BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Di zaman sekarang ini, bertukar informasi tidak lagi menjadi hal yang sulit dilakukan. Banyak teknologi revolusioner bermunculan yang mendukung kemudahan pertukaran informasi, seperti telepon rumah, internet, *websites,* dan *mobile devices*. Salah satu dari kemudahan tersebut adalah pengiriman pesan ke banyak orang secara bersamaan, atau dikenal dengan sebutan *broadcast messaging. Broadcast* datang dalam berbagai macam bentuk, antara lain *e-mail*, layanan *group messaging* seperti Skype, *cell broadcast* menggunakan *short messaging service* (SMS) atau rekaman suara. *Broadcast* umumnya digunakan untuk menyebarkan informasi penting atau di dalam dunia *marketing* (Wilson, Tracy V., 2007), *broadcast* dimanfaatkan untuk mempromosikan produk (*Degree Directory*, 2014). Selain menggunakan *broadcast*, di dunia *marketing* saat ini juga sudah mulai menerapkan penggunaan *Location Based Service* (LBS) untuk memberikan pesan promosi atau konten yang relevan dan sesuai sasaran. Tidak hanya dunia *marketing* saja, beberapa layanan *social media* seperti Facebook, Twitter dan Path juga menerapkan penggunaan LBS pada fitur layanan mereka.

LBS menggunakan teknologi seperti *global positioning sytem* (GPS), atau jaringan komunikasi seluler untuk menentukan posisi pengguna, hanya saja penggunaan GPS dan jaringan seluler pada LBS memiliki kelemahan karena tidak dapat digunakan untuk menentukan posisi pengguna dalam gedung. Selain GPS dan jaringan seluler yang digunakan dalam LBS, terdapat satu teknologi lagi,

yang dikenal dengan nama iBeacon. Penggunaan iBeacon pada LBS dikarenakan iBeacon mengatasi kelemahan pada GPS dan jaringan seluler, yaitu iBeacon dapat menentukan lokasi pengguna di dalam gedung atau ruangan. iBeacon merupakan teknologi yang dikembangkan oleh Apple Inc.. iBeacon sendiri bukan merupakan teknologi baru karena iBeacon memanfaatkan teknologi yang sudah ada yakni Bluetooth 4.0 (sebutan lainnya: *Bluetooth Low Energy*) (Ranger, Steve, 2014).

Di tengah kehebatannya, teknologi juga ternyata tidak terlepas dari masalah. Beberapa teknologi dalam penggunaannya membutuhkan pengamanan yang tepat. Sudah banyak penjahat *cyber* bermunculan untuk menyerang dunia maya di internet, melakukan penculikan, atau bahkan mencuri informasi-informasi penting baik pribadi maupun negara. Para pengguna dunia maya juga banyak yang lalai dalam mengamankan informasi pribadinya. Lihat saja tahun 2014, foto-foto selebriti besar dunia tersebar di dunia maya karena pengguna menggunakan *password* yang mudah ditebak (Kastrenakes, Jacob, 2014).

Kelalaian yang terjadi juga tidak hanya dari sisi pengguna, terkadang penyedia layanan juga lalai dalam mengamankan informasi penggunanya. Di tahun 2013 saat Adobe mengalami serangan, ratusan jutaan *password* milik para pengguna layanan Adobe tersebar *online*. Menurut Chris Welch di tahun 2013, *password* pengguna Adobe dienkripsi menggunakan teknik enkripsi yang diragukan. Walaupun tidak disebutkan enkripsi yang digunakan, Adobe menggunakan mode operasi *electronic codebook* (ECB) untuk enkripsinya (Hern, Alex, 2013), sebuah mode operasi yang tidak aman karena apabila terdapat dua buah *password* yang sama, maka hasil enkripsi keduanya juga akan sama. Tidak hanya itu, Adobe juga ternyata tidak mengenkripsi *password hint* milik

penggunanya, yang tentunya dapat membuat penjahat *cyber* menebak *password* para pengguna layanan Adobe.

Pengamanan informasi dapat dilakukan dengan menggunakan enkripsi dan enkripsi yang merupakan standar saat ini adalah *Advanced Encryption System* (AES) karena keamanannya dan keefisienannya pada saat implementasi (Surian, 2006). Sebelum penelitian kali ini, sudah pernah ada penelitian yang mengimplementasikan algoritma AES-128 pada perangkat *mobile* berbasis Android yang dilakukan oleh saudara Joko Tri Susilo Widodo dalam publikasinya yang berjudul *"Implementasi Algoritma Kriptografi AES 128 bit Sebagai Pengaman SMS pada Smartphone Berbasis Android"*. Pada penelitian kali ini penulis akan menggabungkan enkripsi dengan teknologi iBeacon. Penulis akan mengimplementasikan algoritma enkripsi AES ke dalam aplikasi BroadcastMe yang memanfaatkan teknologi iBeacon.

1.2. Rumusan Masalah

Berdasarkan latar belakang, penulis merumuskan masalah yang akan diteliti, yaitu bagaimana mengimplementasikan algoritma enkripsi AES-128 pada aplikasi BroadcastMe untuk mengamankan informasi yang dikirimkan kepada perangkat iOS lainnya.

1.3. Batasan Masalah

Berikut ini adalah batasan masalah dalam penelitian ini.

a. Informasi yang dikirim merupakan informasi dalam bentuk teks.

b. Blok kunci yang digunakan untuk aplikasi ini yaitu 128 bit.

1.4. Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan penelitian ini adalah mengimplementasikan algoritma AES-128 untuk mengamankan informasi yang dikirimkan ke perangkat iOS yang berada dalam jangkauan iBeacon melalui aplikasi BroadcastMe.

1.5. Manfaat Penelitian

Penelitian ini diharapkan memiliki manfaat untuk mengamankan informasi yang dikirimkan menggunakan BroadcastMe ke perangkat iOS lainnya.

1.6. Sistematika Penulisan Laporan Penelitian

Sistematika yang digunakan dalam penulisan laporan ini adalah sebagai berikut.

BAB I LATAR BELAKANG

Bab ini berisikan tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan laporan.

BAB II LANDASAN TEORI

Bab ini berisikan tentang uraian-uraian dari teori-teori yang relevan dan digunakan dalam penelitian ini.

BAB III METODE PENELITIAN DAN PERANCANGAN SISTEM

Bab ini berisikan tentang metode penelitian serta rancangan pengembangan sistem yang dibuat.

BAB IV IMPLEMENTASI DAN HASIL PENELITIAN

Bab ini berisikan tentang hasil implementasi dari rancangan pengembangan dan pengujian atas penelitian yang dilakukan serta hasil dari pengujian.

BAB V SIMPULAN DAN SARAN

Bab ini berisikan tentang simpulan dari hasil penelitian atas tujuan penelitian serta saran untuk para pembaca yang ingin melakukan pengembangan lebih lanjut terhadap penelitian ini.