

Abstrak

Semakin berkembangnya teknologi informasi pada saat ini telah menjadikan pengembangan aplikasi berbasis *mobile* semakin banyak dan digemari karena tampilan antarmuka yang sederhana tetapi masih dapat berfungsi secara maksimal. *Webservice* menjadi pilihan untuk aplikasi *mobile* dalam memperoleh informasi yang dibutuhkan dari server penyedia layanan informasi. Aplikasi *mobile* yang di bangun menggunakan *phonegap* dapat dibuat menggunakan bahasa pemrograman berbasis web seperti *html*, *css* dan *javascript*. Untuk aplikasi yang dibangun menggunakan bahasa pemrograman web, untuk dapat melakukan akses ke *webservice* dapat menggunakan *javascript* untuk melakukan proses pertukaran datanya. Informasi tentang *webservice* yang akan diakses beserta proses bisnis dari aplikasi *mobile* tersebut terdapat pada *file javascript* yang ada di dalam aplikasi *mobile* dan didistribusikan kepada user yang ingin menggunakannya.

Salah satu kelemahan aplikasi *mobile* ini adalah *sourcecode javascript* yang berisi informasi bisnis proses dapat dilihat oleh semua orang yang melakukan ekstraksi terhadap aplikasi *mobile* dan bisa dilakukan *reverse-engineering* dan *sourcecode-cloning* terhadap *javascript* tersebut. 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.

Penelitian ini bertujuan untuk memperkuat sistem proteksi *javascript* menggunakan algoritma enkripsi AES untuk melindungi *javascript* yang ada pada pada aplikasi *mobile* sehingga sekalipun *user* dapat mengakses *sourcecode javascript* tetapi ia tetap tidak akan bisa melakukan proses *reverse-engineering* dan *sourcecode-cloning* karena sudah terproteksi menggunakan algoritma enkripsi AES.

Aplikasi yang dibuat terdiri aplikasi *mobile*, server aplikasi dan aplikasi enkripsi untuk mengenkripsi dan menyisipkan *javascript* ke dalam *file html*. Berdasarkan hasil penelitian ini dapat dibuktikan bahwa dengan menggunakan metode yang diajukan, proses *reverse-engineering* dan *sourcecode-cloning* tidak dapat dilakukan karena *sourcecode javascript* telah terlindungi dan membutuhkan kunci yang tepat untuk dapat membuka *javascript* yang telah terenkripsi.

Kata Kunci : Javascript Protector, Advance Encryption Standard, Rijndael, Reverse-Engineering, Mobile Application, Phonegap, Obfuskasi.