Pengamanan Telepon Seluler dengan Menggunakan Tanda Tangan Digital

Anggi shena permata (13505117)

Departemen Teknik Informatika
Institut Teknologi Bandung
Jl. Ganesha 10 Bandung 40132

E-mail : if15117@students.if.itb.ac.id[1]

Abstraksi

Telepon selular atau yang biasa kita kenal dengan sebutan hp sudah dapat dikatakan menduduki tingkat kebutuhan primer pada masa ini dimana teknologi terus berkembang dan menuntut adanya fasilitas yang mampu mendukung kelancaran komunikasi antar pihak. Berbagai jenis telepon selular telah beredar dimasyarakat dengan harga yang berbeda-beda pula, mulai dari tingkat harga yang dapat dijangkau oleh masyarakat dengan golongan ekonomi menengah kebawah sampai hp dengan harga tinggi yang dilengkapi fitur-fitur menarik yang menjadikan barang tersebut berarti sesuai dengan harga yang diberikan. Besarnya kebutuhan masyarakat akan sarana berkomunikasi ini secara tidak disadari juga telah menaikan tingkat kriminalitas khususnya dalam hal pencurian hp yang sedang marak-maraknya terjadi ditengah-tengah masyarakat kita. Banyak cara telah dilakukan untuk mencegah terjadinya pencurian tersebut, namun sejalan dengan makin tingginya kebutuhan masyarakat akan hp, maka makin tak terkendali pula arus pencurian yang terjadi. Dari berbagai cara yang ditawarkan oleh vendor telepon selular, sampai saat ini pengamanan yang umum dilakukan hanyalah mampu mencegah para pelaku kejahatan untuk dapat menggunakan hasil curiannya tersebut dengan adanya kode sekuriti yang tersimpan dalam hp tersebut. Oleh karena itu, pada makalah ini penulis berusaha memberikan suatu solusi untuk dapat mencari keberadaan telpon selular yang dicuri dengan penambahkan sistem pangamanan yaitu digital signature pada hp yang kelak akan bermanfaat untuk mengotentikasi kepemilikan hp tersebut.

Kata kunci

Telepon seluler, hp, digital signature, pengamanan, kunci, md5

1. PENDAHULUAN

Seperti telah dikemukakan sebelumnya, tingkat pencurian hp dikalangan masyarakat kita terus meningkat sejalan dengan maningkatnya kebutuhan masyarakat akan telepon selular. Berikut merupakan beberapa sistem pengamanan yang telah ditawarkan oleh beberapa vendor hp saat ini :

1. PIN
   PIN merupakan kunci yang dapat di set oleh sipemilik hp untuk dapat mengaktifkan sim card yang dimilikinya. Analogi kerja sim ini dapat dibayangkan sebagai kunci pintu sebuah rumah, dimana pin merupakan kuncinya sedangkan Sim card merupakan rumah yang ingin dimasuki

2. Security Code
   Security Code yang ditawarkan oleh beberapa vandor hp berfungsi sebagai kunci untuk dapat mengaktifkan hp tersebut atau masuk ke dalam sistem operasi dari hp tersebut. Biasanya sistem akan meminta masukan Security Code ini jika terjadi penggantian Sim card. Dengan adanya sistem ini, diharapkan tidak ada pihak lain yang dapat menggunakan hp tanpa sepengetahuan pemiliknya yaitu orang yang memegang kunci tersebut.

3. Pelacakan
   Fitur pelacakan ini biasanya digunakan seseorang untuk mencari keberadaan handphone tempat dimana sim card tersebut ditanamkan berdasarkan sinyal dan informasi-informasi yang ditangkap. Palacakan ini dapat dilakukan hanya jika kita mengetahui no hp yang akan dilacak.

Dan masih banyak lagi sistem pengamanan lain yang ditawarkan

Dari beberapa sistem pengamanan telepon selular yang ditawarkan diatas, sebagian besar hanyalah berperan dalam hal pencegahan terjadinya pencurian, karena dengan adanya

kesulitan yang harus dihadapi dari sistem tersebut , setidaknya pencuri akan berpikir dua kali sebelum melakukan tindak pencurian. Dalam hal ini, penulis mencoba memberikan solusi yang dapat digunakan untuk menangani pencurian hp yang telah terjadi dimana dengan ide yang penulis tawarkan, akan diusahakan agar pemilik hp tersebut dapat memperoleh kembali hp nya dengan mencari tau keberadaannya. Dengan sistem palacakan yang telah disediakan oleh setiap provider jaringan komunikasi (telkomsel,indosat, dll) akan mempermudah pengerjaan karena pelacakan pada sistem ini akan mencari berdasarkan keterangan hp yang akan di simpan dalam sim card agar kemudian dapat dilacak keberadaannya.
Sebelum berlanjut pada penjelasan prodedur sistem pangamanan ini, berikut merupakan beberapa dasar teori dan pengetahuan yang digunakan untuk mendukung jalannya sistem ini.

Fungsi hash satu arah

Fungsi hash merupakan fungsi yang menerima masukan string yang panjangnnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnnya tetap dan umumnya berukuran jauh lebih kecil dari panjang string semula. Keluaran fungsi hash biasa disebut *nilai hash* atau *message digest*. String pesan yang masuk akan dikompresi oleh fungsi hash melalui persamaan

$$h = H(M)$$

Fungsi hash satu arah merupakan fungsi hash yang bekerja dalam satu arah. Pesan yang telah diubah menjadi message digest tidak dapat dikembalikan lagi menjadi pesan semula.

Sifat-sifat yang dimiliki oleh fungsi hash satu arah adalah sebagai berikut :

- Fungsi H dapat diterapkan pada blok data yang berukuran berapa saja
- Nilai hash yang dihasilkan memiliki panjang yang tetap
- Untuk setiap h yang diberikan, tidak mungkin menemukan suatu x sedemikian sehingga H(x)=h.
- Untuk setiap x yang diberikan, tidak mungkin mencari pasangan $x \neq y$ sedemikian sehingga H(x)=H(y).

Algoritma MD5

MD5 adalah fungsi hash satu arah menerima masukan pesan yang berukuran sembarang dan menghasilkan message digest yang panjangnnya 128 bit. Langkah-langkah pembuatan message digest secara garis besar adalah sebagai berikut :

1. Penambahan bit-bit pengganjal (padding bits)

Pesan ditambah dengan sejumlah bit pengganjal sehingga panjang pesan kongruen dengan 448 modulo 512. Bit pengganjal diisi dengan sebuah bit 1 kemudia diikuti dengan bit 0 untuk sisanya.

2. Penambahan nilai panjang pesan semula

Pesan yang telah diberi bit-bit pangganjal selanjutnya ditambahkan lagi dengan 64 bit yang menyatakan panjang pesan.

3.Inisialisasi penyangga (buffer) MD

MD5 membutuhkan 4 buah penyangga yang masing-masingnya berukuran 32 bit. Keempat bit penyangga ini menampung hasil antara dan hasil akhir. Keempat bit penyangga dan inisialisasinya adalah sebagai berikut :

A = 01234567
B = 89ABCDEF
C = FEDCBA98
D = 76543210

4.Pengolahan pesan dalam blok berukuran 512

Pesan dibagi menjadi L buah blok yang masing-masing panjangnya 512 bit. Setiap blok di proses berasama penyangga MD yang menghasilkan keluaran 128 bit, proses ini di sebut HMD5. Proses HMD5 terdiri dari 4 putaran dimana setiap putaran melakukan 16 operasi dasar MD5 dan tiap operasinya memakai sebu h elemen T yang nilainya tertera pada tabel T yang di peroleh dari perihitungan berdasarkan rumus yang telah ditentukan.

Operasi MD5 dapat ditulis dengan persamaan sebagai berikut :

A <-- b + CLSs(a + g(b,c,d) + X[k] + T[i])

yang dalam hal ini ,
a,b,c,d --> empat buah penyangga 32 bit
g --> salah satu fungsi F, G, H, I
CLSs --> circular left bit sebanyak s bit
X[k] --> kelompok 32 bit ke-k dari blok 512 bit message ke-q.
T[i] --> elemen tabel ke i (32 bit)
+ --> penjumlahan modulo 2^32

Karena ada 16 kali operasi dasar yang dilakukan, maka setiap kali satu operasi dasar dilakukan, penyangga-penyangga itu di geser ke kanan secara sirkuler dengan cara pertukaran sebagai berikut :

Temp --> d
d --> c
c --> b
b --> temp

Tabel fungsi-fungsi dasar MD5

Nama	Notasi	g(b,c,d)
□f	F(b,c,d)	(b ^ c) v (~b ^ d)
*f*G	G(b,c,d)	(b ^ d) v (c ^ ~d)
*f*H	H(b,c,d)	b Xor c Xor d
*f*I	I(b,c,d)	c Xor (b V ~d)

Tanda Tangan Digital

Tanda-tangan Digital merupakan suatu nilai kriptorafis yan terkandung pada pesan dan pengirim pesan. Dengan tanda-tangan digital , maka integritas data dapat terjamin dan juga dapat digunakan untuk membuktikan asal pesan serta pihak yang mengirimkan pesan tersebut. Panandatanganan pesan dapat dilakukan dengan dua cara yaitu :

1. Enkripsi Pesan

Dengan meng-enkripsi pesan, secara otomatis telah menyediakan ukuran otentikasi yang menyatakan bahwa pesan tersebut telah ditandatangani. Penandatanganan dengan cara enkripsi pesan dapat dilakukan dengan menggunakan algoritma kriptografi kunci simetri atau kriptografi kunci publik.

2. *Dengan Fungsi Hash*

Penandatanganan dengan menggunakan fungsi hash hanya menyediakan fitur untuk membuktikan otentikasi pasan saja namun tidak menyembunyikan pesan tersebut kedalam bentuk cipherteks, karena dalam beberapa persoalan, terdapat beberapa dokumen yang memang hanya membutuhkan otentikasi saja tapi tidak untuk kerahasiaannya

Komunikasi dengan Telpon Seluler

Penggunaaan telpon seluler berisifat *mobile* yang memungkinkan seseorang dapat berkomunikasi dimana saja dan juga *nirkabel* yang pada implementasinya, pengiriman pesan akan dilakukan melalui media gelombang mikro ke Base Station (BST) terdekat untuk selanjutnya dikirim ke ponsel penerima.

Hampir saluruh penerapan aplikasi telepon selular saat ini menggunakan SIM card yang merupakan kartu cerdas dimana didalamnya berisi :

1. Identitas pengguna berupa IMSI yang unik nilainya.
2. Kunci rahasia yang akan digunakan untuk otentikasi pengguna jaringan.
3. PIN, jika di set
4. Program enkripsi

Ponsel bekerja dengan mengandalkan sinyal yang dipancarkan dari sebuah pemancar dengan frekuensi tertentu. Untuk membagi-bagi daerah agar terdapat frekuensi yang merata pada daerah tersebut maka sebuah daerah atau kota dibagi menjadi seperti sebuah irisan yang digambarkan sebagai irisan berbentuk hexagonal atau disebut dengan sel (cell). Masing-masing sel tersebut dapat mempunyai frekuensi sebanyak 800 dan mempunyai cakupan kisaran sekitar 26 kilometer bujur sangkar. Masing-masing sel mempunyai suatu menara dan suatu bangunan kecil yang berisi peralatan. Saat kita sedang berjalan dengan mengendarai kendaraan, sinyal akan dipancarkan dari sel ke sel oleh suatu tower atau menara dari tiap sel tersebut.

Semua ponsel mempunyai kode khusus yang berhubungan dengan pemiliknya atau operator teleponnya. Secara umum terdapat 3 pokok kode yang terdapat pada ponsel antara lain:

1. Electronic Serial Number (ESN), suatu nomor 32-bit yang unik diprogramkan ke dalam telepon saat dibuat (kita kenal dengan istilah nomor IMEI)

2. Mobile Identification Number (MIN), l0 digit nomor dari nomor telepon

3. System Identification Code (SID), 5 digit nomor yang dikeluarkan oleh badan resmi dunia yang menangani bidang telekomunikasi (FCC).

GSM merupakan teknologi telepon selular yang paling banyak digunakan diseluruh dunia. Pada GSM diperlukan kebutuhan penjaga keamanan yaitu untuk otentikasi pengguna telpon dan kerahasiaan percakapan yang dilakukan. Oleh karena itu, setiap paket data yang terkirim saat berkomunikasi akan dienkripsi untuk mencegah terjadinya penyadapan. Pada saat pengguna melakukan panggilan, identitasnya akat dikirm melalui BST terdekat kepada operator untuk kemudian digunakan dalam keperluan otentikasi.

2. TANDA TANGAN DIGITAL PADA HP

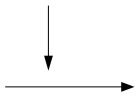
Dengan berbekal dasar teori dan pengetahuan yang telah dijabarkan secara ringkas diatas, penulis merancang suatu sistem pengamanan pada telepon selular yang memungkinkan adanya pelacakan jika tarjadi tindak pencurian untuk mengetahui keberadaan ponsel tersebut dan memperolehnya kembali.

Sistem yang dirancang oleh penulis adalah dengan memberikan tanda tangan digital yang akan di simpan oleh sistem ponsel yang akan dijaga kerahasiaannya dengan menggunakan suatu kode atau kunci yang kelak dalam implementasinya akan digunakan sebagai kunci enkripsi dari data-data yang tersimpan tersebut. Tanda tangal digital yang diberikan untuk setiap ponsel tersebut bersifat rahasia dan hanya diketahui oleh pemilik handphone. Data-data yang tersimpan dalah ponsel tersebut tidak akan hilang sekalipun terjadi penggantian kartu SIM pada hp. Informasi tersebut tidak dapat diubah terkecuali oleh pemilik yang mengetahui persis kuncinya yang dibutuhkan untuk melalukan perubahan data. Dengan demikian, otentikasi kepemilikan dari suatu handphone dapatlah dibuktikan.

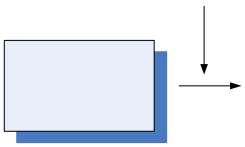
Berikut merupakan langkah-langkah yang dirancang untuk memberi tanda tangan digital pada sistem ponsel :

1. Ponsel merupakan alat komunikasi yang didalamnya terdapat suatu sistem yang menyerupai sistem komputer dimana kita dapat menyimpan data pada tempat yang disediakan. Pada sistem keamanan ini setiap ponsel dirancang untuk memiliki ID unik yang kelak akan digunakan sebagai dasar pelacakan.
2. Setiap pemilik ponsel dapat menyimpan informasi kepemilikannya yang kemudian akan dikenal dengan sebutan tanda tangan digitalnya. Setiap ponsel diset tanda tangan digital awal dan kunci awal oleh vendor ponselnya masing-masing yang kemudian dapat di ubah oleh pemiliknya.
3. Pada proses penandatanganan, pemilik ponsel akan diminta untuk memasukan data yang dibutuhkan seperti nama, alamat, no identitas (KTP/kartu pelajar atau kartu identitas lainnya) dan kode rahasia (min 8 karakter) yang kemudian akan berperan sebagai kunci enkirpsi. Untuk selanjutnya dengan tujuan mempermudah penjelasan makan data- data yang dimasukan tersebut digabungkan dengan ID ponsel yang unik akan kita sebut sebagai ***data_S*** dan kode rahasia dengan sebutan ***key*** . panjang kunci minimal 8 karakter hanya ditujukan untuk keamanan yang lebih baik.

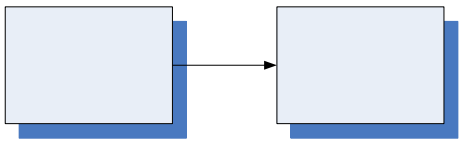
4. Selanjutnya data_S tesebut akan dihitung nilai hash nya dengan mengunakan algoritma MD5 seperti yang telah dijelaskan diatas dan akan diperoleh nilai hash nya yaitu ***H(S).***



5. Kemudian ***H(S)*** akan dilekatkan pada ***data_S*** menjadi suatu data yang kita sebut saja ***data_G***.
6. ***Data_G*** tersebut kemudian akan dienkripsi dengan menggunakan algoritma kunci simetri yang terpercaya keamanannya.



7. Data_G terenkripsi tersebut bersama dengan ID ponsel akan disimpan pada tempat penyimpanan diponsel tersebut dan akan digandakan untuk disimpan pula pada kartu SIM yang sedang digunakan menjadi tanda tangan digital yang dimaksud. Setiap kartu sim yang sedang aktif pada ponsel, akan diperiksa tanda tangan digitalnya, jika tidak terdapat kecocokan dengan yang tersimpan pada ponsel, maka tanda tangan digital yang tersimpan pada kartu SIM tersebut akan ditimpa datanya dengan data yang berkesuaian.



8. Setelah penandatanganan dilakukan, ponsel akan mengembalikan nilai ID ponsel untuk diingat sedangkan sistem tidak akan menyimpan kunci rahasia dengan alasan pencegahan para kriptanalis untuk mencuri kunci tersebut, sehingga pemilik harus mengingat baik-baik kunci yang telah dibuatnya sendiri karena sistem tidak akan menyimpannya sama sekali.
9. ID ponsel yang disimpan pula informasinya pada kartu SIM akan dikirim informasinya pada BTS terdekat seperti pengiriman sinyal yang dilakukan pada sistem telepon selular.

3. PEMINDAHTANGANAN KEPEMILIKAN

Ada dua kondisi dimana suatu ponsel dapat berpindah tangan atau dengan kata lain berganti kepemilikan. Dua kondisi tersebut merupakan kondisi yang legal dan tidak legal. Pemindahtanganan secara legal biasanya dilakukan dengan cara memberikannya kepada orang lain atau dapat pula melalui proses jual beli, sedangkan pemindahtanganan secara tidak legal dilakukan melalui pencurian atau tindak kejahatan lainnya. Berikut akan dijelaskan langkah-langkah yang harus dilakukan jika terjadi pemindahtanganan atau penggantian kepemilikan pada ponsel.

1.Pemindahtanganan secara legal

Dalam keadaan ini, pemilik yang baru akan memiliki ponsel yang dimaksud dengan sepengetahuan atau seijin pemilik sebelumnya. Oleh karena hal tersebut, maka pemilik sebelumnya akan bersedia memberitahukan kunci rahasia yang digunakan untuk mengenkripsi informasi kepemilikannya menjadi tanda tangan digital, sehinga setelah ponsel tersebut berpindah tangan, maka pemilik yang baru dapat segera merubah data kepemilikan pada ponselnya sesuai dengan data dirinya dan membuat kunci baru untuk keamanan.

2.Pemindahtanganan secara tidak legal

Keadaan ini terjadi jika ponsel tersebut berpindah tangan tanpa seijin pemilik sebelumnya, pada tindakan pencurian misalnya. Dalam keadaan ini, pemilik yang baru tidak akan mengetahui kunci rahasia pemilik ponsel sebelumnya oleh karena itu, maka sang pencuri tidak akan dapat merubah data kepemilikan pada ponsel tesebut. Keadaan yang demikian sebenarnya bisa saja diatasi dengan mereset ulang sistem ponsel, namun hal tersebut harus dilakukan melalui customer service dari tiap vendor ponsel tersebut. Untuk mencegah hal tersebut, maka pada setiap pelayanan yang meminta dilakukannya reset pada ponsel, setiap pemilik ponsel harus terlebih dahulu memberikan kunci rahasianya untuk proses otentikasi apakah orang tersebut marupakan pemilik yang sebenarnya dari ponsel yang akan diproses. Jika otentikasi berhasil, maka proses reset baru dapat dilakukan.

Baik dalam kondisi legal maupun tidak legal, pemindahtanganan biasanya berujung pada penggantian kartu SIM ataupun tidak. Pada kedua kondisi tesebut, jika terjadi penggantian kartu SIM maka DATA_G terenkripsi dan ID ponsel yang tersimpan dalam sistem ponsel akan segera digandakan dan simpan pada kartu SIM yang baru. Jika telah terdapat data sebelumnya, maka akan diperiksa terlebih dahulu oleh sistem. Jika datanya sama, maka tidak akan dilakukan apa-apa, namun jika datanya berbeda maka akan dilakukan penimpaan data yang lama dengan yang data yang tersimpan pada sistem ponsel.

4. PELACAKAN PONSEL YANG HILANG

Berikut merupakan langkah-langkah yang dapat dilakukan jika seseorang kehilangan ponselnya, baik itu tertinggal disuatu tempat atau dicuri orang lain, dan orang tersebut ingin mengetahui keberadaan ponselnya agar dapat memperoleh ponselnya kembali :

1. Pertama-tama yang harus dilakukan oleh pemilik ponsel tersebut adalah mendatangi customer service setiap provider jaringan komunikasi.
2. Pada setiap privider, pemilik ponsel akan minta dicarikan keberadaan ponselnya berdasarkan ID ponsel yang dimilikinya. Keberadaan ponsel tersebut dapat dideteksi oleh sistem provider karena data mengenai ID ponsel tersebut telah disimpan pada kartu sim apapun yang sedang aktif pada ponsel tersebut. Keberadaan ponsel tetap dapat tedeteksi meskipun sipencuri ponsel telah mengganti kartu sim sebelumnya dengan kartu sim yang baru miliknya.
3. Jika keberadaan ID ponsel yang dimaksud ditemukan oleh provider jaringan tersebut, maka kemudian petugas akan meminta kunci rahasia pemilik ponsel untuk memastikan kebenaran kepemilikan ponsel tersebut.
4. Petugas akan mengambil DATA_G terenkripsi dari SIM yang ditemukan untuk kemudian didekripsi dengan mengunakan kunci rahasia sipemilik tadi. Setelah itu verivikasi tanda tangan digital akan dilakukan dengan membandingkan H(s) dengan hasil perhitungan nilai hash dari DATA_S yang tersimpan. Jika sama maka tanda tangan digital tersebut tidak mengalami perubahan.
5. Dari DATA_S yang sudah terverifikasi, petugas akan meminta bukti-bukti yang menunjukan kepemilikan akan ponsel tersebut yaitu kartu identitas yang berisi data-data yang sama dengan yang tertera pada DATA_S. KTP dan kartu garansi ponsel misalnya.
6. Jika sesuai, maka petugas akan memberitahukan keberadaan ponsel tersebut dari BTS yang terdeteksi.

5. KELEBIHAN DAN KEKURANGAN

Demikian telah dijelaskan rancangan sistem pengamanan ponsel dengan menggunakan tanda tangan digital yang disimpan dalam ponsel tersebut. Rancangan ini barulah sebuah ide yang belum terimplementasi. Adapun beberapa

kelebihan dan kekurangan yang diperoleh dari hasil analisis penulis sebagai berikut :

Kelebihan :

1. Sistem keamanan yang ditawarkan saat ini masih belum mendukung untuk ditemukannya ponsel yang hilang atau dicuri orang lain dengan kemungkinan penggantian kartu SIM, oleh karena itu, kelebihan yang ditawarkan dari sistem ini cukup bisa memberikan rasa aman yang cukup bagi para pengguna ponsel terlebih lagi para pemilik ponsel yang bagus dan mahal.
2. Dengan adanya tanda tangan digital yang disimpan dalam sistem ponsel, tentunya akan sangat bermanfaat sebagai acuan dalam mengotentikasi kepemilikan ponsel jika terjadi suatu hal yang kurang berkenan.
3. Dengan adanya kunci rahasia dan nilai hash akan menambahkan tingkat keamanan tesimpannya data, karena akan sulit sekali bagi seseorang yang berniat jahat mengubah DATA_S dan nilai hash yang ada sehingga menghasilkan nilai perbandingan yang saling berkesesuaian.
4. Kunci tidak dapat dicuri orang lain karena tidak disimpan dalam sistem melaikan hanya digunakan pada saat pembuatan tanda tangan digital lalu kemudian akan dihancurkan dari sistem.

Kekurangan :

1. Setiap vendor ponsel dan priveder jaringan komunikasi harus menyepakati algoritma pengenkripsian yang sama untuk memudahkan proses pelacakan jika terjadi kehilangan ponsel.
2. Teknologi ini harus didukung oleh semua provider jaringan komunikasi, karena akan percuma saja jika tidak semua provider jaringan menyediakan fasilitas ini, Maka para pencuri akan menggati kartu sim pada ponsel curiannya dengan kartu sim yang merupakan produk dari provider jaringan yang tidak dapat mendeteksi keberadaan ponsel.
3. Biaya yang digunakan akan besar karena dibutuhkan standarisasi teknologi pada provider jaringan komunikasi dan vendor ponsel.
4. Masih terlalu kompleks dan rumit untuk diimplementasikan

6. KESIMPULAN DAN SARAN

Tindak kriminalitas khususnya pencurian ponsel makin marak sejalan dengan meningkatnya jumah pemakai ponsel pribadi, oleh karena itu dibutuhkan sistem keamanaan yang cukup baik dan dapat mengatasi pencurian yang banyak terjadi saat ini. Salah satu cara yang ditawarkan oleh menulis adalah dengan memberikan tanda tangan digital pada setiap ponsel dimana didalamnya terdapat data kepemilikan ponsel tersebut yang diproteksi dengan memberikan nilai hash dan kunci enkripsi yang akan digunakan untuk merubah data-data tersebut menjadi pesan yang tidak dapat dikenali.

Dalam perancangan sistem ini, masih banyak kendala-kendala yang ditemukan untuk dapat mengimplementasi sistem ini. Disamping biaya yang cukup tinggi yang dibutuhkan, kerumitan detail pengerjaannya juga menjadi salah satu kendala. Oleh karena itu, diharapkan bagi pembaca yang berkenan mendajadikan makalah ini sebagai referensi untuk perancangan sistem pengamanan yang lebih baik, dapat memperimbangkan dan memperhatikan detail pengerjaannya dengan baik sehingga rancangan tersebut dapat terimplemetasi dengan baik dan memperkecil kerumitan yang terdapat didalamnya serta dapat memfasilitasi para pengguna sistem dengan hasil yang terpercaya.

Sekian makalah ini saya buat, atas perhatian pembaca saya mengucapkan terima kasih.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Kriptografi*, Institut Teknologi Bandung, 2006.

[2] http://bhank-adi.blogs.friendster.com/_welcome_to_blogs_bhanks_/2007/01/cara_kerja_pons.html

[3] http://elektronika-elektronika.blogspot.com/2007/03/cara-kerja-handphone.html

[4] http://www.e-dukasi.net/pengpop/pp_full.php?ppid=184&fname=tekno.htm