



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Berbagai macam kartu dimiliki oleh orang yang disimpan di dalam dompetnya. Hal ini dapat dilihat dalam survei yang dilakukan pada tanggal 19 Februari 2017 sampai 24 Februari 2017 dengan tujuh puluh tiga responden. Dari tujuh puluh tiga responden, empat puluh satu responden memiliki lima sampai sepuluh kartu di dalam dompetnya. Dua puluh tiga responden memiliki kurang dari lima kartu, dan sembilan responden memiliki lebih dari sepuluh kartu. Dari beberapa kartu tersebut, cenderung timbul suatu masalah bagi pemilik kartu.

Salah satu contoh jenis kartu yang menimbulkan masalah bagi pemilik adalah kartu Surat Ijin Mengemudi (SIM). Pemilik kartu harus pergi ke kantor Sistem Administrasi Manunggal Satu Atap (SAMSAT) untuk dapat membuat kartu SIM yang baru ketika kartu SIM yang lama rusak atau hilang. Timbulnya masalah tersebut juga ada pada salah satu kartu bank yaitu kartu Anjungan Tunai Mandiri (ATM). Hal tersebut dapat dilihat pada survei yang telah dilakukan, sebanyak tiga puluh lima responden pernah mengalami masalah dengan kartu ATM. Masalah yang pernah dialami responden adalah kartu ATM rusak atau kedaluwarsa sehingga harus diganti dengan kartu yang baru, kartu ATM ditelan oleh mesin, dan kartu ATM harus segera ditutup atau diblokir dikarenakan kartu ATM hilang.

Dengan berbagai masalah yang cenderung ditimbulkan dalam pemakaian kartu ATM, maka diperlukan sebuah solusi bagaimana caranya melakukan transaksi pada mesin ATM tanpa pemakaian kartu ATM. Salah satu solusi yang dapat digunakan adalah menggunakan mekanisme One Time Password sebagai

pengganti penggunaan kartu ATM agar transaksi pada mesin ATM dapat dilakukan. Terdapat penelitian terdahulu (Acharya dkk., 2013) tentang “Two Factor Authentication Using Smartphone Generated One Time Password” yang mengimplementasikan One Time Password untuk proses transaksi perbankan, maka pemakaian kartu ATM dapat digantikan oleh One Time Password.

Di dalam transaksi mesin ATM terdapat proses validasi dan verifikasi. Proses validasi terjadi saat kartu ATM dimasukkan untuk mengakses mesin ATM. Sedangkan proses verifikasi dilakukan dengan memasukkan informasi pribadi seperti PIN, nama ibu, no rekening, tanggal lahir, atau nomor telepon yang didaftarkan (Acharya dkk., 2013).

One Time Password (OTP) adalah sebuah metode otentikasi dengan menggunakan password yang hanya sekali pakai. OTP memiliki jangka waktu kedaluwarsa yang membuat OTP tidak dapat dipakai ketika sudah melewati waktu kedaluwarsa. OTP tidak rentan terhadap serangan *replay-attacks* dikarenakan OTP hanya dapat dipakai sekali (Hamdare dkk., 2014). OTP yang dihasilkan digunakan sebagai proses validasi pengganti kartu pada mesin ATM. OTP didapatkan ketika pengguna berada di lokasi mesin ATM tertentu.

Lokasi mesin ATM dapat diperoleh dari pemanfaatan perangkat teknologi terkini yaitu Bluetooth Low Energy Beacon. Bluetooth Low Energy (BLE) Beacon adalah sebuah perangkat elektronik kecil dengan Bluetooth untuk mengirimkan sinyal kepada radius Bluetooth yang telah ditentukan (Rijswijk-Deij, 2013). Sinyal yang dikirimkan dapat disesuaikan kebutuhan dengan perubahan pada nilai konfigurasi kekuatan sinyal BLE Beacon. *Smartphone* yang memiliki aplikasi untuk menerima sinyal tersebut dapat merespon jika *smartphone* berada pada radius

pengiriman sinyal BLE Beacon. Berbagai aktivitas dapat dilakukan ketika *smartphone* menerima sinyal dari BLE Beacon. Menampilkan pesan pada aplikasi, mengirimkan data ke server, dan melihat informasi sebuah produk dalam aplikasi merupakan contoh aktivitas yang dapat diterapkan dengan menggunakan BLE Beacon.

BLE Beacon memiliki beberapa keunggulan jika dibandingkan dengan NFC dan RFID (Eaton, 2013). Berbeda dengan NFC dan RFID yang perlu didekatkan ke perangkat *reader* untuk dapat membaca sinyal. BLE Beacon tidak perlu didekatkan dengan *smartphone* untuk dapat dilakukan pembacaan sinyal. Selain itu, jika dibandingkan dengan *Wireless Fidelity* atau yang biasa disebut dengan WiFi, BLE Beacon merupakan suatu alat yang *programmable* sehingga sinyal yang akan dipancarkan oleh BLE Beacon dapat dimodifikasi. Sedangkan WiFi tidak dapat dimodifikasi di dalam mekanisme pengiriman sinyal.

AES merupakan salah satu standar enkripsi yang digunakan dan diakui oleh pemerintah Amerika Serikat. AES merupakan metode kriptografi dengan kunci simetris dan salah satu standar enkripsi pertama yang dapat diakses publik dan sandi terbuka yang disetujui oleh NSA untuk informasi rahasia (Putra, 2015).

Oleh karena itu, dibutuhkan sebuah sistem yang mengimplementasikan One Time Password sebagai pengganti kartu ATM dengan memanfaatkan teknologi BLE Beacon dan kriptografi AES 128-bit yang diharapkan dapat mengurangi masalah yang cenderung timbul pada pemakaian kartu ATM.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang dijelaskan sebelumnya, masalah yang dirumuskan adalah bagaimana cara mengimplementasikan One Time Password

sebagai pengganti kartu ATM dengan teknologi BLE Beacon dan keamanan AES-128 bit?

1.3 Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut.

- A. Setiap nasabah terdaftar di dalam sistem yang telah memiliki implementasi One Time Password.
- B. Aplikasi yang dibuat menggunakan Ionic Framework dan NGCordova Library untuk mendukung *hybrid programming*.
- C. Metode AES-128 bit yang digunakan adalah Cipher Block Chaining (CBC). Dengan ukuran data 128 bit dimana key merupakan nomor telepon selular yang telah didaftarkan.
- D. Library crypto-js dan openssl digunakan untuk mengimplementasikan AES-128 Bit CBC dalam sistem yang dibuat.
- E. One Time Password dihasilkan melalui library yang merujuk pada RFC 6238 tentang Time Based One Time Password.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan dari dilakukannya penelitian ini adalah mengimplementasikan One Time Password sebagai pengganti kartu ATM dengan teknologi BLE Beacon dan keamanan AES-128 bit.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari implementasi One Time Password sebagai pengganti kartu ATM dengan teknologi BLE Beacon dan keamanan AES-128 bit adalah permasalahan yang cenderung muncul pada penggunaan kartu ATM dapat

dikurangi melalui One Time Password yang digunakan sebagai pengganti kartu ATM.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penyajian laporan skripsi ini adalah sebagai berikut.

1. BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penelitian yang dilakukan dalam penelitian.

2. BAB II LANDASAN TEORI

Bab ini menjelaskan teori dan konsep dasar yang mendukung terkait dengan permasalahan yang dibahas di dalam penelitian.

3. BAB III METODE DAN PERANCANGAN SISTEM

Bab ini menjelaskan mengenai metode-metode yang digunakan dalam penelitian seperti metode pengumpulan data, metode perancangan sistem, serta rancangan sistem yang dibuat.

4. BAB IV IMPLEMENTASI DAN UJI COBA

Bab ini menjelaskan implementasi aplikasi yang telah dilakukan serta uji coba penelitian yang dilakukan beserta dengan hasil analisis uji coba.

5. BAB V SIMPULAN DAN SARAN

Bab ini membahas tentang simpulan dari hasil penelitian terhadap tujuan penelitian dan saran untuk pengembangan penelitian lebih lanjut.