# BAB I

# PENDAHULUAN

## 1.1. Latar Belakang

Teknologi internet pada masa ini bisa dikatakan sebagai sarana utama di berbagai aktivitas. *Chatting*, bermain game, surat-menyurat, mengirim data, mendengarkan lagu atau melihat film favorit dan masih banyak hal lain yang menggunakan teknologi internet. Syarat yang dibutuhkan pun cukup mudah yaitu cukup memiliki account di situs yang di tuju (baik yang berbayar ataupun gratis) , maka pengguna akan dapat menggunakan fasilitas yang ada. Tetapi, apa yang terjadi jika pihak yang salah dapat mengakses *account* anda?. Hal-hal seperti : merusak data-data yang anda miliki, men-*download* data-data secara tidak bertanggung jawab, mengambil data-data penting pribadi anda, melakukan hal-hal yang tidak bertanggung-jawab menggunakan account anda, dan masih banyak hal lainya, yang kerap terjadi apabila account anda berhasil di akses oleh orang yang tidak bertanggung jawab. Cara mengatasinya ada berbagai cara, sebagai contoh: *virtual keyboard*, enkripsi, *password* yang kompleks (terdiri dari berbagai karakter) dan lainya. Bahkan suatu game online bernama Rising Force (RF) yang dikembangkan oleh LYTO, mengharuskan user memasukkan dan menghafalkan 2 password masing-masing minimal 8 karakter (harus dalam bentuk huruf dan angka), agar user dapat bermain dalam game.

Hal itu dilakukan tentu demi alasan keamanan, tetapi cukup merepotkan apabila kita memiliki *account* yang banyak di berbagai situs. Namun teknik keamanan tersebut pun belum cukup aman dengan adanya:

*1. Keylogger*

Program yang didesain agar mencatat semua karakter yang user ketikkan dalam *keyboard*.

2. Penyadapan

Serangan terhadap kerahasiaan, dimana pihak lain "ikut melihat" data-data yang dikirimkan dalam jaringan. Hal ini merupakan masalah utama yang dihadapi dalam kriptografi dan keamanan jaringan.

Penulis mencoba untuk mengatasi hal tersebut dengan menggunakan metode *One Time Password* yaitu metode agar password yang dimiliki oleh user selalu berubah. Dengan cara demikian tidak masalah apabila ada orang lain mengetahui password kita, karena password kita selalu berubah. Tetapi, bagaimana bila orang lain mengetahui password itu sebelum kita (masalah Penyadapan), maka dengan teknologi *wireless* yaitu SMS (*Short Message Service*) . Dengan *one time password* menggunakan *SMS gateway* diharapkan mampu mengatasi masalah-masalah diatas.

**1.2. Rumusan Masalah**

Laporan ini akan dikhususkan untuk membahas *One Time Password* menggunakan *SMS Gateway*. Hal-hal yang akan dibahas dalam laporan ini antara lain sebagai berikut:

1. Sistem apakah yang cocok dengan penerapan konsep "*One Time Password* menggunakan *SMS Gateway*"?
2. Bagaimanakah perbandingannya dengan login biasa?
3. Hal-hal apa yang perlu diperhatikan dalam penerapan?

## 1.3. Batasan Masalah

Batasan masalah pada tugas akhir "OTP dengan menggunakan SMS Gateway" ini adalah :

1. Data yang dikirimkan oleh user adalah data yang valid.
2. Penulis menggunakan operator XL dan handphone Sony Ericsson dalam pembuatan skripsi ini.
3. Testing dilakukan melalui aplikasi forum diskusi (Vanilla 1.1.4 pada bagian login)

## 1.4. Tujuan

Tujuan yang ingin dicapai adalah sebagai berikut :

1. Membangun aplikasi *One Time Password* menggunakan *SMS Gateway*
2. Melatih dan menerapakan ilmu yang sudah didapat dalam bangku perkuliahan dalam kehidupan nyata.
3. Melatih kemampuan mahasiswa dalam mengumpulkan data, memahami informasi yang diperoleh, menyajikan informasi dan data-data tersebut ke dalam bentuk perangkat lunak, dan menyusunnya ke dalam suatu laporan.

## 1.5. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah:

1. Studi Pustaka atau Literatur

   Metode ini dilakukan dengan mengumpulkan data dari buku-buku referensi dan media cetak maupun sumber-sumber lain.
2. Wawancara

   Metode ini dilakukan dengan melakukan tanya jawab dengan beberapa responden yang berpengalaman dalam bidang ini.

3. Analisis kebutuhan perangkat lunak

   Metode ini dilakukan dengan cara menganalisis data dan informasi yang diperoleh untuk merancang perangkat lunak sehingga menghasilkan SKPL.

4. Perancangan perangkat lunak

   Metode ini dilakukan untuk mendesain atau merancang tampilan antarmuka perangkat lunak, sehingga menghasilkan DPPL.

5. Implementasi

   Menerapkan hasil perancangan perangkat lunak untuk membangun aplikasi " One Time Password Menggunakan SMS Gateway".

6. Pengujian

   Menguji coba perangkat lunak yang telah dibuat, dimana menghasilkan PDHUPL.

**1.6. Sistematikan Penulisan**

Secara garis besar penulisan tugas akhir ini disusun sebagai berikut :

**BAB I PENDAHULUAN**

Bagian ini berisi informasi mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan, metode yang digunakan dan sistematika penulisan tugas akhir.

**BAB II LANDASAN TEORI**

Berisi teori-teori, pendapat, prinsip dan sumber-sumber lain yang dapat dipertanggungjawabkan secara ilmiah dan dapat dipergunakan sebagai pembanding atau acuan yang digunakan dalam tugas akhir.

**BAB III ANALISIS DAN PERANCANGAN SISTEM**

Bab ini berisi tentang tinjauan aspek informatika berupa analisis dan desain perancangan perangkat lunak yang terdiri dari spesifikasi kebutuhan dan deskripsi perangkat lunak.

**BAB IV IMPLEMENTASI SISTEM dan ANALISIS HASIL**

Bab ini berisi tentang implementasi program yang telah dihasilkan, gambaran umum sistem dan evaluasi sistem.

**BAB V PENUTUP**

Berisi mengenai kesimpulan yang dapat diambil dari penyusunan tugas akhir, serta saran-saran penulis yang diharapkan dapat bermanfaat bagi pihak-pihak lain yang berkepentingan.

**DAFTAR PUSTAKA**