringkas [8].

Sistem proteksi javascript yang ada pada saat ini menggunakan metode pengacakan *sourcecode* javascript atau yang biasa disebut dengan obfuskasi. Hasil proses obfuskasi *sourcecode* masih memungkinkan untuk dilakukan proses deobfuskasi dengan menggunakan perangkat lunak tertentu untuk merapihkan javascript yang telah di obfuskasi dan kemudian dilakukan proses *reverse-engineering* dan *sourcecode-cloning* sehingga sistem proteksi dengan menggunakan metode obfuskasi belum aman. Tugas akhir yang akan dibuat difokuskan untuk melakukan proteksi enkripsi untuk melindungi javascript pada aplikasi *mobile* berbasis *phonegap*.

1.2. Perumusan Masalah

Bagaimana mengamankan javascript pada client-side aplikasi android yang dibangun menggunakan *phonegap*, apabila dilakukan ekstraksi *file installer*-nya sehingga semua *sourcecode* javascriptnya bisa dilihat dan dilakukan *reverse-engineering* sehingga aplikasi menjadi mudah untuk ditiru dan dilakukan eksploitasi untuk hal-hal yang tidak diinginkan.

1.3. Tujuan

Mengimplementasikan proteksi enkripsi pada javascript yang terdapat pada aplikasi android sebelum aplikasi tersebut didistribusikan secara luas, kemudian membuat *service server*

decriptor untuk melakukan proses dekripsi dari sintaks javascript yang telah terenkripsi agar dapat digunakan oleh aplikasi *mobile*.

1.4. Batasan Masalah

Pada sistem enkripsi javascript ini tidak ada pertukaran kunci dari aplikasi *mobile* ke server, sehingga *key* yang digunakan sudah ditentukan pada saat enkripsi dan dekripsi. Digunakan untuk aplikasi *native* android yang dibangun menggunakan html, css dan javascript serta di *build* menggunakan phonegap. Menggunakan komunikasi ajax post ketika mengirimkan javascript terenkripsi dari *mobile* aplikasi ke server decriptor.

1.5. Hipotesa

Dengan melakukan enkripsi terhadap javascript pada aplikasi *mobile*, maka javascript menjadi tidak bisa dimengerti tetapi tidak merubah fungsinya, Serta memberikan perlindungan dari metode *reverse-engineering* dan *sourcecode-cloning* yang bisa dilakukan pada aplikasi *mobile*. Perlindungan enkripsi ini dilakukan ketika *request* dan *response* dari *service provider server*, sehingga hasil dekripsi javascript dari *service provider* adalah javascript yang akan dipakai oleh aplikasi *mobile* yang menjalankannya. Proses enkripsi menggunakan algoritma AES karena algoritma ini dapat melakukan proses enkripsi dengan cepat pada sistem yang memiliki spesifikasi komputasi rendah. Hal ini bagus karena tidak memakan biaya yang besar untuk organisasi bisnis yang akan mengimplementasikan sistem ini.

Adapun judul dari penelitian yang akan dibuat oleh penulis adalah,

Javascript Protection and Encryption menggunakan Advance Encryption Standard (AES) Symetric-Key Algorithm Untuk Aplikasi Mobile Berbasis Phonegap.

1.6. Metodologi Penelitian

Metodologi penelitian yang digunakan tugas akhir ini yaitu dengan langkah-langkah sebagai berikut.

- a. Studi Pustaka
Studi Pustaka dilakukan dengan mempelajari literatur-literatur yang berkaitan dengan enkripsi simetris, enkripsi AES, dan mengenai sistem obfuskasi javascript.
- b. Analisis Kebutuhan
Pada tahap ini akan dilakukan analisis kebutuhan terhadap perancangan sistem enkripsi javascript pada aplikasi *mobile* dengan menggunakan Advanced Encryption Standard simetric-key algorithm agar sistem yang dibuat mampu melindungi sintaks javascript dari proses *reverse engineering*.
- c. Perancangan Sistem
Pada tahap ini dilakukan perancangan sistem dengan menyelaraskan javascript yang telah terenkripsi pada *filetext* dan algoritma AES yang akan dipakai dalam sistem ini, serta merancang integrasi setiap perangkat sehingga dapat berjalan

dengan baik dan dapat mensimulasikan proses enkripsi pesan pada sistem dengan AES.

d. Implementasi dan Pengujian Sistem

Pada tahap ini sistem akan dibuat sesuai rancangan dan sumber yang ada. Menguji dan

menganalisis performansi enkripsi AES pada sistem proteksi javascript yang melakukan komunikasi dengan server decryptor. Pada bagian ini dipaparkan pengujian dan analisis hasil perancangan sistem proteksi javascript pada aplikasi *mobile* menggunakan enkripsi AES dapat terimplementasi dengan baik dan membandingkan performansi dari segi waktu serta ukuran *file* suatu javascript dengan ditambahkan enkripsi AES dengan *key* 128bit.

e. Penyusunan Laporan Tugas Akhir dan Kesimpulan.

Pada tahap ini dilakukan penyusunan laporan terhadap penelitian yang telah dilaksanakan

yang tentunya akan menghasilkan suatu kesimpulan. berisi kesimpulan hasil pengujian dan

analisis penelitian serta berisi saran untuk pengembangan lebih lanjut.

