BAB II

LANDASAN TEORI DAN TINJAUAN PUSTAKA

2.1. OTP (*One Time Password*)

Tujuan dari pembuatan OTP (*password* sekali pakai) adalah untuk mempersulit pihak-pihak yang tidak bertanggung jawab dalam mengakses data yang rahasia. Seperti *account* komputer. Biasanya *password* statis lebih mudah untuk diakses pihak-pihak yang tidak bertanggung jawab, cukup dengan adanya usaha dan waktu. Dengan secara konstan merubah *password* setiap kali penggunaanya, maka resiko *password* diketahui pihak lain dapat dikurangi.

OTP terdapat 5 tipe (en.wikipedia.org):

1. Tipe Algoritma Matematika

   Dengan menggunakan algoritma matematika *password* baru dibentuk berdasarkan penghitungan *password* lama. Contoh : apabila *password* sekarang adalah s, maka *password* berikutnya adalah f(s), kemudian *password* berikutnya adalah f(f(s)) dan seterusnya. Dengan cara demikian apabila ada orang yang tahu *password* sekarang, maka dia hanya bisa login pada saat itu juga, karena pada saat berikutnya *password* juga akan berubah.

2. Tipe Sinkronisasi Waktu

   Tipe Sinkronisasi Waktu membuat *password* berdasarkan sinkronisasi waktu antara *server* dan *client*. Untuk tipe ini digunakan suatu alat (yang dipegang oleh user) dimana didalamnya terdapat waktu akurat yang sudah di sinkronkan dengan waktu server. Dalam OTP jenis ini waktu adalah hal yang penting karena

waktu digunakan dalam algoritma pembentukkan *password* baru.

Gambar 2.1 Alat RSA SecurID
(en.wikipedia.org)

3. Tipe *Password* Baru

Tipe ini hampir sama dengan tipe algoritma matematika, hanya saja *password* baru tidak dibentuk berdasarkan *password* lama dan dalam penggunaanya menggunakan alat. Tipe ini banyak digunakan di kartu kredit Eropa.

Gambar 2.2 Alat Entrust IdentityGuard Mini
(en.wikipedia.org)

4. Tipe *Transaction Authentication Number* (TAN)

Tipe ini digunakan oleh layanan bank online untuk membuat OTP yang nantinya akan digunakan untuk transaksi. Contohnya: seorang customer pergi ke bank meminta TAN, kemudian bank akan mengeluarkan 50 nomor yang unik dan random kepada custumer tersebut. Kemudian untuk setiap transaksi customer tinggal memasukkan salah satu dari TAN tersebut. Jika TAN cocok diterima, jika tidak maka transaksi gagal. TAN yang sama tidak bisa digunakan dua kali.

5. Tipe menggunakan SMS (*Short Message Service*)

Tipe ini menggunakan SMS karena: SMS menggunakan saluran sendiri, sudah memasyarakat, biaya yang digunakan rendah. Jenis-jenis OTP yang lain biayanya tinggi bila diimplementasikan, dan terlalu mahal dalam perawatan. Jenis ini dapat dikatakan lebih simple dan aman dibanding dengan metode yang lain.

2.2. SMS Gateway

Seperti arti katanya, *Gateway* berarti pintu gerbang, sehingga dalam istilah ini, *SMS Gateway* berarti pintu gerbang atau jembatan antara dua buah device atau lebih, yang berkomunikasi via SMS (sms-gammu.blogspot.com) . Umumnya *SMS Gateway* ini berupa sebuah komputer yang didalamnya telah terinstall aplikasi untuk menangani pengiriman SMS antar HP. Dalam hal ini, SMS gateway berfungsi sebagai aspek pusat yang menangani pengiriman surat sesuai dengan alamat yang dituju. Dalam skripsi ini penulis mengembangkan program *SMS Gateway* menggunakan Gammu.

2.2.1. Protokol SMS

SMS dikirim dan diterima melalui jaringan *wireless*. Sudah tentu sebuah jaringan mempunyai protokol yang digunakan sebagai penunjangnya. Protokol yang sering dipakai oleh SMS adalah sebagai berikut (sms-gammu.blogspot.com):

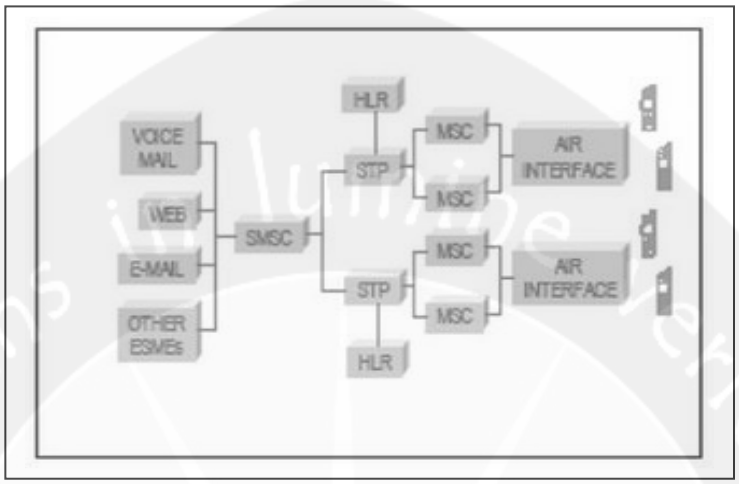
1. HTTP (*Hypertext Transfer Protocol*)

   HTTP merupakan protokol yang paling sering digunakan dalam internet saat ini. Tujuan utama HTTP pada mulanya adalah untuk menyediakan cara dalam menyajikan dan mengambil dari halaman HTML. Saat ini penggunaan HTTP tidak terbatas dalam penyajian halaman HTML saja.

2. SMPP (*Short Message Peer-to-Peer Protocol*)

   Short message protocol peer-to-peer (SMPP) merupakan sebuah protokol standar industri yang digunakan dalam pertukaran short message antara *Eternal Short Messaging Entity* (ESME), *Routing Entity* (RE), dan *Message Centre* (MC). *Message Centre* merupakan terminologi generik untuk menyebutkan beberapa entitas seperti *Short Message Service Centre* (SMSC), *GSM Unstructured Supplementary Service Data* (USSD) *server*, atau *Cell Broadcast Centre* (CBC). ESME merupakan entitas yang berada diluar jaringan komunikasi wireless .

2.2.2. Elemen Jaringan SMS



Gambar 2.3 Elemen SMS
(sms-gammu.blogspot.com)

Layanan SMS dibangun dari berbagai entitas yang saling terkait, yang mempunyai tugas dan fungsi masing-masing. Tidak ada satupun dalam sistem SMS yang dapat bekerja secara parsial. Entitas dalam jaringan SMS ini disebut juga elemen jaringan SMS. SMS memiliki elemen-elemen seperti berikut(sms-gammu.blogspot.com):

1. *External Short Messaging Entities* (ESME)

Dapat dikatakan bahwa *Short Message Entity* (SME) merupakan entitas dalam sistem SMS yang dapat berada pada jaringan, berupa perangkat bergerak, atau merupakan *service Centre* yang berada di luar jaringan. ESME sendiri, sesuai namanya, merupakan sebuah SME yang berada di luar jaringan SMS. Saat ini sebagian besar ESME berada pada jaringan data seperti jaringan TCP/IP yang di dalamnya termasuk internet. Beberapa macam ESME di antaranya adalah:

1. *Voice Mail System* (VMS)

VMS merupakan perangkat yang berfungsi untuk

menerima, menyimpan, dan menjalankan *voice message*, ditujukan untuk pelanggan yang sedang sibuk dan sedang tidak dapat dihubungi melalui sambungan *voice*.

2. Web

Web merupakan sebuah layanan yang sangat populer pada jaringan data terutama internet. Pesatnya perkembangan internet dengan jumlah pertumbuhan penggunanya yang juga sangat tinggi, membuat internet sebagai sebuah entitas dalam sistem SMS yang banyak membangkitkan trafik SMS.

3. Email

Email merupakan salah satu layanan yang paling banyak digunakan dalam internet. SMS harus dapat mendukung interkoneksi dengan teknologi email. Untuk itu kemudian muncul layanan yang juga cukup banyak digemari, yaitu *email-to-sms* dan *sms-to-mail*.

2. *Short message service Centre* (SMSC)

Terminologi SMSC mengacu pada sesuatu yang berupa *hardware* dan *software*. SMSC merupakan sebuah entitas yang bertanggung jawab untuk menyimpan, routing, dan meneruskan short message dari satu titik ke titik lain yang merupakan tujuan, misalnya dari suatu SME ke perangkat telepon bergerak. Sebuah SMSC harus memiliki keandalan yang tinggi, kapasitas yang cukup, dan throughout yang memadai dalam menangani trafik short message. Selain itu, sistem harus bersifat fleksibel dan scalable agar dapat mengakomodasi pertumbuhan permintaan layanan SMS.

Faktor lain yang juga harus diperhatikan adalah aplikasi harus dapat dioperasikan dengan mudah, begitu juga pemeliharaannya. Sebagai contoh adalah fleksibilitas untuk aktivasi layanan baru dan upgrade *software*.

3. Elemen *Wireless Network*

Ada beberapa elemen *wireless network*, yang merupakan elemen jaringan SMS, diantaranya sebagai berikut:

1. *Signal Transfer Point* (STP)

   STP merupakan elemen dalam jaringan yang biasanya digelar dalam intelligent netrwork (IN), digunakan sebagai media interkoneksi berbasis *Signaling system* 7 (SS7) untuk menghubungkan ke lebih dari satu elemen jaringan lain.

2. *Home Location Register* (HLR)

   HLR merupakan sebuah database yang digunakan sebagai tempat penyimpanan data permanen data dan profil pelanggan.

3. *Visitor Location Register* (VLR)

   VLR merupakan sebuah database tempat menyimpan informasi sementara berisi data pelanggan HLR yang sedang roaming pada HLR lain.

4. *Mobile Switching Center* (MSC)

   MSC merupakan sebuah sistem yang melakukan fungsi switching dan mengontrol panggilan telepon dalam sebuah jaringan komunikasi bergerak.

5. *Air Interface*

   Merupakan antarmuka media transmisi yang dalam hal ini berupa ruang udara. Terdapat beberapa teknologi standar sebagai air interface dalam komunikasi bergerak, diantaranya GSM, TDMA, dan CDMA.

6. *Base Station System*

   Base station system merupakan kesatuan sistem yang bertanggung jawab mengatur transmisi signal elektromagnetik untuk membawa data dari MSC ke perangkat telepon bergerak. *Base Station System* terdiri dari *Base Station Controller* (BSC), dan *Base Transceiver System* (BTS)

7. *Mobile Device*

   Merupakan perangkat yang mempunyai kemampuan mengirimkan dan menerima *short message*, biasanya berupa telepon seluler dan teknologi digital

2.3. Gammu

Gammu adalah nama sebuah project yang ditujukan untuk membangun aplikasi, script dan drivers yang dapat digunakan untuk semua fungsi yang memungkinkan pada telepon seluler atau alat sejenisnya (www.gammu.org). Sekarang gammu telah menyediakan *codebase* yang stabil dan mapan untuk berbagai macam model telepon yang tersedia di pasaran dibandingkan dengan project sejenis.

Gammu merupakan project yang berlisensi GNU GPL 2 sehingga menjamin kebebasan menggunakan tool ini tanpa perlu takut dengan masalah legalitas dan biaya yang mahal yang harus dikeluarkan. Gammu mendukung berbagai macam model telepon seluler dengan berbagai jenis koneksi dan type. Gammu beroperasi menggunakan AT command

Gammu merupakan salah satu tool untuk mengembangkan aplikasi SMS Gateway yang cukup mudah diimplementasikan dan pastinya gratis. Kelebihan Gammu adalah :

1. Gammu bisa di jalankan di Windows maupun Linux.
2. Banyak device yang kompatibel oleh gammu.
3. Baik kabel data USB maupun SERIAL, semuanya kompatibel di Gammu.

2.4. AT Command

AT Command adalah instruksi yang digunakan untuk mengontrol sebuah modem (www.developershome.com). AT singkatan dari *Attention*. Setiap perintah atau syntax akan dimulai dengan perintah AT. GSM/GPRS modem atau mobile phones mensupport jenis perintah ini. *AT command* juga disesuaikan dengan berbagai fungsi yang ada di teknologi GSM, dimana didalamnya termasuk SMS. Contohnya: AT+CMGS (mengirim SMS), AT+CMSS (mengirim SMS dari media penyimpanan), AT+CMGL (melihat SMS dalam bentuk list) and AT+CMGR (membaca pesan SMS) dan masih banyak berbagai macam syntax lainya. Perlu diketahui bahwa setiap produsen HP tidak mengimplementasikan semua jenis AT command. Parameter dan nilai AT command tiap merk belum tentu sama dan setiap syntax belum tentu menghasilkan hasil yang sama.

Modem GSM /GPRS lebih mensupport *AT command* dibandingkan dengan hp biasa. Sebagai tambahan AT command juga bergantung dari jenis jaringan yang digunakan.