Makalah Seminar Tugas Akhir

SIMULASI KUNCI ELEKTRONIK TER-ENKRIPSI UNTUK APLIKASI *BLUETOOTH* PADA TELEPON SELULAR

Agung Satya Wardana[1], Imam Santoso[2], R. Rizal Isnanto[2]
Jurusan Teknik Elektro, Fakultas Teknik, Universitas Diponegoro
Jl. Prof. Sudharto, Tembalang, Semarang
e-mail : agung_satya_w@yahoo.com

Abstrak - Selama ini untuk membuka sebuah kunci pintu seseorang harus menggunakan sebuah anak kunci, sehingga untuk mengakses banyak pintu harus digunakan banyak anak kunci yang berbeda. Namun jika ponsel dijadikan sebagai kunci elektronik yang menerapkan kontrol akses, tentunya semua anak kunci tersebut tidak dibutuhkan lagi, cukup dengan satu ponsel dapat membuka banyak kunci.

Pada penelitian ini, dirancang simulasi kunci elektronik yang menggunakan ponsel sebagai pengendali jarak jauh, dan komputer sebagai pusat pengontrolnya. Komunikasi antara ponsel dan komputer menggunakan bluetooth. Kunci elektronik yang dikembangkan dalam penelitian ini disajikan dalam bentuk simulasi tiga buah gembok kunci yang ditampilkan pada perangkat lunak kontrol/server di komputer. Sistem kunci elektronik ini menerapkan kontrol akses dan sistem keamanan menggunakan enkripsi RC4 dan fungsi hash MD5.

Hasil pengujian menunjukkan bahwa telah berhasil dibangun sebuah sistem pengaturan kunci elektronik melalui jarak jauh, dimana dapat membuka/menutup simulasi gembok kunci dengan menggunakan ponsel, dan hanya orang-orang yang telah terdaftar serta memiliki hak akses saja yang dapat membuka/menutup simulasi gembok kunci elektronik tersebut. Selain itu, pemantauan status kunci dapat dilakukan baik dari komputer maupun ponsel.

Kata Kunci : Kunci elektronik, Kunci bluetooth, BTkey, Enkripsi, MD5, RC4

I PENDAHULUAN

1.1 Latar Belakang

Bluetooth dan inframerah pada telepon selular merupakan teknologi yang telah lama muncul. Menyusul sekarang teknologi *Wi-fi* pada piranti tersebut. Akan tetapi aplikasi-aplikasi yang memanfaatkannya belum banyak digali. Salah satu aplikasi yang dapat diterapkan pada ponsel berfasilitas *bluetooth* adalah menggunakannya sebagai perangkat pengakses kunci elektronik secara nirkabel. Kunci elektronik yang dimaksud adalah suatu kunci pintu yang untuk membuka atau menguncinya tidak memerlukan anak kunci tapi dengan menggunakan perintah yang disampaikan secara digital.

Kunci elektronik biasanya digunakan untuk mengunci sesuatu yang penggunaannya dibatasi, jadi hanya orang-orang tertentu yang mempunyai hak akses. Sehingga, kunci elektronik yang baik harus memiliki sistem kendali akses yang terjamin keamanannya, dan juga harus memiliki catatan terhadap semua pengaksesan yang terjadi pada kunci elektronik tersebut.

1.2 Tujuan

Tujuan yang ingin dicapai dalam Tugas Akhir ini adalah : menghasilkan sebuah simulasi kunci elektronik dengan tingkat keamanan yang cukup baik melalui proses enkripsi yang dapat dikontrol secara digital melalui ponsel berfasilitas *bluetooth.*

1.3 Batasan Masalah

Untuk lebih terfokus dalam proses analisa Tugas Akhir ini maka ada beberapa hal yang dijadikan sebagai batasan masalah yaitu :

1. Sistem yang dirancang difokuskan pada sistem keamanan dengan pembatasan akses (*Access Control)* terhadap kunci elektronik yang dilakukan oleh komputer, dan pada keamanan pengiriman perintah dari ponsel ke komputer melalui *bluetooth*.
2. Proses enkripsi yang digunakan (MD5 dan RC4) tidak dibahas secara mendalam karena hanya digunakan sebagai pembanding dari perintah yang diterima oleh server dengan data yang telah tersimpan pada basisdata server.
3. Kunci elektroniknya berupa simulasi menggunakan perangkat lunak yang dibuat sebagai server/kontrol pada komputer.
4. Pesan dikirimkan dari ponsel ke komputer menggunakan *bluetooth*, Sehingga ponsel yang digunakan harus mendukung Java MIDP 2.0 dan JSR-82 dan menggunakan sistem operasi Symbian series 60 2nd Edition.
5. Modul Anak Kunci *Bluetooth* akan dibuat dengan bahasa pemrograman J2ME.
6. Modul Kontrol Kunci *Bluetooth* akan dibuat dengan bahasa pemrograman Java dengan editor teks Netbeans IDE 4.1

II DASAR TEORI

2.1 Teknologi *Bluetooth*

2.1.1 Pengertian *Bluetooth*

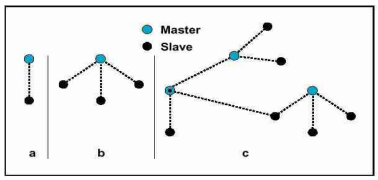
Bluetooth adalah sebuah teknologi komunikasi tanpa kabel yang beroperasi pada pita frekuensi 2,4 GHz *unlicensed ISM (Industrial, Scientific and Medical)* dengan menggunakan sebuah *frequency hopping transceiver* yang mampu menyediakan layanan komunikasi data dan suara secara waktu-nyata antara *host-host bluetooth* dengan jarak jangkauan layanan yang terbatas.

Pengembangan teknologi ini dipromotori oleh lima perusahaan yaitu Ericsson, IBM, Intel, Nokia dan Toshiba yang membentuk sebuah *Special Interest*

[1] Mahasiswa Teknik Elektro UNDIP
[2] Staf Pengajar Teknik Elektro UNDIP

Group (SIG) Pada bulan Mei 1998. Penggunaan kata "*bluetooth"* karena terinspirasi oleh seorang raja Viking (Denmark) yang bernama Harald Blatand. Raja Harald Blatand ini berkuasa pada abad ke-10 dengan menguasai sebagian besar daerah Denmark dan daerah Skandinavia pada masa itu. Dikarenakan daerah kekuasaannya yang luas, raja Harald Blatand ini membiayai para ilmuwan dan insinyur untuk membangun sebuah proyek berteknologi tinggi yang bertujuan untuk mengontrol pasukan dari suku-suku di daerah Skandinavia tersebut dari jarak jauh. Maka untuk menghormati ide raja Viking tersebut, yaitu Blatand yang berarti *bluetooth* (dalam bahasa Inggris) proyek ini diberi nama.

Komunikasi antar peralatan *bluetooth* akan menghasilkan sebuah jaringan *bluetooth* yang dinamakan dengan *piconet.* Sebuah *piconet* paling sederhana terdiri atas dua buah peralatan *bluetooth* dimana salah satu modul yang menginisiasi koneksi disebut sebagai *master,* sedangkan peralatan lain yang menerima inisiasi tadi dinamakan *slave.* Jika hanya dua peralatan yang berkomunikasi, maka koneksi dikatakan sebagai *point-to-point* (Gambar 2.1 (a)). Satu *master* dapat memiliki lebih dari satu koneksi secara simultan dengan beberapa *slave* pada saat bersamaan. Koneksi ini dinamakan dengan koneksi *point-to-multipoint* (Gambar 2.1 (b)). Kedua koneksi tersebut masih merupakan bagian dari *piconet. Piconet-piconet* dapat saling berkomunikasi untuk membentuk sebuah jaringan baru yang dinamakan *scatternet* (Gambar 2.1 (c)).



Gambar 2.1 *Bluetooth piconet* dan *scatter net*
(a) *point-to-point*
(b) *point-to-multipoint*
(c) *scatternet*

2.1.2 Keamanan *Bluetooth*

1. **Autentikasi,** memastikan identitas peralatan *bluetooth*.
2. ***Pairing,*** suatu prosedur autentikasi yang membuktikan keaslian dua alat berdasarkan sebuah kata kunci, untuk menciptakan hubungan yang dapat dipercaya antara alat tersebut.
3. **Autorisasi,** suatu proses untuk menentukan apakah alat diizinkan untuk menggunakan suatu layanan dari alat lain.
4. **Enkripsi,** untuk melindungi komunikasi dari penyadapan.

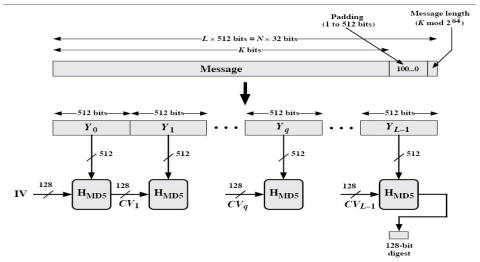
2.2 Enkripsi dan Dekripsi

Enkripsi adalah sebuah proses untuk mengamankan dan melindungi suatu informasi dengan menggunakan algoritma tertentu yang akan mengacak informasi asli (*plaintext*) menjadi bentuk yang tidak dapat dibaca atau dilihat (*ciphertext*) oleh orang atau pihak yang tidak berhak.

Gambar 2.2 Proses Enkripsi dan Dekripsi

2.2.1 Algoritma Message Digest 5 (MD5)

Algoritma ini mengambil masukan berupa panjang pesan (dalam bit) dari sebuah pesan, kemudian diproses dalam blok-blok dengan panjang blok 512 bit, sehingga menghasilkan keluaran berupa 128 bit pesan pendek (*digest*). Algoritma MD5 terdiri dari 5 langkah, langkah-langkah tersebut dapat dilihat pada Gambar 2.3.

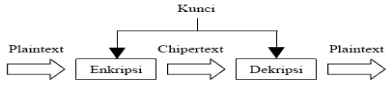


Gambar 2.3 Langkah-langkah Algoritma MD5

1. Menambahkan bit tambahan (*padding*).
2. Menambahkan panjang pesan.
3. Inisialisasi *buffer* MD.
4. Proses pesan didalam blok 512 bit.
5. Hasil Keluaran.

2.2.2 Algoritma Rivest Code 4 (RC4)

RC4 merupakan salah satu jenis *stream cipher* yang dibuat oleh Ronald Rivest pada tahun 1987. RC4 merupakan *stream cipher* berarti *plaintext* (pesan asli) akan diproses per-bit, dengan demikian *ciphertext* (pesan ter-sandi) dan *plaintext* akan memiliki panjang yang sama. RC4 menggunakan kunci simetris sehingga pada proses enkripsi dan dekripsi akan menggunakan kunci yang sama.

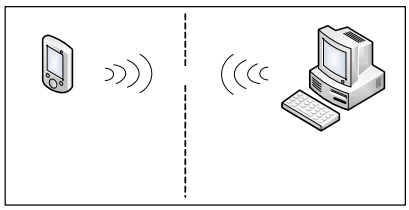


Gambar 2.4 Enkripsi-Dekripsi kunci simetris RC4

III PERANCANGAN SISTEM

Perancangan simulasi kunci elektronik terenkripsi untuk aplikasi *bluetooth* pada telepon selular bertujuan untuk membuat sebuah *prototype* kunci elektronik yang pengontrolannya dilakukan dengan mengirimkan perintah terenkripsi oleh ponsel melalui koneksi *bluetooth*.

Sistem yang dirancang ini terdiri dari dua modul yaitu modul Anak Kunci *Bluetooth* (AKB) berupa aplikasi pada ponsel dan modul Kontrol Kunci *Bluetooth* (KKB) berupa aplikasi pada komputer. Blok diagram dari simulasi kunci elektronik terenkripsi untuk aplikasi *bluetooth* pada telepon selular dapat dilihat pada Gambar 3.1.

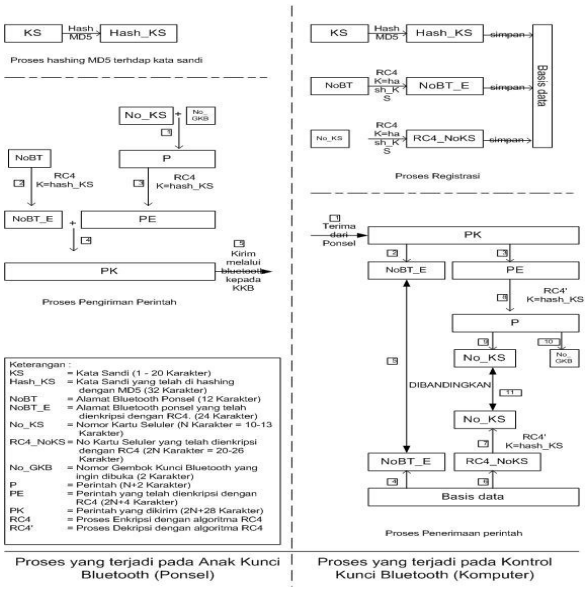


Gambar 3.1 Perancangan sistem

Kebutuhan dasar untuk menggunakan perangkat lunak pada program tugas akhir ini, yaitu ponsel yang digunakan harus mendukung pemrograman komunikasi *bluetooth* dengan J2ME. Kedua, komputer yang bekerja sebagai server harus memiliki sistem operasi Windows XP Service Pack 2 dan sebuah *bluetooth dongle* yang didukung secara *plug and play* oleh sistem operasi tersebut.

3.1 Blok Diagram perancangan Aplikasi

Pada Gambar 3.2, pada proses registrasi di aplikasi Kontrol Kunci *Bluetooth* pengguna akan diminta untuk memasukan data yang diperlukan, yaitu: kata sandi, nomor ID *bluetooth*, dan nomor kartu selular yang digunakan sebagai identitas pengguna pada saat hendak mengontrol kunci. Kata sandi nantinya akan dienkripsi menggunakan algoritma MD5 untuk mendapatkan nilai hash-nya, ID *bluetooth* dan nomor kartu selular dienkripsi menggunakan algoritma RC4, ketiga hal tersebut kemudian disimpan pada basisdata.



Gambar 3.2 Blok diagram proses yang terjadi pada aplikasi

Proses pengiriman perintah dari aplikasi AKB ke KKB pada Gambar 3.2 dapat dijelaskan sebagai berikut: pada AKB, nomor kunci yang akan diakses, nomor kartu selular, dan nomor ID *bluetooth* dienkripsi menggunakan algoritma RC4 dengan kata kunci yang merupakan kata sandi yang telah diambil nilai hash-nya, hasil enkripsi tersebut akan menjadi perintah yang akan dikirimkan ke server. Kemudian perintah yang telah dikirimkan oleh ponsel diterima aplikasi server KKB

Pada server, perintah yang diterima dibagi menjadi ID *bluetooth* dan perintah yang telah dienkripsi. ID *bluetooth* yang telah dienkripsi kemudian dibandingkan dengan yang tersimpan pada basisdata, jika sesuai maka selanjutnya perintah dapat diproses.

Perintah yang dienkripsi dengan RC4 kemudian didekripsi menggunakan kata kunci nilai *hash* dari kata sandi, sehingga didapat perintah asli. Perintah asli juga dibagi menjadi nomor kartu selular dan nomor kunci yang diakses, nomor kartu selular ini akan dibandingkan dengan hasil dekripsi dari nomor kartu selular yang tersimpan pada basisdata. Jika sesuai, maka perintah siap dieksekusi oleh server dengan membuka/menutup kunci yang diakses. Setelah perintah dieksekusi server kemudian mengirimkan pesan konfirmasi ke ponsel bahwa kunci telah terbuka/tertutup. Proses ini juga berlaku jika pengguna AKB akan mengakses riwayat pengaksesan.

3.2 Keamanan sistem yang dirancang

Keamanan komputer melingkupi empat aspek, yaitu *privacy, integrity, authentication, dan availability*. Selain keempat aspek tersebut, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan keamanan komputer, yaitu kontrol akses dan *non-repudiation.*

Privacy/Confidentiality (Kerahasiaan) adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Dalam sistem yang dirancang, pengguna harus melakukan pendaftaran terlebih dahulu untuk memperoleh hak pengaksesan, pada saat pendaftaran calon pengguna akan memberikan data yang diperlukan, Tentunya data tersebut harus dijaga kerahasiaannya, untuk itu data tersebut tidak langsung disimpan ke dalam basisdata, namun akan dilakukan pengacakan sebelum disimpan ke basisdata, dengan demikian akan terjamin kerahasiaannya.

Integrity (keutuhan) menekankan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi. Sebuah pesan dapat saja "ditangkap" (*intercept*) di tengah jalan, diubah isinya (*altered*, *tampered*, *modified*), kemudian diteruskan ke alamat yang dituju. Dalam sistem yang dirancang, perintah yang dikirimkan harus dijaga keutuhannya. Perintah sebelum dikirimkan akan dienkripsi dengan RC4 dengan kata sandi yang telah di-hash dengan MD5 sebagai kuncinya.

Authentication (pembuktian keaslian) berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Dalam sistem yang dirancang, Terdapat tiga pembuktian yang dilakukan yaitu pembuktian terhadap ponsel yang digunakan berdasarkan ID *bluetooth* ponsel, pembuktian terhadap nomor kartu selular yang digunakan, dan pembuktian dengan kata sandi. Data tersebut (alamat *bluetooth*, nomor kartu selular dan kata sandi) akan dikirimkan sebagai perintah untuk

membuka/menutup kunci oleh ponsel kepada komputer. Komputer akan membandingkan ketiga data tersebut dengan basisdata yang ada.

Availability (ketersediaan) berhubungan dengan ketersediaan informasi ketika dibutuhkan. Dalam hal ini maka server *bluetooth* pada komputer harus selalu diaktifkan dan server dapat memberikan layanan (membuka dan menutup kunci) tiap kali dibutuhkan. Selain itu, komputer harus dilengkapi dengan energi cadangan seperti batere guna mengatasi permasalahan jika listrik PLN padam.

Access Control (kontrol akses) berhubungan dengan cara pengaturan akses kepada informasi. Pada sistem yang dirancang, pengguna akan dibatasi aksesnya, pembatasan tersebut berupa: pembatasan waktu penggunaan, pembatasan terhadap kunci yang dapat diakses. Jadi pengguna hanya dapat mengakses kunci tertentu dan pada waktu tertentu saja. Pengaturan terhadap akses kontrol ini dilakukan melalui komputer.

Non-repudiation (tanpa penyangkalan) menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dalam sistem yang dirancang, agar seorang pengguna tidak dapat menyangkal telah melakukan pengaksesan kunci, maka akan dilakukan pencatatan terhadap semua pengaksesan yang terjadi.

IV PENGUJIAN DAN ANALISIS SISTEM

Pengujian yang dilakukan meliputi lima tahap, yaitu.

4.1 Pengujian Perangkat Lunak

Pengujian dilakukan dengan memilih setiap menu dari modul anak kunci *bluetooth* dan modul kontrol kunci *bluetooth*.

4.2 Pengujian koneksi antara Ponsel dengan Komputer menggunakan komunikasi *Bluetooth*

Pengujian ini bertujuan untuk mengetahui keberhasilan komputer (server) dan ponsel (klien) dalam membangun koneksi *bluetooth*. Untuk dukungan komunikasi *bluetooth* pada komputer akan digunakan USB Bluetooth Adapter. Pengujian dilakukan sebanyak 9 kali dengan jarak antara komputer dengan ponsel sejauh 2 meter.

TABEL 4.1 PENGUJIAN KONEKSI PONSEL DENGAN KOMPUTER MENGGUNAKAN *BLUETOOTH*

Pengujian ke-	klien yang telah terkoneksi	Ponsel yang digunakan	Komputer menanggapi	Status koneksi
1	Belum ada	Nokia 6600	Ya	Berhasil
2	Belum ada	Nokia 3230	Ya	Berhasil
3	Belum ada	Nokia 7610	Ya	Berhasil
4	Satu klien	Nokia 6600	Ya	Berhasil
5	Satu klien	Nokia 3230	Ya	Berhasil
6	Satu klien	Nokia 7610	Ya	Berhasil
7	Dua klien	Nokia 6600	Ya	Berhasil
8	Dua klien	Nokia 3230	Ya	Berhasil
9	Dua klien	Nokia 7610	Ya	Berhasil

4.3 Pengujian pengaturan perintah Buka/Tutup kunci melalui Ponsel dan Komputer

Pada pengujian ini akan dilakukan pengontrolan menggunakan ponsel seri Nokia 6600 dan Nokia 7610 dengan klien terdaftar yang berbeda. Tiap klien diberi wewenang penuh untuk dapat membuka/menutup semua kunci dan pengujian dilakukan dengan membuka masing-masing kunci oleh kedua klien. Jika server menanggapi dan mengeksekusi perintah maka pengujian berhasil, jika klien salah memasukkan kata sandi dan nomor kunci maka server akan mengirimkan laporan kesalahan.

TABEL 4.2 PENGUJIAN PENGATURAN KUNCI DENGAN PONSEL

uji ke-	Kunci di akses	Ponsel di gunakan	Nama pengguna terdaftar	Status kunci sebelum	Status kunci setelah	Status pengaturan
1	1	Nokia 6600	Agung	Tertutup	Terbuka	Berhasil
2	1	Nokia 6600	Agung	Terbuka	Tertutup	Berhasil
3	2	Nokia 6600	Agung	Tertutup	Terbuka	Berhasil
4	2	Nokia 6600	Agung	Terbuka	Tertutup	Berhasil
5	3	Nokia 6600	Agung	Tertutup	Terbuka	Berhasil
6	3	Nokia 6600	Agung	Terbuka	Tertutup	Berhasil
7	1	Nokia 7610	Ata	Tertutup	Terbuka	Berhasil
8	1	Nokia 7610	Ata	Terbuka	Tertutup	Berhasil
9	2	Nokia 7610	Ata	Tertutup	Terbuka	Berhasil
10	2	Nokia 7610	Ata	Terbuka	Tertutup	Berhasil
11	3	Nokia 7610	Ata	Tertutup	Terbuka	Berhasil
12	3	Nokia 7610	Ata	Terbuka	Tertutup	Berhasil

Pengujian pengaturan kunci dari komputer dilakukan dengan membuka atau menutup kunci tertentu dengan cara meng-klik salah satu gembok kunci yang terdapat pada panel kunci, jika perangkat yang dipilih terbuka/tertutup berarti pengujian berhasil.

TABEL 4.3 PENGUJIAN PENGATURAN KUNCI MELALUI SERVER

Pengujian ke-	Kunci yang diakses	Nama pengguna terdaftar	Status kunci sebelum	Status kunci setelah	Status pengaturan
1	1	Administrator	Tertutup	Terbuka	Berhasil
2	2	Administrator	Tertutup	Terbuka	Berhasil
3	3	Administrator	Tertutup	Terbuka	Berhasil
4	1	Administrator	Terbuka	Tertutup	Berhasil
5	2	Administrator	Terbuka	Tertutup	Berhasil
6	3	Administrator	Terbuka	Tertutup	Berhasil

Berdasarkan data hasil pengujian pengaturan pada Tabel 4.2 dan Tabel 4.3 menunjukkan bahwa pengaturan kunci dapat dilakukan yang membuktikan keberhasilan dari pengujian.

4.4 Pengujian Kontrol Akses terhadap pengguna Ponsel

Pengujian kontrol akses terhadap pengguna ponsel dilakukan dengan mengatur kunci yang dapat diakses dan waktu pengaksesan dan mencoba mengakses kunci pada hak akses yang diperbolehkan dan tidak diperbolehkan, jika perangkat yang dipilih terbuka/tertutup dan server menanggapi berarti pengujian berhasil. Pengujian ini bertujuan untuk mengetahui tingkat keamanan sistem dalam menjalankan perintah sesuai dengan hak akses yang diberikan.

TABEL 4.4 PENGUJIAN PENGATURAN KONTROL AKSES PENGGUNA

Uji ke-	Kunci di akses	Hari akses	Ponsel	klien terdaftar	Hak akses kunci	Hak hari akses*	Status kontrol
1	1	Senin	Nokia 6600	Agung	1, 2, 3	YYYYYYY	Berhasil
2	2	Selasa	Nokia 6600	Agung	1, 2, 3	YYYYYYY	Berhasil
3	3	Jumat	Nokia 6600	Agung	1, 2, 3	YYYYYYY	Berhasil
4	1	Senin	Nokia 7610	Ata	1,2	YNYNYNY	Berhasil
5	2	Kamis	Nokia 7610	Ata	1,2	YNYNYNY	Tidak berhasil
6	3	Rabu	Nokia 7610	Ata	1,2	YNYNYNY	Tidak berhasil
7	1	Senin	Nokia 6600	Agung	1	NNYNNNY	Tidak berhasil
8	1	Rabu	Nokia 6600	Agung	1	NNYNNNY	Berhasil
9	3	Rabu	Nokia 6600	Agung	1	NNYNNNY	Tidak berhasil
10	1	Selasa	Nokia 7610	Ata	2,3	NYNNYYN	Tidak berhasil
11	2	Selasa	Nokia 7610	Ata	2,3	NYNNYYN	Berhasil
12	2	Senin	Nokia 7610	Ata	2,3	NYNNYYN	Tidak Berhasil

* Keterangan; YYYYYYY = Senin, Selasa, Rabu, Kamis, Jum'at, Sabtu, Minggu (setiap hari)
YNYYNNY = Senin, Rabu, Kamis, Minggu
Y = Bisa Akses
N = Tidak bisa Akses

Data hasil pengujian kontrol akses terhadap pengguna ponsel pada Tabel 4.4, menunjukkan bahwa dari 12 kali pengujian dengan klien yang berbeda, kontrol akses berhasil dilakukan. klien diberikan fasilitas berbeda seperti pada pengujian pertama digunakan ponsel Nokia 6600 yang diberikan hak akses penuh terhadap kunci dan hari pengaksesan, kemudian klien memberikan perintah ke server untuk mengatur kunci dan server menanggapi dan mengeksekusi perintah yang diberikan. Karakter "Y" pada hari akses berarti memiliki hak akses, dan karakter "N" menunjukkan tidak memiliki hak akses, Karakter pertama menunjukkan hak akses pada hari Senin, karakter kedua menunjukkan hak akses pada hari Selasa, karakter ketiga menunjukkan hak akses pada hari Rabu, karakter keempat menunjukkan hak akses pada hari Kamis, karakter kelima menunjukkan hak akses pada hari Jumat, karakter keenam menunjukkan hak akses pada hari Sabtu, dan karakter ketujuh menunjukkan hak akses pada hari Minggu.

4.5 Pengujian jarak komunikasi *Bluetooth*

Pengujian jarak komunikasi *bluetooth* dilakukan dengan melakukan pengaturan kunci dari jarak yang berbeda-beda. Pengujian ini bertujuan untuk mengetahui jarak maksimal dari pengaturan perangkat antara ponsel dengan komputer sebagai server. Pada tiap pengujian juga akan dicoba, mengatur kunci baik dengan menghadap server, maupun membelakangi server.

TABEL 4.5 PENGUJIAN JARAK KOMUNIKASI *BLUETOOTH* SAAT PENGATURAN KUNCI

Uji ke-	Jarak (meter)	Tipe ruangan	Status pengaturan	Keterangan
1	2	Dengan halangan	Berhasil	Membelakangi dan menghadap server
2	4	Dengan halangan	Berhasil	Membelakangi dan menghadap server
3	5	Dengan halangan	Berhasil	Membelakangi dan menghadap server
4	6	Dengan halangan	Berhasil	Menghadap server
5	8	Dengan halangan	Berhasil	Menghadap server
6	9	Dengan halangan	Gagal	Menghadap server
7	2	Tanpa halangan	Berhasil	Membelakangi dan menghadap server
8	6	Tanpa halangan	Berhasil	Membelakangi dan menghadap server
9	10	Tanpa halangan	Berhasil	Menghadap server
10	15	Tanpa halangan	Berhasil	Menghadap server
11	20	Tanpa halangan	Berhasil	Menghadap server
12	30	Tanpa Halangan	Berhasil	Menghadap server

Dari data hasil pengujian pada Tabel 4.5, dapat diketahui untuk tipe ruangan dengan halangan, jarak maksimal pengaturan adalah 8 meter. Pada pengujian jarak pengaturan untuk jenis ruangan terbuka (tanpa halangan) didapatkan jarak maksimal yaitu 30 meter. Hasil yang sama didapatkan baik dengan cara menghadap ke server, maupun dengan membelakangi server.

V PENUTUP

5.1 Kesimpulan

Dari hasil pengujian dan analisis dapat disimpulkan hal – hal penting sebagai berikut :

1. Program aplikasi simulasi ini memiliki sistem keamanan dengan menerapkan kontrol akses, autentikasi dan verifikasi yang menggunakan fungsi hash MD5 dan enkripsi RC4.
2. Data pengguna yang disimpan di dalam basisdata dapat terjamin kerahasiaannya. Karena data tersebut tidak disimpan secara langsung di dalam basisdata, tapi data tersebut telah diacak terlebih dahulu dengan menggunakan algoritma fungsi

hash MD5 dan enkripsi RC4. Setelah proses pengacakan, barulah data disimpan di dalam basisdata.

3. Pengaturan kerja kunci dapat dilakukan dari komputer sebagai pusat pengendali, ini dibuktikan dari 6 kali pengujian, kunci dapat dibuka/ditutup 6 kali. Keberhasilan juga didapat ketika melakukan pengujian membuka/menutup kunci sebanyak 12 kali dari ponsel melalui komunikasi *bluetooth*.
4. Proses pemantauan status keadaan kunci dapat dilakukan, baik dari komputer maupun dari ponsel.
5. Sistem keamanan aplikasi juga terancang cukup baik, hal ini dibuktikan dari pengujian kontrol akses yang berhasil diterapkan dimana dari 12 kali pengujian terhadap 2 klien dengan hak akses yang berbeda server mampu menanggapi dan mengeksekusi perintah dengan baik.
6. Aplikasi dapat diterapkan pada kondisi ruangan yang terhalang tembok maupun tanpa halangan, dimana untuk kondisi ruangan dengan halangan diperoleh jarak maksimal pengaturan 8 meter dan tanpa halangan diperoleh jarak maksimal pengaturan 30 meter.

5.2 Saran

Berdasarkan hasil perancangan program simulasi ini, ada beberapa saran yang muncul agar perancangan ini dapat dilanjutkan dengan beberapa pengembangan, antara lain:

1. Keamanan sistem akan sangat terjamin selama klien maupun admin tidak memberitahukan ke pihak lain mengenai data pengguna yang tersimpan pada basisdata.
2. Simulasi kunci elektronik yang hanya menggunakan perangkat lunak dapat dikembangkan lagi menjadi rangkaian kunci elektronik yang benar-benar bisa digunakan.
3. Modul kontrol kunci *bluetooth* dan gembok kunci *bluetooth* juga dapat dikembangkan tanpa menggunakan komputer. Jadi langsung menggunakan mikrokontroler yang mendukung *chip bluetooth*. Dengan demikian ponsel langsung berkomunikasi dengan rangkaian elektronik yang menggunakan mikrokontroler sebagai kunci elektroniknya.

DAFTAR PUSTAKA

[1] Afandi, R. "*Penggunaan Telepon genggam dengan menggunakan teknologi Bluetooth sebagai interface pusat pengaturan kerja penerangan dan pintu garasi rumah"*. Tugas Akhir, UNDIP, Semarang. 2007.

[2] Benhui. "*Connecting PC and Phone with Java Bluetooth API–Part 1"*. http://www.benhui.net/modules.php?name=Bluetooth&page=Connect_PC_Phone_Part_1.html , Februari 2008.

[3] Gehrmann, C. J. Persson. and B. Smeets. "*Bluetooth Security"*. Artech House; Boston. 2004.

[4] Dasgupta, K. "*Protocols in Bluetooth Architecture"*. http://www.cs.utk.edu/~dasgupta/bluetooth/blueprotocols.htm, Februari 2008.

[5] Haartsen, Japp. "*Bluetooth Baseband"*. http://www.palowireless.com/infotooth/tutorial/baseband.asp, Februari 2008.

[6] Hartanto, A. A. *"Kajian dan Implementasi Sistem Keamanan Data pada Ponsel Berbasis J2ME Menggunakan Profile MIDP 1.0"*. http://budi.insan.co.id/courses/ec7010/2003/report-antonius.pdf. Februari 2008.

[7] Wahana Komputer. "*Panduan praktis Pengolahan Database dengan MySQL*",. Penerbit Andi, Yogyakarta, 2006.

[8] Nokia. "*Bluetooh Technologi Overview*", http://forum.nokia.com/ , Maret 2008.

[9] Sanjaya, R. "*Pengolahan Database MySQL 5 dengan Java 2"*. Penerbit Andi, Yogyakarta, 2005.

[10] Shalahuddin, M.. "*Pemrograman J2ME"*. Penerbit Informatika, 2006.

[11] Siyamta. "*Pengantar Teknologi Bluetooth"*. http://www.ilmukomputer.com, Februari 2008.

[12] Sutanto, T. "*Aplikasi Kriptografi dengan algoritma Message Digest 5* (MD5)". Tugas Akhir, UNDIP. Semarang. 2006

[13] Stallings, W. "*Crytography and Network Security Principles And Practices", 3rd Edition*. Upper Saddle River: Prentice Hall, 2003.

BIOGRAFI

Agung Satya Wardana

Lahir di Gemuhblanten, Kendal pada tanggal 01 Agustus 1985. Menempuh pendidikan di SDN 1 Tebo-Tengah lulus pada tahun 1997, kemudian melanjutkan ke SLTP Negeri 1 Tebo-Tengah lulus pada tahun 2000, kemudian melanjutkan ke SMU Negeri 1 Tebo-Tengah lulus tahun 2003. Saat ini sedang menyelesaikan studi Strata-1 di Jurusan Teknik Elektro Fakultas Teknik Universitas Diponegoro Semarang dengan Konsentrasi Elektronika dan Telekomunikasi.

Mengetahui/Mengesahkan,

Pembimbing I,

Imam Santoso, S.T., M.T.
NIP. 132 162 546

Pembimbing II,

R. Rizal Isnanto, S.T., M.M., M.T.
NIP. 132 288 515