BAB I PERSYARATAN PRODUK

I.1. Pendahuluan

Perkembangan teknologi mengakibatkan manusia selalu ingin mendapatkan kebutuhan pokoknya secara cepat dan akurat. Informasi dapat dikatakan sebagai salah satu kebutuhan pokok bagi manusia. Informasi berperan penting dalam menentukan kelangsungan hidup manusia. Kemajuan teknologi informasi berjalan begitu cepat dan dapat diterima oleh masyarakat, karena dapat memberikan efisiensi dan efektifitas yang mendukung peningkatan sumber daya manusia. Salah satu contoh hasil dari teknologi informasi adalah kemudahan dalam menyampaikan informasi kepada masyarakat.

Salah satu contoh pemanfaatan teknologi saat ini adalah adanya Internet Banking. Istilah Internet Banking bukan lagi asing di kalangan masyarakat Indonesia. Hal tersebut disebabkan semakin banyaknya perbankan nasional menggunakan metode Internet Banking, sebagai fasilitas transaksi yang dapat diakses oleh nasabah kapanpun dan dimanapun. Dengan menggunakan media koneksi internet agar bisa mengakses fasilitas Internet Banking tersebut. Adanya Internet Banking maka nasabah dapat melakukan transaksi, tanpa harus datang langsung ke Bank untuk melakukan transaksi.

Disisi lain seiring dengan pemanfaatan Internet Banking, maka akan semakin banyak pihak-pihak yang mencari kelemahan dari sistem Internet Banking yang ada. Mulai dari keamanan sistem yang diberikan hingga keamanan saat melakukan transaksi. Hal ini merupakan resiko utama dalam penerapan Internet Banking. Dengan adanya hal tersebut dapat menimbulkan ketidaknyamanan bagi nasabah untuk menggunakan pelayanan yang ada pada Bank. Karena tidak terjaminnya keamanan sehingga dapat merugikan nasabah. Ada beberapa tipe serangan yang dilakukan, antara lain *Active Attack* dan *Passive Attack*. Berikut istilah

serangan untuk *Active Attack* adalah *Masquerade, Replay, Modification of Messages,* dan *Denial of Service*. Sedangkan untuk *Passive Attack* antara lain *Release of Message Contents* dan *Traffic Analysis*.

Untuk meminimalkan terjadinya penyerangan terhadap Internet Banking yang diuraikan sebelumnya. Maka ada beberapa hal yang harus diperhatikan dari sebuah sistem Internet Banking antara lain konsep kriptografi meliputi kerahasiaan, integritas data, dan otentikasi.

Dengan memahami konsep pengamanan data. Maka dibuatlah sebuah aplikasi yang akan menggunakan konsep keamanan dalam melakukan transaksi pada Internet Banking.

I.1.1. Tujuan

Tujuan dibuatnya Implementasi Transaksi Internet Banking dengan Otentikasi Pesan Singkat ini antara lain:

1. Untuk menanggulangi kebocoran informasi nomor pin dari nasabah. Maka akan menggunakan metode pemberian nomor pin transaksi kepada nasabah menggunakan media pesan singkat.
2. Meningkatkan keamanan pada saat nasabah melakukan transaksi, dengan menggunakan otentikasi pertanyaan yang bersifat pribadi.
3. Menerapkan konsep kriptografi dengan menggunakan protokol *HTTPS* atau *SSL*. Dengan menggunakan protokol tersebut, maka dapat menjaga kerahasiaan dari jalur komunikasi antara *Server* dan *Clinet*.

I.1.2. Ruang Lingkup Proyek

Melihat dari sisi ruang lingkup dari Implementasi Internet Banking dengan Otentikasi Pesan Singkat ini, maka sistem yang akan dibuat memiliki beberapa batasan masalah sebagai berikut :

1. Pemberian nomor pin yang yang diterima pengguna, hanya digunakan satu kali dalam transaksi. Dimana pemberian nomor pin tersebut pengguna melakukan transaksi, dan pengguna melakukan aktifasi *account*.

2. Penerapan konsep kriptografi dengan menggunakan protokol *HTTPS*. Maka jalur komunikasi akan dienkripsi, sehingga meminimalisasikan terjadinya kebocoran informasi transaksi pengguna.
3. Untuk meningkatkan keamanan dalam transaksi. Maka digunakan beberapa proses validasi berupa pertanyaan yang harus dijawab oleh pengguna, dan proses validasi nomor pin.
4. Konsep *SMS Broadcast* yang dilakukan bersifat satu arah. Sehingga hanya digunakan untuk mengirimkan nomor pin kepada pengguna, Maka pengguna tidak perlu membalas pesan yang diterima.

I.1.3. Definisi, Akronim, dan Singkatan

Dalam penyusunan laporan dari aplikasi Implementasi Internet Banking dengan Otentikasi Pesan Singkat ini, terdapat berbagai Definisi, Akronim, dan Singkat anantara lain sebagai berikut :

1. *Active attack* adalah penyerangan pada data yang dilakukan oleh penyusup dengan merubah kuantitas informasi dari data tersebut.
2. *Passive attack* adalah penyerangan pada data yang dilakukan oleh penyusup dengan tidak merubah kuantitas informasi dari data tersebut.
3. *SMS Broadcast* adalah suatu cara dalam pengiriman pesan singkat yang dimana pesan singkat tersebut langsung dikirimkan ke semua *client.*
4. *Client* adalah sebuah sistem yang diperbolehkan untuk masuk ke dalam sebuah jaringan komunikasi dan mengambil atau menggunakan segala sumber daya yang tersedia didalam jaringan tersebut.
5. *Server* adalah sebuah sistem yang menydiakan sumber daya informasi, sehingga dapat digunakan oleh pengguna.
6. *Otentikasi* adalah identifikasi dimana kedua pihak harus saling berkomunikasi, dan saling mengenal.
7. *Integritas Data* adalah menjaga data dari modifikasi atau menjaga keutuhan data yang dicoba untuk diubah oleh penyerang.

8. *Masquerade* atau Penyamaran dilakukan dengan cara seseorang melakukan pengiriman pesan dengan menggunakan identitas orang lain.
9. *Replay* atau Pengiriman Pesan Kembali yaitu penyerang melakukan perubahan terhadap data kepada alamat yang dituju. Sehingga sudah tidak terjamin keasliannya.
10. *Modification of Message* adalah merubah pesan yang akan dikirim sehingga informasi yang didapat berubah, hampir sama dengan metode *Replay.*
11. *Denial of Service* adalah mengganggu komputer *server*, sehingga membuat komputer *server* menjadi kelebihan beban dalam melayani permintaan.
12. *Release of Message* yaitu bertujuan untuk mengetahui data yang dikirim ke pengguna.
13. *Traffic Analysis* yaitu tidak hanya bertujuan untuk mengetahui isi dari data yang sedang ditransfer, melainkan juga pola pengiriman data yang dikirim.

I.1.4. Overview Laporan

Penyajian laporan kerja dibagi menjadi beberapa bab dengan tujuan. Sehingga mempermudah pencarian data yang dibutuhkan, serta menunjukan penyelesaiaan pekerjaan yang sistematis. Pembagian bab tersebut adalah sebagai berikut:

1. BAB I (Persyaratan Produk), dalam bab ini dijelaskan tujuan dari pembuatan aplikasi yang dibuat, ruang lingkup proyek, definisi akronim singkatan, overview laporan, perspektif produk, fungsi produk, karakteristik pengguna, batasan-batasan, asumsi ketergantungan, dan penundaan persyaratan.
2. BAB II (Spesifikasi Produk), pada bab ini membahas mengenai antar muka dengan pengguna, antarmuka perangkat keras, antarmuka

perangkat lunak, antarmuka komunikasi, dan fitur produk perangkat lunak.

3. BAB III (Desain Perangkat Lunak), dalam bab ini akan dijelaskan tentang pendahulan yang merupakan identifikasi dan overview sistem, keputusan desain perangkat lunak secara keseluruhan, dan arsitektur perangkat lunak.
4. BAB IV (Pengembagan Sistem), pada bab ini akan dijelaskan mengenai perencangan tahap implementasi yang berupa pembagian dan keterkaitan antar modul, dan perjalanan tahap implementasi.
5. BAB V (Testing dan Evaluasi Sistem), Pada bab ini dijelaskan mengenai recana pengujian sistem terimplementasi, perjalanan metodologi pengujian, dan ulasan hasil evaluasi.
6. BAB VI (Kesimpulan dan Saran), pada bab ini dibahas tentang kesimpulan dan saran terhadap sistem yang telah dibuat.

I.2. Gambaran Keseluruhan

Implementasi Transaksi Internet Banking dengan Otentikasi Pesan Singkat. Merupakan salah satu pengimplementasian tentang keamanan dari transaksi seorang nasabah dalam melakukan transaksi menggunakan layanan Internet Banking. Implementasi Transaksi Intenet Banking dengan Otentikasi Pesan Singkat dibuat untuk meminimalisasikan terjadinya kebocoran terhadap nomor pin atau *password* dari nasabah saat melakukan transaksi yang dilakukan oleh para penyerang, sehingga bisa merugikan berbagai pihak.

Pada applikasi Implementasi Transaksi Intenet Banking dengan Otentikasi Pesan Singkat, menggunakan cara pemberian nomor pin yang hanya bisa digunakan untuk satu kali transaksi saja. Dimana nomor pin yang didapatkan dikirim langsung ke pengguna, degan media telepon genggam. Dengan memanfaatkan konsep *SMS Broadcast* yang akan membantu dalam pengiriman nomor pin ke pengguna yang akan dijadikan nomor pin dalam melakukan transaksi dan proses aktifasi *account*.

Penerapan protokol *HTTPS* atau *SSL* pada aplikasi Implementasi Transaksi Intenet Banking dengan Otentikasi Pesan Singkat ini. Merupakan sebuah cara penggunaan media enkripsi data pada jalur komunikasi yang menghubungkan antara *Clinet* dan *Server*. Sehingga dapat menyulitkan para penyerang dalam pencarian informasi penting.

I.2.1. Perspektif Produk

Aplikasi Implementasi Transaksi Internet Banking dengan Otentikasi Pesan Singkat ini, menggunakan koneksi *HTTPS* dengan penggunaan modul *SSL* (*Socket Secure Layer*). Dimana berfungsi sebagai penanggulangan penyadapan data yang sering terjadi. Dengan penggunaan metode tersebut data yang berjalan pada jalur komunikasi akan langsung dienkripsi dengan menggunakan metode-metode enkripsi yang ada. Sedangkan dengan adanya pertanyaan-pertanyaan yang bersifat pribadi dan rahasia, maka akan mengurangi kemudahan para penyerang untuk dapat melakukan transaksi. Dalam pembagian nomer rahasia pada saat transaksi, maka digunakan konsep *SMS Broadcast*. Sehingga semakin meninggkatkan keamanan dalam bertransaksi.

Pada pengembangan aplikasi ini akan digunakan suatu aplikasi tambahan untuk mencoba melakukan serangan *SQL Injection*, dan *Sniffing Data* yang dimana kerap tejadi pada sebuah transaksi *online*.

I.2.2. Fungsi Produk

Fungsi dari applikasi Implementasi Transaksi Intenet Banking dengan Otentikasi Pesan Singkat ini antara lain:

1. Melakukan transfer dana antar rekening dalam satu perbankan.
2. Melakukan pembayaran tagihan rekening air.
3. Melakukan pembayaran tagihan rekening listrik.
4. Mengecek informasi saldo tabungan pengguna.
5. Memberikan keamanan dalam melakukan transaksi dengan menggunakan jalur komunikasi *HTTPS.*

6. Menggunakan metode *Sms Gateway* dalam pemberian nomor pin untuk melakukan otentikasi pada saat melakukan transaksi dan aktifasi *account*.
7. Menggunaka pertanyaan yang harus dijawab sebagai metode otentikasi lainya selain otentikasi nomor pin.

I.2.3. Karaterikstik Pengguna

Pada aplikasi ini karakteristik pengguna antara lain sebagai berikut :

1. Administator yaitu pengguna yang mempunya otoritas paling tinggi yang melakukan pekerjaan sebagai berikut :
   a. Fungsi pengelolaan pengguna antara lain fungsi untuk mengaktifkan pengguna yang dinonaktifkan, menambahkan pengguna baru, menghapus data pengguna, mengubah data pengguna yang telah ada, dan serta dapat melihat informasi saldo pengguna.
   b. Fungsi pengelolaan data tagihan listrik yang berfungsi sebagai tempat penambahan data tagihan, mengubah data tagihan, dan menghapus data pengguna.
   c. Fungsi pengelolaan data tagihan air yang berfungsi sebagai tempat pengaturan data master tagiahan air. Seperti penambahan data tagihan, penghapuskan data tagihan air, dah pengubahan data tagihan.
   d. Fungsi pengaturan data pertanyaan yang berfungsi sebagai penyedia data-data pertanyaan, yang akan dijawab pada saat transaksi.
2. Pengguna aplikasi hanya dapat mengakses aplikasi untuk bisa melakukan transaksi perbankan *online*. Antara lain sbb:
   a. Melakukan transaksi transfer dana antar sesama Bank.
   b. Melakukan pembayaran tagihan listrik.
   c. Melakukan pembayaran tagihan air.
   d. Melihat informasi saldo tabungan.
   e. Mengubah pengaturan *account* pengguna.

I.2.4. Batasan – Batasan

Dengan penggunaan *Sms Gateway* dengan sifat tidak mengunakan *Auto Replay*, maka pada aplikasi ini pengguna tidak bisa melakukan aktifitas Internet Banking, dengan menggunakan metode pengiriman pesan singkat. Pengiriman pesan singkat yang dilakukan oleh *Server* hanya untuk mengirimkan nomor pin untuk otentikasi pada saat melakukan transaksi dan aktifasi *account* pengguna.

I.2.5. Asumsi dan Ketergantungan

Aplikasi ini dibuat dengan menggunakan suatu perangkat lunak yang mendukung bahasa pemograman *PHP*, dan sebagai alat untuk merancang program. Menggunakan *Webserver* dengan menggunakan modul *SSL* sebagai penggunaan metode enkripsi data. Penggunaan *Mysql* sebagai pengolahan dan manajemen basisdatanya. Serta penggunaan *Sms Daemon Services* agar proses pengiriman nomor pin biasa sampai kepengguna.

I.2.6. Penundaan Persyaratan

Pada pengembangan aplikasi adapun yang tidak dikerjakan pada lingkup sistem antara lain sebagai berikut:

1. Transfer dana ke Bank lain.
2. Pembayaran tagihan kartu kredit.
3. Pembelian pulsa telepon *CDMA*, atau pulsa telepon *GSM*.
4. Pembelian tiket maskapai penerbangan.
5. Pembayaran biaya pendidikan.