
PERANCANGAN KUNCI ELEKTRIK DENGAN ENKRIPSI MELALUI BLUETOOTH PADA PONSEL

Audi Nantan¹, Mudrik Alaydrus²

Program Studi Teknik Elektro, Fakultas Teknik

Universitas Mercu Buana, Jakarta, Indonesia

Email: mudrikalaydrus@yahoo.com

Abstrak - Saat ini fasilitas yang disediakan oleh ponsel sangat beragam. Mulai dari telepon, SMS, kamera, music player, semuanya dijadikan satu. Tentunya ponsel juga dapat dijadikan sebagai kunci elektrik menggantikan kunci analog yang ada saat ini. Biasanya untuk membuka sebuah kunci pintu seseorang harus menggunakan sebuah anak kunci, jadi untuk mengakses banyak pintu harus memiliki banyak anak kunci yang berbeda-beda. Namun jika ponsel dijadikan sebagai kunci elektrik yang menerapkan access control tentunya semua anak kunci tersebut tidak dibutuhkan lagi, cukup dengan satu ponsel dapat membuka banyak kunci.

Kata kunci : kunci elektrik, enkripsi, bluetooth

PENDAHULUAN

Saat ini setiap orang tidak terlepas dari ponsel sebagai sarana

telekomunikasi mereka, terutama bagi mereka yang bermobilitas tinggi. Awalnya fungsi ponsel hanya sebagai alat komunikasi telepon, tapi karena perkembangannya sangat cepat maka sekarang ponsel bukan sekedar alat komunikasi saja. Ponsel saat ini sudah dipadukan dengan Pocket PC, kamera digital, dan perangkat digital lainnya, sehingga ponsel saat ini semakin pintar dan disebut smartphone. Layaknya sebuah komputer, ponsel-ponsel terbaru saat ini memiliki banyak aplikasi dan aplikasi tersebut dapat ditambahkan sesuai dengan kebutuhan. Aplikasi tersebut seperti game, pemutar musik dan video, kamus, pengolah gambar, penjelajah internet, chatting, dan berbagai aplikasi lainnya.

Tujuan Penelitian

Tujuan penelitian ini adalah merancang suatu sistem simulasi kunci elektrik melalui bluetooth agar

kedepan dapat menciptakan suatu sistem security access sehingga teknologi bluetooth yang kita dapatkan gratis dapat dimanfaatkan tidak hanya mengirim data melainkan dapat mengakses suatu sistem dengan memanfaatkan kelebihan dari fitur bluetooth itu sendiri.

Kunci Elektrik ini dapat digunakan untuk kunci pintu locker yang membutuhkan tingkat keamanan yang tinggi seperti deposit box pada bank, tempat penitipan barang, atau locker karyawan, selain untuk kunci locker juga dapat digunakan untuk kunci pintu ruangan yang membutuhkan pembatasan akses seperti ruang server komputer.

Pembatasan Masalah

Perancangan kunci elektrik ini akan dibatasi oleh beberapa hal yaitu:

- a. Pesan dikirimkan dari ponsel ke komputer menggunakan bluetooth. Sehingga ponsel yang digunakan harus mendukung Java yang mendukung JSR82 seperti Nokia 6200 yang menggunakan sistem operasi Symbian OS 7.0s

- b. Terdapat 3 buah kunci yang bersifat paralel.

Ada pembatasan akses, misalkan: user A hanya dapat mengakses kunci 1 dan 2, user B dapat mengakses kunci 2 dan 3, dan user C hanya dapat mengakses kunci 1 saja. Selain itu juga dapat dibatasi waktu penggunaannya. Pembatasan akses tersebut dapat dikontrol melalui Komputer. Terdapat catatan terhadap setiap pengaksesan yang terjadi. Pada penerapannya komputer sebaiknya dilengkapi dengan energi cadangan seperti mesin diesel untuk berjaga-jaga bila listrik PLN padam.

LANDASAN TEORI

Sistem yang Dirancang

Sistem yang dirancang berupa simulasi kunci elektrik yang dikontrol melalui ponsel berfasilitas bluetooth. Pengontrolan dilakukan dengan cara mengirimkan perintah melalui bluetooth kepada komputer yang bertindak sebagai penghubung antara ponsel dan simulasi kunci elektrik. Sistem yang dirancang difokuskan pada sistem keamanan dengan pembatasan pengaksesan (Access Control) terhadap kunci elektrik yang dilakukan oleh

komputer, dan pada keamanan pengiriman perintah dari ponsel ke komputer melalui bluetooth. Sedangkan kunci elektriknya hanya berupa simulasi dengan menggunakan lampu LED yang dihubungkan melalui parallel port pada komputer.

Bluetooth

Teknologi Bluetooth tidak dirancang untuk melakukan komunikasi data dan suara yang memerlukan kapasitas yang besar. Karenanya, Bluetooth tidak dapat menggantikan LAN (Local Area Network), WAN (Wide Area Network) maupun kabel backbone. Teknologi Bluetooth memang khusus dirancang untuk mendukung pengguna peralatan mobile seperti notebook beserta peralatan pendukungnya seperti printer, scanner, mouse dan peralatan komunikasi seperti ponsel dan PDA.

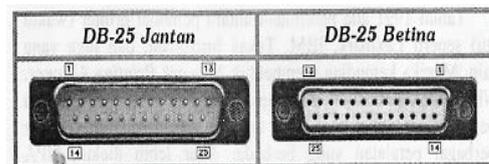
Algoritma MD5 dan RC4

Algoritma MD5 dikembangkan oleh Ron Rivest pada tahun 1992 di MIT (Massachusetts Institute of Technology). Algoritma ini melakukan hashing terhadap pesan dengan panjang tak terhingga per block sebesar 512 bit untuk

menghasilkan 128 bit message Digest.

RC4 merupakan salah satu jenis stream cipher yang dibuat oleh Ron Rivest. RC4 merupakan stream cipher berarti plaintext akan diproses per-bit, dengan demikian ciphertext dan plaintext akan memiliki panjang yang sama. RC4 menggunakan kunci simetris sehingga pada proses enkripsi dan dekripsi akan menggunakan kunci yang sama. Panjang kunci yang digunakan bebas antara 1 sampai 256 byte

Parallel Port

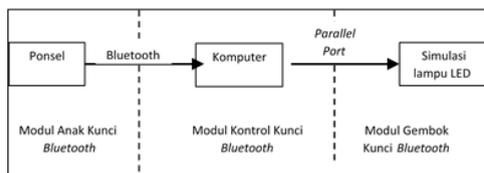


PERANCANGAN DAN PEMBUATAN

Perancangan Sistem

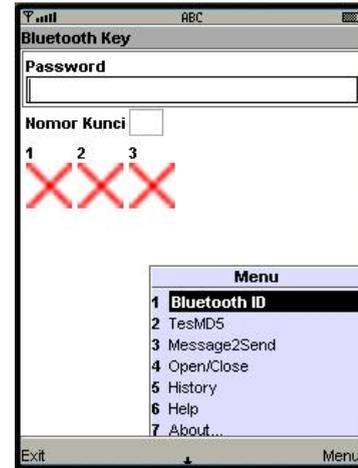
Perancangan Simulasi Kunci Elektrik dengan Enkripsi Melalui Bluetooth pada Ponsel bertujuan untuk membuat sebuah prototype kunci elektrik yang pengontrolannya dilakukan dengan mengirimkan perintah terenkripsi oleh ponsel melalui bluetooth. Perancangan Simulasi ini diawali dengan perancangan blok diagram dari

sistem yang dirancang, dan dilanjutkan dengan perancangan semua modul yang akan dibuat berupa: perancangan menu; perancangan antarmuka program; perancangan laporan, pesan kesalahan dan Error Handling, dan perancangan basis data. Setelah itu baru dibuat aplikasi secara keseluruhan.



Pembuatan aplikasi Anak Kunci Bluetooth.

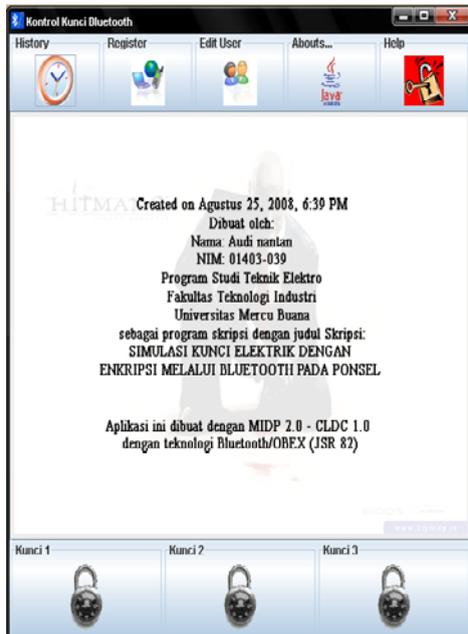
Modul ini merupakan sebuah aplikasi yang akan diinstal pada ponsel. Fungsi utama dari modul ini adalah mengirimkan perintah terenkripsi melalui bluetooth kepada komputer (kontrol kunci bluetooth) untuk membuka kunci. Aplikasi ini dibuat dengan menggunakan Java2 Micro Edition (J2ME).



Pembuatan aplikasi Kontrol Kunci Bluetooth.

Pembuatan aplikasi Kontrol Kunci Bluetooth juga menggunakan Komputer yang sama seperti pembuatan aplikasi Anak Kunci Bluetooth diatas. Sedangkan perangkat lunak yang digunakan adalah sebagai berikut :

1. J2SDK 1.4.2.
2. Jcreator Pro 3.00
3. MySQL 5.0.18.
4. MySQL Front 5.1.191
5. mysql-connector-java-3.0.9
6. Blulet library
7. BlueCove library
8. Parallel port library
9. RC4Engine dan MD5Digest
10. HTML Help Workshop
4.74.8702
11. Macromedia Dreamweaver MX
12. Macromedia Flash MX
13. Adobe PhotoShop 7.0



Modul Gembok kunci Bluetooth

Modul Gembok kunci Bluetooth ini merupakan suatu perangkat keras yang dibuat dengan menggunakan:

1. Satu Buah DB25 Jantan.
2. Satu Meter Kabel yang berisi delapan ruas.
3. Tiga buah lampu LED berbeda warna.



PENGUJIAN

Pengujian program simulasi

Pengujian program simulasi kunci elektrik dengan enkripsi melalui Bluetooth pada ponsel

dilakukan untuk menguji dan memastikan bahwa program simulasi yang telah dirancang dan dibuat ini dapat berfungsi dengan baik dan sesuai dengan rumusan rancangan yang telah ditetapkan sebelumnya. Tanpa adanya pengujian, maka tidak dapat diketahui apakah program yang telah dibuat sesuai dengan spesifikasi rancangan program aplikasi.

Adapun kendala yang dihadapi dalam pengujian yaitu tidak sinkron seting BIOS Operating System komputer yang akan digunakan dalam pengujian simulasi. Setelah proses analisa yang cukup memakan waktu dan merubah seting sistem koneksi LPT1 di dalam BIOS disamakan dengan yang terdapat didalam seting Paralel Port ternyata proses simulasi berjalan dengan normal.

Kesimpulan dari Modul Anak Kunci Bluetooth adalah:

1. Kemampuan menjalankan menu open/close untuk mengirimkan perintah terenkripsi kepada Kontrol Kunci Bluetooth.
2. Kemampuan untuk menampilkan laporan dan pesan kesalahan sebagai hasil dari proses membuka atau menutup kunci.

3. Kemampuan menjalankan menu *history* untuk melihat catatan *history* dari penggunaan yang pernah dilakukan
4. Kemampuan menjalankan menu *About* untuk menampilkan keterangan mengenai aplikasi ini.
5. Kemampuan menjalankan menu *Help* untuk menampilkan pertolongan penggunaan aplikasi ini.
6. Kemampuan menjalankan menu *Exit* untuk keluar dari aplikasi.
5. Kemampuan menjalankan menu *Register* untuk melakukan pendaftaran pengguna baru.
6. Kemampuan menjalankan menu *Edit User* untuk melakukan perubahan pada data pengguna.
7. kemampuan menjalankan menu *About* untuk menampilkan keterangan mengenai aplikasi ini.
8. kemampuan menjalankan menu *Help* untuk menampilkan pertolongan penggunaan aplikasi ini.

Kesimpulan dari Modul Anak Kunci Bluetooth adalah:

1. Kemampuan mengirimkan pesan, laporan kesalahan dan catatan *history* kepada modul Anak Kunci Bluetooth.
2. Kemampuan membuka dan menutup modul Gembok Kunci Bluetooth.
3. Kemampuan untuk melakukan verifikasi dan pembatasan akses penggunaan Kunci.
4. Kemampuan menjalankan menu *history* untuk menyimpan dan menampilkan semua catatan *history* setiap pengaksesan aplikasi yang terjadi.

Kesimpulan dari Modul Anak Kunci Bluetooth adalah:

1. Lampu LED menyala sesuai dengan perintah yang dikirimkan oleh kontrol kunci Bluetooth yang menandakan kunci yang dimaksudkan terbuka.
2. Lampu LED padam sesuai dengan perintah yang dikirimkan oleh kontrol kunci Bluetooth yang menandakan kunci yang dimaksudkan tertutup.

METODE PENGUJIAN

Pengujian program simulasi kunci elektrik dengan enkripsi melalui Bluetooth pada ponsel ini

dilakukan dengan menggunakan metode *Black Box Testing*. Metode *Black Box Testing* ini merupakan pengujian program berdasarkan fungsi dari program. Tujuan dari metode *Black Box Testing* ini adalah untuk menemukan kesalahan fungsi pada program.

Pengujian dengan metode *Black Box Testing* dilakukan dengan cara memberikan sejumlah *input* pada program aplikasi yang kemudian diproses sesuai dengan kebutuhan fungsionalnya untuk melihat apakah program aplikasi menghasilkan *output* yang diinginkan dan sesuai dengan fungsi dari program aplikasi tersebut. Bila dari *input* yang diberikan proses menghasilkan *output* yang sesuai dengan kebutuhan fungsionalnya, maka program aplikasi yang bersangkutan telah benar, tetapi bila *output* yang dihasilkan tidak sesuai dengan kebutuhan fungsionalnya, maka masih terdapat kesalahan pada program aplikasi tersebut.

Pengujian dilakukan dengan mencoba semua kemungkinan yang terjadi dan dilakukan secara berulang-ulang. Jika dalam pengujian ditemukan kesalahan, maka akan

dilakukan penelusuran dan perbaikan (debugging) untuk memperbaiki kesalahan yang terjadi. Jika telah selesai melakukan perbaikan maka akan dilakukan pengujian kembali. Pengujian dan perbaikan dilakukan secara terus menerus hingga diperoleh hasil yang terbaik.

KESIMPULAN

Adapun kesimpulan yang diperoleh dari perancangan dan pembuatan program simulasi kunci elektrik dengan enkripsi melalui bluetooth pada ponsel, antara lain:

- 1 Program aplikasi simulasi ini dapat mengirimkan perintah terenkripsi dari ponsel ke komputer melalui koneksi bluetooth.
- 2 Program aplikasi simulasi ini memiliki sistem keamanan yang cukup baik dengan menerapkan kontrol akses, otentifikasi dan verifikasi yang menggunakan Hashing MD5 dan Enkripsi RC4.
- 3 Data pengguna yang disimpan didalam basis data dapat terjamin kerahasiaannya. Karena data tersebut tidak disimpan

secara langsung didalam basis data, tapi data tersebut telah diacak terlebih dahulu dengan menggunakan algoritma hashing MD5 dan enkripsi RC4. Setelah proses pengacakan barulah data disimpan didalam basis data.

- 4 Program aplikasi Kontrol Kunci Bluetooth hanya bisa dijalankan pada Sistem Operasi minimum Windows XP SP2 atau pada Windows XP SP1 yang telah ditambahkan tambahan *pack Hotfix Q323183*
- 5 Program aplikasi simulasi ini dapat mengontrol nyala dan padamnya lampu LED melalui *parallel port*.

Saran

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

1. Simulasi kunci elektrik yang hanya menggunakan lampu LED dapat dikembangkan lagi menjadi rangkaian kunci elektrik yang benar-benar

bisa digunakan. Dan jika memungkinkan, selanjutnya dapat di produksi secara massal dan menjadikannya sebagai trend yang baru yaitu membuka kunci tanpa menggunakan anak kunci melainkan menggunakan ponsel.

2. Modul Anak Kunci Bluetooth akan lebih baik jika dikembangkan dengan menggunakan bahasa pemrograman C/Symbian. Karena bahasa C/Symbian lebih mendukung fitur-fitur yang ada pada ponsel, khususnya yang bersistem operasi Symbian.
3. Modul Kontrol Kunci Bluetooth dan Gembok Kunci Bluetooth juga dapat dikembangkan tanpa menggunakan komputer. Jadi langsung menggunakan mikrokontroler yang mendukung chip bluetooth. Sehingga ponsel langsung berkomunikasi dengan rangkaian elektronik yang menggunakan mikrokontroler sebagai kunci elektroniknya

tanpa harus menggunakan pc / komputer sebagai akses administrator (pusat kontrol kunci bluetooth).

DAFTAR PUSTAKA

1. 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 , 17 Maret 2005.
2. Dasgupta, Korak. Protocols in Bluetooth Architecture, <http://www.cs.utk.edu/~dasgupta/bluetooth/blueprotocols.htm>, 18 Februari 2005.
3. Gehrmann, Christian; Persson, Joakim; and Smeets, Ben. Bluetooth Security. Boston : Artech House, 2004.
4. Haartsen, Japp. Bluetooth Baseband, <http://www.palowireless.com/infotooth/tutorial/baseband.asp>, 17 Februari 2005.
5. Nokia. Bluetooth Technology Overview, <http://forum.nokia.com/>, 2 Desember 2004.
6. Portillo, Juan Gabriel Del Cid. Parallel Printer Port Access through Java, <http://www.geocities.com/Juanga69/parport/>, 15 Mei 2005.
7. Stallings, William. Cryptography and Network Security Principles And Practices. 3rd Edition. Upper Saddle River: Prentice Hall, 2003.
8. Sutadi, Dwi. I/O Bus & Motherboard. Yogyakarta: ANDI Yogyakarta, 2002.3.