SIMULASI KUNCI ELEKTRONIK DENGAN ENKRIPSI MELALUI *BLUETOOTH* PADA PONSEL

Indri Neforawati[1]; Hoga Saragih[2]

[1] Jurusan Telekomunikasi, Fakultas Teknik Elektro, Politeknik Negeri Jakarta, Kampus Baru UI Depok, Bogor 16424
[2] Jurusan Magister Teknik Informatika, Fakultas Ilmu Komputer, Universitas Bina Nusantara, Jln. Kebun Jeruk Raya No. 27, Jakarta Barat 11530
kekake_3@yahoo.com; hogasaragih@gmail.com

ABSTRACT

Currently the facility provided by mobile phones is very diverse. Starting from the phone, SMS, camera, music player, all rolled into one. Obviously the phone can also be used as electronic keys to replace the existing analog key at this time. Usually, to open a door key one must use a key, so to access a lot of doors must have a lot of different keys. But if the phone is used as an electronic key access control must implement all the keys are not needed anymore, just with one phone can open many locks. Simulation of an electronic lock is designed to use the phone as a remote control, and the computer as a central controller. Communication between mobile phones and computers using Bluetooth. While functioning as a door lock which is connected via parallel port of computer. This electronic key system to apply Access Control using RC4 encryption and MD5 Hashing. Design modules are built using NetBeans IDE 4.1 and the MySQL database, with some additional libraries. Libraries that are mobility netbeans 4.1, mysql-connector-java-3.0.9, BlueCove, Bluelet-Benhui. Phones that use must support the Java MIDP 2.0 and JSR-82.

Keywords: *Hashing MD5, Enkripsi RC4, NetBeans IDE 4.1, mysql-connector-java-3.0.9*

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 elektronik 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 elektronik yang menerapkan access control tentunya semua anak kunci tersebut tidak dibutuhkan lagi, cukup dengan satu ponsel dapat membuka banyak kunci. Simulasi kunci elektronik dirancang yang menggunakan ponsel sebagai remote kontrol, dan komputer sebagai pusat pengontrolnya. Komunikasi antara ponsel dan komputer menggunakan bluetooth. Sedangkan yang berfungsi sebagai kuncinya berupa pintu yang dihubungkan melalui parallel port komputer. Sistem kunci elektronik ini menerapkan Access Control dengan menggunakan enkripsi RC4 dan Hashing MD5. Modul-modul rancangan ini dibuat dengan menggunakan NetBeans IDE 4.1 dan basis data MySQL, dengan beberapa library tambahan. Library yang dibutuhkan adalah netbeans mobility 4.1, mysql-connector-java-3.0.9, BlueCove, Bluelet-Benhui. Ponsel yang digunakan harus mendukung Java MIDP 2.0 dan JSR-82.

Kata kunci: *Hashing MD5, Enkripsi RC4, NetBeans IDE 4.1, mysql-connector-java-3.0.9*

PENDAHULUAN

Saat ini setiap orang tidak terlepas dari ponsel sebagai sarana telekomunikasi mereka, terutama bagi mereka yang mempunyai mobilitas 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.

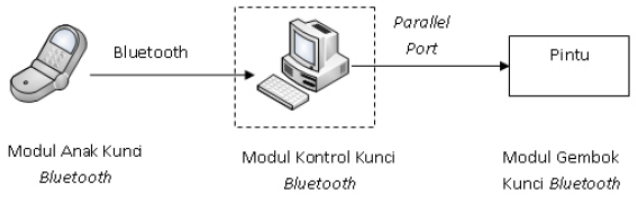
Ponsel juga dilengkapi dengan infra merah dan *bluetooth*, yang digunakan untuk melakukan transmisi data jarak dekat dengan peralatan-peralatan nirkabel lainnya. *Bluetooth* adalah suatu teknologi radio jarak pendek yang memungkinkan konektivitas tanpa kabel antara perangkat yang bersifat *mobile.* Namun, seperti diketahui koneksi nirkabel rentan tehadap sistem keamanannya; demikian pula dengan *bluetooth*. Untuk itu, aplikasi yang menggunakan *bluetooth* harus memiliki sistem keamanan tambahan seperti menggunakan enkripsi RC4 dan *hashing* MD5.

Salah satu aplikasi yang dapat diterapkan pada ponsel yang mempunyai fasilitas *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. Perintah yang disampaikan secara digital tersebut dapat berupa sensor infra red, kode yang dimasukan melalui papan ketik, sensor retina mata, sensor sidik jari, atau sensor suara.

Kunci elektronik biasanya digunakan untuk mengunci sesuatu yang penggunaannya dibatasi. Jadi, hanya orang-orang tertentu yang mempunyai hak akses. Sebagai contohnya adalah kunci elektronik digunakan pada pintu-pintu gedung yang memerlukan keamanan tingkat tinggi; serta pada ruangan yang hanya orang tertentu saja boleh masuk seperti ruang pusat kendali jaringan komputer, pada *deposit box* bank, atau bisa juga pada *locker-locker* karyawan sehingga kunci elektronik yang baik harus memiliki sistem pengontrolan akses yang terjamin keamanannya, dan juga harus memiliki catatan terhadap semua pengaksesan yang terjadi pada kunci elektronik tersebut. Catatan tersebut dapat digunakan untuk pelacakan jika diperlukan.

Pada rancangan ini, akan dibuat kunci elektronik yang untuk mengaksesnya menggunakan ponsel berfasilitas *bluetooth*. Sebenarnya, ada banyak cara yang dapat digunakan untuk mengakses kunci elektronik. Namun, rancangan ini memilih ponsel berfasilitas *bluetooth* karena beberapa pertimbangan seperti ponsel merupakan peralatan yang sudah sangat umum digunakan sehingga sangat memungkinkan, jika nantinya ponsel dapat menggantikan peran anak kunci yang biasanya digunakan. Koneksi untuk pengaksesannya menggunakan *bluetooth* karena penggunaan teknologi *bluetooth* tidak melalui operator telekomunikasi sehingga bersifat gratis, berbeda dengan SMS atau telepon.

Sistem yang dirancang berupa simulasi kunci elektronik, yang dikontrol melalui ponsel berfasilitas *bluetooth*. Pengontrolan dilakukan dengan cara mengirimkan perintah melalui *bluetooth* kepada komputer yang bertindak sebagai penghubung antara ponsel dan kunci elektronik. Sistem yang dirancang difokuskan pada sistem keamanan dengan pembatasan pengaksesan (*Access Control*) terhadap kunci elektronik yang dilakukan oleh komputer, dan pada keamanan pengiriman perintah dari ponsel ke komputer melalui *bluetooth*. Sedangkan kunci elektroniknya hanya berupa simulasi dengan menggunakan pintu yang dihubungkan melalui *parallel port* pada komputer.



Gambar 1 Blok Diagram Rancangan Kunci Elektronik dengan Enkripsi melalui *Bluetooth* pada Ponsel

Rancangan kunci elektronik melalui *Bluetooth* pada ponsel ini terdiri dari 3 buah modul, yaitu modul Anak Kunci *Bluetooth* (AKB) berupa aplikasi pada ponsel, modul Kontrol Kunci *Bluetooth* (KKB) berupa aplikasi pada komputer, dan modul Gembok Kunci *Bluetooth* (GKB) berupa simulasi pintu elektronik yang dihubungkan ke komputer melalui *parallel port*.

Fungsi utama dari modul Kontrol Kunci *Bluetooth* (KKB) adalah menerima kata sandi yang dikirimkan oleh anak kunci Microsoft dan membandingkannya dengan basis data, kemudian mengirimkan perintah kepada modul kunci (gembok kunci *Microsoft*) untuk membuka kunci sesuai dengan nomor kunci yang ingin dibuka; di mana semua proses tersebut dapat berjalan secara otomatis tanpa memerlukan operator. Operator atau administrator bertanggung jawab jika ada yang ingin registrasi, mengubah data pengguna atau ingin membuka blokir. Berikut diagram alir dari modul Kontrol Kunci *Bluetooth* (KKB) pada Microsoft (Gambar 2).

Setelah perintah yang dikirim diterima oleh komputer (Kontrol Kunci *Bluetooth*), maka perintah tersebut akan diproses sehingga dapat membuka kunci (Anak Kunci *Bluetooth*). Proses tersebut, yaitu (1) Mengambil *identified* (pengenal) berupa alamat *bluetooth* yang terenkripsi dari ponsel pengirim perintah, yang berada pada 24 karakter pertama dari pengguna yang diterima serta mengambil nomor pintu yang akan dibuka, yang terdapat pada 2 karakter terakhir dari pengguna; (2) Jika nomor alamat *bluetooth* tersebut terdaftar, maka dilanjutkan pada tahap ketiga. Jika tidak, maka proses dibatalkan dan dikirimkan pesan kesalahan kepada anak kunci *Microsoft* pada ponsel yang memberitahukan kata sandi yang digunakan salah atau ponsel, yang digunakan tidak terdaftar; (3) Dilakukan pengecekan pada basis data, apakah pengguna memiliki hak akses terhadap nomor pintu yang akan dibuka/ditutup. Jika memiliki hak akses, maka dilanjutkan pada tahap selanjutnya. Namun, jika tidak proses, maka dibatalkan dan dikirimkan pesan kesalahan kepada anak kunci *bluetooth*, yang memberitahukan pengguna tidak memiliki hak akses terhadap kunci yang bersangkutan; (4) Dilakukan pengecekan pada basis data, apakah saat ini pengguna yang bersangkutan memiliki hak akses atau tidak. Jika memiliki hak akses pada saat ini, maka dilanjutkan ke modul gembok kunci *Bluetooth* (pintu). Jika tidak, maka proses dibatalkan dan dikirimkan pesan kesalahan kepada anak kunci *Microsoft* yang memberitahukan bahwa pada saat ini pengguna tidak memiliki hak akses; (5) Dilakukan pengecekan terhadap Gembok Kunci *Bluetooth* (pintu) yang bersangkutan, apakah sedang terbuka atau tertutup. Jika sedang terbuka, maka Gembok Kunci *Bluetooth* (pintu) tersebut akan ditutup. Jika sedang tertutup, maka Gembok Kunci *Bluetooth* (pintu) tersebut akan dibuka. Sampai di sini proses selesai.

Basis data yang digunakan pada basis data Kontrol Kunci *Bluetooth* (KKB) adalah MySQL, dengan menggunakan 2 buah Tabel, yaitu (1) tabel *user*, yang berfungsi menyimpan data-data pengguna; dan (2) tabel *history*, yang berfungsi untuk menyimpan seluruh *history*. Sedangkan spesifikasi Micro dapat dilihat pada Tabel 1.

Aplikasi Kontrol Kunci *Bluetooh* (KKH) dibuat seluruhnya dengan menggunakan pemrograman java melalui suatu *software* yang bernama Netbeans. Adapun keseluruhan perangkat lunak yang digunakan adalah (1) J2SDK 1.4.2; (2) NetBeans IDE 4.1, yang digunakan untuk menuliskan *coding* dan kompilasi; (3) Basis data yang digunakan adalah MySQL 4.0.21; (4) Mysql-connector-java-3.0.9, *library* yang digunakan untuk konektivitas antara java dan MySQL; (5) Blulet *library* merupakan *open source library*. Library ini berfungsi untuk mempermudah pembuatan aplikasi java yang menggunakan *Microsoft*; (6) *BlueCove library,* merupakan *open source library*. Library ini berfungsi untuk menghubungkan java dengan Microsoft. Untuk menggunakan BlueCove, *driver Bluetooth* yang digunakan haruslah driver dari Microsoft. Untuk itu, sistem operasi yang harus digunakan adalah Microsoft Windows XP SP2.; (7) *Parallel port library. Library* ini berfungsi sebagai *tool* untuk mempermudah java membaca dan mengirimkan satu byte data dari dan ke pararel port. Untuk penggunaan *library* harus dilakukan beberapa pengaturan terlebih dahulu; dan (8) RC4Engine dan MD5Digest, merupakan *open source library*. *Library* ini berfungsi untuk melakukan enkripsi RC4 dan Hashing MD5. Pada pembuatan aplikasi Kontrol Kunci *Bluetooh* ini menggunakan enam 6, yaitu *FormRegister, FormAbout, FormEdit, FormUtama, FormHistory*, dan *CekDriver*.

PEMBAHASAN

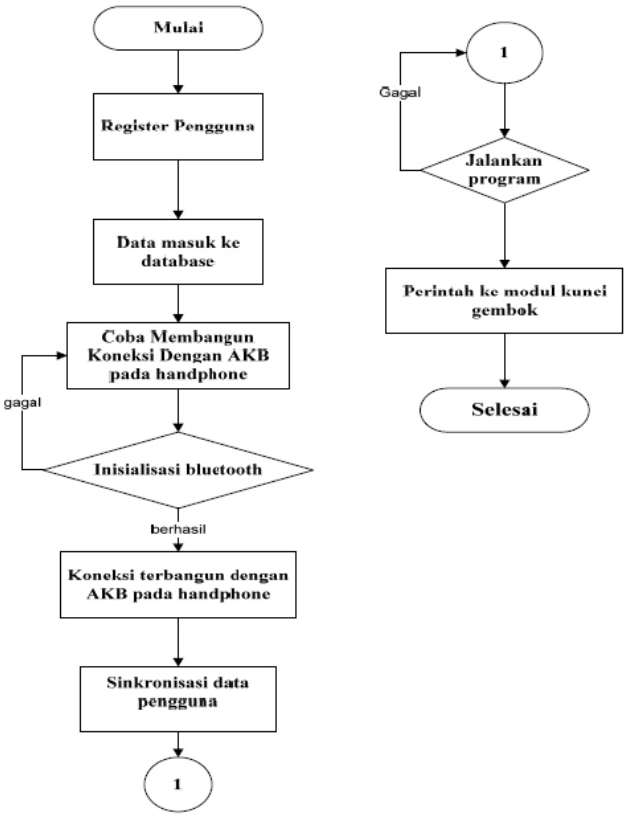
Analisa Data Pengujian

Setelah melakukan pengujian terhadap semua modul-modul program simulasi ini, maka dapat disimpulkan bahwa pengujian telah menunjukkan hasil *output* dan proses yang sesuai dengan rumusan rancangan program simulasi ini. Dari hasil pengujian tersebut, dapat dikatakan bahwa program simulasi telah berfungsi dengan baik dan benar karena

terbukti keseluruhan aplikasi ini telah dapat membuka dan menutup simulasi kunci elektronik pada komputer dengan menggunakan ponsel melalui koneksi *Bluetooth*. Aplikasi ini juga dapat mengontrol hak akses penggunaan kunci dengan melakukan verifikasi dan otentifikasi.

Namun, berdasarkan hasil pengujian secara keseluruhan, didapatkan beberapa keterbatasan dari program simulasi kunci elektronik dengan enkripsi melalui *Bluetooth* pada ponsel ini, antara lain (1) Aplikasi Anak Kunci *Bluetooth* (AKB) hanya dapat diterapkan pada ponsel yang telah mendukung java MIDP 2.0, JSR-82 dan JSR-135; (2) Aplikasi Kontrol Kunci *Bluetooth* (KKB) hanya dapat diterapkan pada komputer dengan sistem operasi minimum Windows XP SP2; (3) Pintu yang bisa dibuka hanya satu dan saling bergantian, artinya pintu yang lain dapat dibuka apabila semua pintu dalam keadaan tertutup.

Gambar 3 menunjukkan tampilan utama menu *history*, yaitu pengujian menjalankan menu *history* untuk menyimpan dan menampilkan semua catatan *history* setiap pengaksesan aplikasi yang terjadi; Gambar 4 menunjukkan tampilan awal untuk mencari *user* yang akan diubah, yaitu pengujian terhadap menu *edit use*; Gambar 5 menunjukkan tampilan saat mengubah data pengguna, yaitu pengujian terhadap menu *edit use*; Gambar 6 menunjukkan tampilan ketika pengubahan berhasil, yaitu pengujian terhadap menu *edit use*; Gambar 7 adalah tampilan menu *about*, yaitu untuk pengujian menjalankan menu *about* pada aplikasi Kontrol Kunci *Bluetooth*; Gambar 8 menunjukkan tampilan menu help dan help.chm, yaitu pengujian terhadap menu *help* pada aplikasi kontrol kunci *bluetooth.*



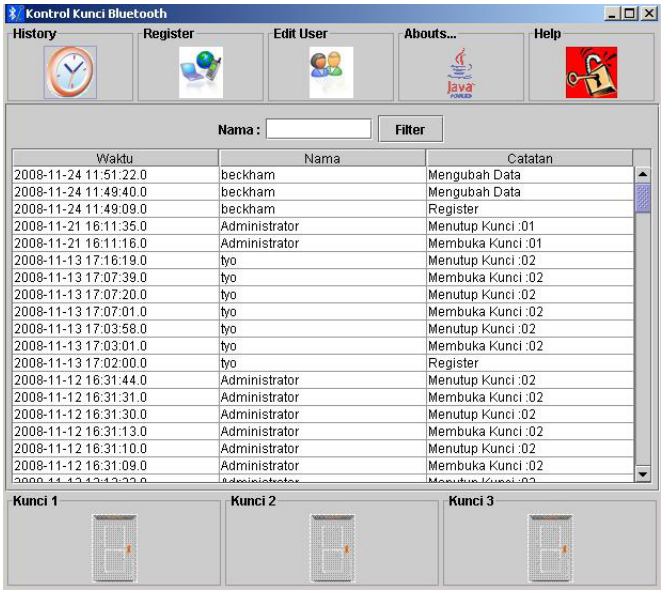
Gambar 2 Diagram Alir Microsoft Kunci *Bluetooth* pada Komputer

Tabel 1 *User* pada Database

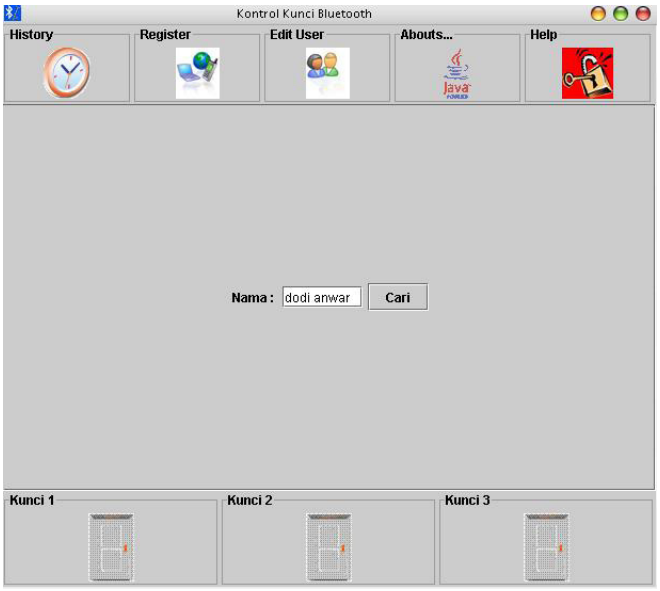
Nama Field	Tipe Data	Ukuran Field	Keterangan
No_BT	Text	24	
Nama	Text	20	Primary Key
No_Seluler	Text	30	
Passowrd	Text	32	
Kunci	Text	3	
Waktu	Text	7	
Status	Text	20	

Tabel 2 *History* pada Database

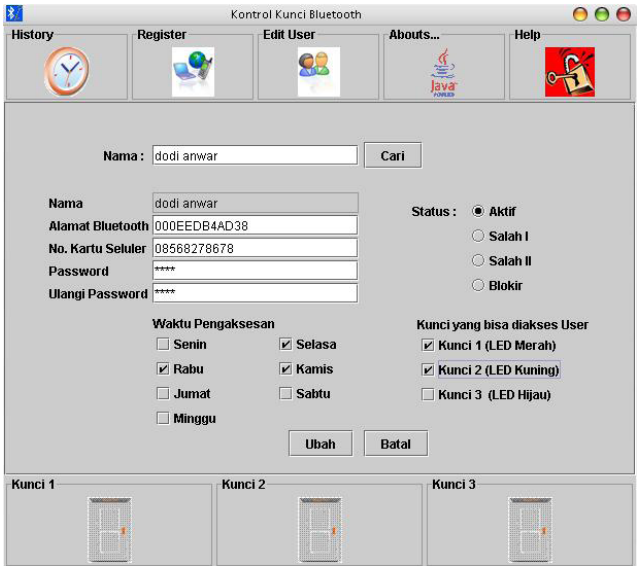
Nama Field	Tipe Data	Ukuran Field	Keterangan
Waktu	DateTime	-	
Nama	Text	20	
History	Text	100	



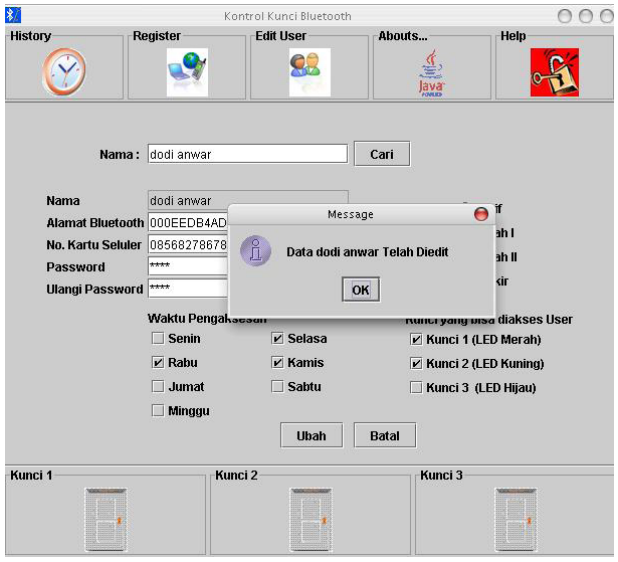
Gambar 3 Tampilan Utama Menu *History*



Gambar 4 Tampilan Awal untuk Mencari *User* yang Akan Diubah

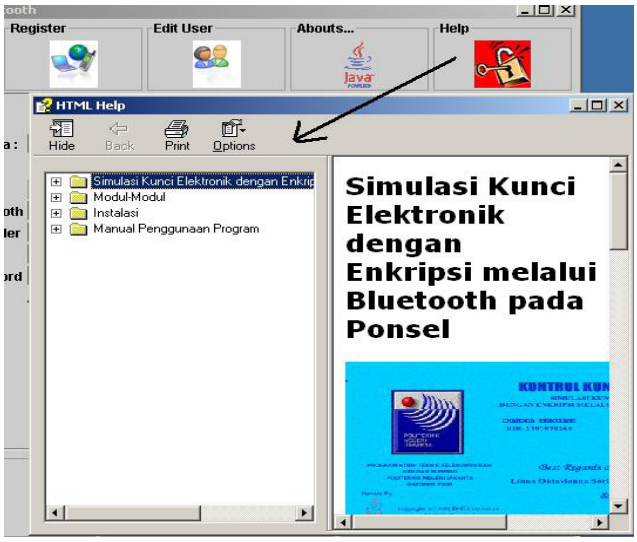


Gambar 5 Tampilan Saat Mengubah Data Pengguna



Gambar 6 Tampilan Ketika Pengubahan Berhasil

Gambar 7 Tampilan Menu *About*



Gambar 8 Tampilan Menu Help dan Help.chm

PENUTUP

Adapun kesimpulan yang diperoleh dari perancangan dan pembuatan program simulasi kunci elektronik dengan enkripsi melalui *bluetooth* pada ponsel, antara lain (1) Program aplikasi Kontrol Kunci *Bluetooth* (KKB) hanya bisa dijalankan pada komputer yang sudah terinstal program kontrol kunci *bluetooth* dan mempunyai *port parallel*; (2) Pengisian alamat *bluetooth* harus 12 karakter; (3) Saat mengulangi *password, password* yang diulang harus sama dengan password yang pertama; (4) Jika data pengguna yang dimasukkan tidak sama dengan yang telah didaftarkan dalam database, maka pengguna tidak dapat membuka pintu dan status pengguna akan secara bertahap berubah menjadi salah satu hingga terblokir jika pengguna salah lebih dari 3 kali; dan (5) Jika telah terblokir, maka untuk dapat mengubahnya menjadi aktif diperlukan administrator yang bisa mengubah status dari pengguna.

DAFTAR PUSTAKA

Benhui. (September, 2008). *Connecting PC and phone with java bluetooth API–part 1*. Retrieved from http://www.benhui.net/modules.php?name=Bluetooth&page=Connect_PC_Phone_Part_1.html.

Gerhmann, C., Persson, J., and Smeets, B. (2004). *Bluetooth security*, Boston: Artech House.

Dasgupta, K. (Agustus, 2008). Protocols in *bluetooth* architecture. http://www.cs.utk.edu/~dasgupta/bluetooth/blueprotocols.html

Haartsen, J. (September, 2008). *Bluetooth baseband*. Retrieved from http://www.palowireless.com/infotooth/tutorial/baseband.asp.

Nokia. (Agustus, 2008). *Bluetooth* technology overview. Retrieved from http://forum.nokia.com.

Portillo, J.G.D.C. (September, 2008). *Parallel printer port access through java*. Retrieved from http://www.geocities.com/Juanga69/parport.

Stallings, W. (2003). *Crytography and network security principles and practices*, 3rd ed., Upper, Saddle River: Prentice.

Sutadi, D. (2002). *I/O bus and motherboard*, Yogyakarta: ANDI.