SISTEM PENGAMANAN PINTU OTOMATIS BERBASIS MIKROKONTROLLER ARDUINO MENGGUNAKAN RADIO FREQUENCY IDENTIFICATION DAN PASSWORD TERENKRIPSI

Haryansyah
Teknik Informatika, STMIK PPKIA Tarakanita Rahmawati
Jl. Yos Sudarso No.8 Tarakan Kalimantan Utara
email: aryabec@live.com

Abstrak *– Radio Frekuensi Identifikasi atau biasa disebut dengan istilah RFID 125 KHz merupakan teknologi yang bekerja berdasarkan frekuensi radio untuk proses pengiriman data. Alat ini terdiri 2 (dua) bagian diantaranya RFID reader yang berfungsi untuk membaca data dan RFID tag yang berfungsi sebagai kartu identifikasi yang nantinya akan dibaca oleh RFID reader.*

Pengamanan pintu pada penelitian ini yaitu dengan memanfaatkan RFID 125 KHz yang terhubung ke mikrokontroler dan bertugas untuk mengendalikan pintu, baik membuka maupun menutup secara otomatis. Akses untuk membuka pintu berdasarkan penggunaan RFID tag yang sebelumnya telah terdaftar pada server disertai dengan password yang harus dimasukkan untuk validasi pengguna. Password yang tersimpan kedalam database juga akan dienkripsi terlebih dahulu.

Untuk dapat berkomunikasi dengan komputer server mikrokontroler terhubung dengan ethernet shield dan tersambung ke komputer menggunakan kabel jaringan. Proses berawal ketika pengguna mendekatkan RFID tag pada jarak tertentu pada RFID reader. Setelah tag terdeteksi selanjutnya pengguna diminta untuk memasukkan password melalui keypad. Apabila password telah dimasukkan selanjutnya, password tersebut akan dienkripsi pada mikrokontroller menggunakan metode Electronic Code Book (ECB) dan dikirimkan ke server bersama dengan nomor tag hasil pembacaan sebelumnya. Validasi nomor tag dan password terenkripsi dilakukan di server dan selanjutnya server mengiriman sinyal untuk membuka pintu apabila nomor tag dan password terdaftar di server. Server juga akan mencatat identitas pengguna yang masuk maupun keluar melalui pintu secara real time.

Kata Kunci: RFID, Microcontroller, Ekripsi, Arduino, Pintu Otomatis

I. PENDAHULUAN

Keamanan sebuah ruangan menjadi hal yang sangat vital untuk beberapa bangunan yang menjadi tempat penyimpanan barang penting atau dianggap berharga. Pengamanan menggunakan kamera CCTV memang menyelesaikan masalah tapi tidak dapat mencegah seseorang untuk mengakses ruang tersebut. Pengamanan yang baik apabila dilakukan mulai pintu masuk ruangan tersebut, namun pengamanan menggunakan kunci juga masih hal biasa dan berkemungkinan untuk dibobol.

Dewasa ini peranan kunci pintu sudah mulai digantikan berbagai alat detektor untuk dapat membuka pintu. Hal ini cukup membantu dalam mengamankan pintu tersebut. Detektor yang dapat digunakan diantaranya adalah Radio Frekuensi Identification (RFID) 125KHz. RFID terdiri dari 2(dua) bagian penting yang tidak dapat dipisahkan yaitu RFID reader dan RFID tag. Pada penelitian ini, selain menggunakan RFID 125KHz, keamanan pintu juga dilengkapi dengan *password* yang terenkripsi yang dilakukan pada mikrontroller maupun pada aplikasi dikomputer server untuk mendaftarkan *password* untuk masing-masing ID tag RFID.

Untuk dapat berkomunikasi dengan komputer server, mikrokontroller terhubung dengan ethernet shield dan tersambung ke komputer menggunakan kabel jaringan. Ethernet shield ini mempunyai fungsi yang sama dengan land card pada komputer yang nantinya akan digunakan untuk pertukaran data antara mikrokontroller dengan komputer server.

Cara kerja alat dimulai dari pendaftaran RFID tag pada aplikasi server yang dikombinasikan dengan password yang terenkripsi untuk memberikan hak kepada pengguna untuk membuka pintu. Selanjutnya setelah RFID tag dan password telah terdaftar, maka pengguna akan mendekatkan RFID tag tersebut pada RFID reader untuk selanjutnya dibaca nomor tag tersebut. Selanjutnya sistem akan meminta inputan *password* kepada pengguna untuk validasi antara nomor *tag* dan *password* yang terdaftar. Password yang dimasukkan melalui keypad shield selanjutnya akan diekripsi pada mikrokontroller dan dikirimkan ke server melalui jaringan bersamaan dengan nomor tag yang telah dibaca sebelumnya.

Pada saat nomor tag dan *password* terenkripsi diterima oleh server, selanjutnya server akan melakukan pengecekan sesuai data yang tersimpan dalam database. Apabila kombinasi nomor

tag RFID dan *password* yang dimasukkan benar dan terdaftar dalam database maka server akan mengirimkan sinyal status valid ke mikrokontroller untuk selanjutnya membuka pintu. Pada saat yang bersamaan, server akan merekam identitas pengguna kedalam database berdasarkan nomor tag yang digunakan pada saat mengakses pintu.

Berdasarkan latar belakang tersebut, maka langkah apa yang dilakukan untuk membuat sebuah rancangan perangkat dengan implementasi RFID 125 KHz untuk pengamanan pintu otomatis, sehingga dengan menggunakan perangkat kunci elektronik tersebut, tingkat keamanan dapat lebih ditingkatkan khususnya untuk pintu yang digunakan pada sebuah ruangan khusus yang tidak diakses secara umum.

Tujuan akhir dari penelitian ini adalah membuat sebuah sistem pengamanan pintu dengan terapan RFID 125 KHz dikombinasikan dengan password terenkripsi menggunakan metode Electronic Code Book (ECB) dengan panjang key 4 bit.

II. LANDASAN TEORI

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita[3]. Ada 4 (empat) tujuan mendasar dari ilmu kriptografi yang juga merupakan aspek keamanan informasi yaitu:

1. Kerahasiaan
   Layanan yang digunakan untuk menjaga isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka atau mengupas informasi yang disandikan.
2. Integritas Data
   Berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak.
3. Autentikasi
   Berhubungan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri.
4. Non-repudiasi
   Usaha untuk mencegah penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan atau yang membuat.

Pada dasarnya kriptografi terdiri dari beberapa komponen, seperti[3]:

1. Enkripsi
   Enkripsi merupakan hal yang sangat penting dalam kriptografi. Enkripsi merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaanya.
2. Dekripsi
   Dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi
3. Kunci
   Kunci merupakan kata sandi yang digunakan untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi 2 (dua) bagian yaitu kunci rahasia (*private key*) dan kunci umum (*public key*)
4. Chipertext
   Chipertext merupakan suatu pesan yang telah melalui proses enkripsi. Pesan yang ada pada teks kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidak mempunyai makna (arti)
5. Plaintext
   Plaintext sering juga disebut dengan *cleartext.* Teks asli atau teks biasa ini merupakan pesan yang ditulis atau diketik ayng memiliki makna (arti). Teks asli inilah yang akan diproses menggunakan algoritma kriptografi untuk menjadi *chipertext* (teks kode).
6. Pesan
   Pesan dapat berupa data atau informasi yang dikirm (melalui kurir, saluran komunikasi data dan sebagainya) atau yang disimpan didalam media perekaman (kertas, storage dan sebagainya)
7. Cryptanalysis
   Cryptanalysis bisa diartikan sebagai analisis kode atau suatu ilmu untuk mendapatkan teks asli tanpa harus mengetahui kunci yang sah secara wajar. Jika suatu teks kode berhasil diubah menjadi teks asli tanpa menggunakan kunci yang sah, proses tersebut dinamakan *breaking code*.

Dalam kriptografi terdapat istilah algoritma sandi yaitu algoritma yang berfungsi untuk melakukan[3]:

1. *Confusion* (konfusi atau pembingungan) dari teks terang sehingga sulit untuk direkonstruksikan secara langsung tanpa menggunakan algoritma deskripsinya.
2. Difusion (difusi atau peleburan) dari teks terang sehingga karakteristik dari teks terang tersebut hilang.

Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara 2 (dua) himpunan yaitu yang berisi elemen teks terang (plaintext) dan yang berisi elemen teks sandi (chipertext)[3].

Enkripsi:

$$E(P) = C \quad \text{..... (1)}$$

Dekripsi:

$$D(C) = P \quad \text{..... (2)}$$

Keterangan:
E = Encrypt (Enkripsi)
P = Plaintext (Teks asli)
C = Chipertext (Teks sandi)
D = Decrypt (Dekripsi)

Secara umum berdasarkan kesamaan kuncinya , algoritma sandi dibedakan menjadi[3]:

1. Symetric Key (Kunci Simestris)
   Umumnya disebut juga algoritma sandi konvensional karena umumnya diterapkan pada

algoritma sandi klasik. Kunci yang digunakan pada saat proses enkripsi adalah sama dengan password yang digunakan pada proses dekripsi

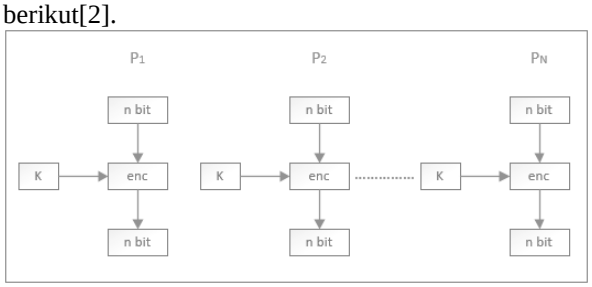
2. Asymetric Key (Kunci Asimetris)
   Umumnya disebut sebagai algoritma sandi modern. Kunci yang digunakan pada saat proses enkripsi berbeda dengan sandi yang digunakan pada proses dekripsi.

Pada penelitian ini, akan menggunakan algoritma sandi *symetric key* yaitu menggunakan metode *Electronic Code Book* (ECB). Selain metode ECB ini, operasi sandi simetris yang lain diantaranya *Chiper Block Chaining* (CBC), *Chiper Feedback, Output Feedback)*

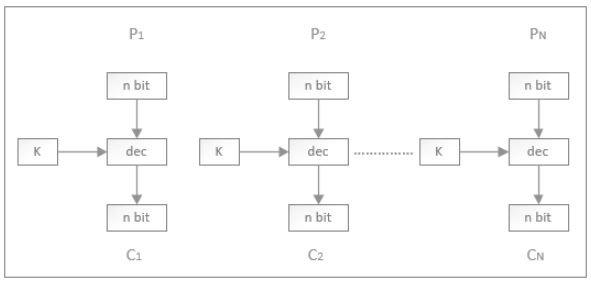
2.1. Electronic Code Book

Mode operasi Electronic Code Book (ECB) merupakan mode yang paling sederhana. ECB beroperasi dengan memecah teks asli berukuran *N x n* bit menjadi *N* blok dengan tiap blok berukuran *n* bit (sesuai dengan ukuran blok sistem penyandian), kemudian tiap blok disandi dengan kunci, dan algoritma enkripsi yang sama.

Untuk proses dekripsi dilakukan hal yang sama hanya saja menggunakan algoritma dekripsi. Model ECB untuk proses enkripsi dan dekripsi diilustrasikan dengan gambar 1 dan gambar 2 berikut[2].



Gambar 1. Model Enkripsi



Gambar 2. Model Dekripsi

Pada metode ECB ini, suatu blok kode yang panjang dibagi dalam bentuk urutan binari menjadi satu blok tanpa mempengaruhi blok-blok yang lain. Satu blok terdiri dari 64 bit atau 128 bit[3].

Secara matematis, enkripsi dengan metode ECB dinyatakan dengan persamaan berikut[3]:

$Ci = Ek(Pi)$ ..... (3)

dan dekripsi sebagai berikut[3]:

$Pi = Dk(Ci)$ ..... (4)

Keterangan :
C_i = teks kode ke-i
P_i = Teks asli ke-i
E_k = Enkripsi dengan key
D_k = Dekripsi dengan key

Contoh kasus implementasi metode ECB:

Diketahui teks asli (dalam biner) adalah:
10100010001110101001

Teks asli dibagi menjadi blok-blok yang berukuran 4 bit:
1010 0010 0011 1010 1001

Atau dalam notasi HEX adalah A23A9

Misalkan kunci (K) yang digunakan adalah (panjangnya juga 4 bit):
1011

Atau dalam notasi HEX adalah B

Misalkan fungsi enkripsi *E* yang sederhana dengan meng-XOR-kan blok teks asli P_i dengan *K*, kemudian geser secara *wrapping* bit-bit dari $P_i + K$ satu posisi ke kiri.

Proses enkripsi untuk setiap blok digambarkan sebagai berikut:

	1010	0010	0011	1010	1001
	1011	1011	1011	1011	1011
Hasil XOR:	0001	1001	1000	0001	0010

Geser 1 bit ke kiri: 0010 0011 0000 0010 0100
dalam notasi HEX: 2 3 0 2 4

Jadi hasil enkripsi teks asli menjadi:
00100011000100100100 (23024 dalam notasi HEX)

2.2. Perangkat Pendukung

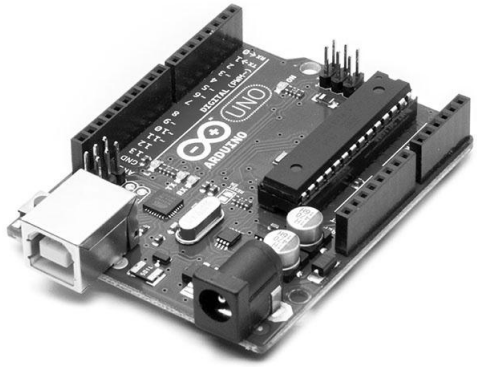
Beberapa perangkat yang digunakan pada penelitian ini sebagai bahan simulasi untuk implementasi metode diantaranya:

2.2.1 Mikrokontroller Arduino Uno R3

Arduino Uno merupakan *board* mikrokontroller berbasis ATmega 328. Arduino Uno mempunyai 14 pin *input* atau *output* digital, 6 (enam) diantaranya bisa digunakan sebagai *output* PWM (Pulse Widt Modulation), 6 (enam) analog *input*, 16 MHz ceramic resonator, stronger reset circuit[4].

Mikrokontroller inilah yang akan mengendalikan perangkat pintu otomatis termasuk perangkat pendukung yang lain. Perangkat ini akan mengendalikan seluruh perangkat berdasarkan perintah yang dimasukkan kedalam chip ATmega 328 yang dibuat dalam bentuk kode program. Arduino Uno R3 dapat diamati pada gambar 3

berikut.

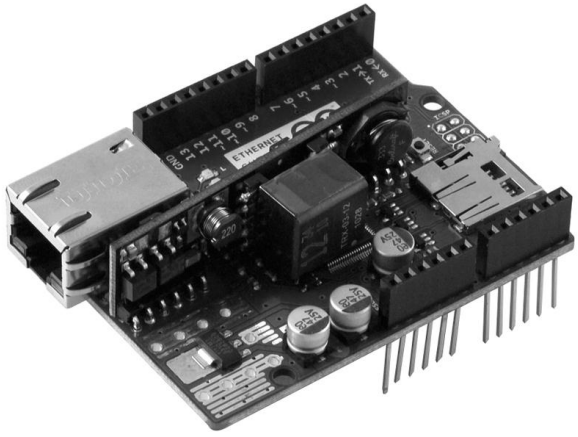


Gambar 3. Arduino Uno R3

2.2.2 Arduino Ethernet Shield

Arduino ethernet shield memungkinkan perangkat board Arduino untuk dapat terkoneksi dengan internet menggunakan *ethernet library* dan sekaligus untuk membaca dan menulis pada SD Card menggunakan *SD library*[5].

Pada penelitian ini Arduino Ethernet Shield digunakan untuk menghubungkan mikrokontroller dengan komputer melalui jaringan kabel sehingga dapat bertukar informasi atau data. melalui perangkat inilah, identitas kartu RFID yang dibaca oleh RFID *reader* dikirimkan ke server untuk diolah lebih lanjut. Gambar 4 adalah bentuk ethernet shield yang digunakan pada penelitian ini.



Gambar 4. Arduino Ethernet Shield

2.2.3 RFID Reader dan RFID Tag 125KHz

RFID reader 125 KHz didesain untuk membaca kode yang terdapat dalam kartu RFID dengan frekuensi yang sama. Jarak maksimal pembacaan kartu RFID dari RFID reader maksimum 150mm. Hasil pembacaan kode nantinya akan dikirimkan ke server bersamaan dengan *password* yang diinputkan melalui keypad shield dengan melalui proses enkripsi sebelumnya. Wujud RFID reader yang digunakan dapat diamati pada gambar 5.

Gambar 5. RFID Reader

Modul RFID reader tidak akan dapat berjalan sendiri tanpa adanya *tag* RFID. Tag ini berfungsi sebagai kartu identitas pengguna yang digunakan untuk dapat mengakses pintu yang ada. Tag ini berisi kode yang unik yang berbeda antara satu kartu dengan kartu yang lain. Kode inilah yang nantinya akan dibaca menggunakan RFID reader. Jenis tag RFID yang digunakan dapat diamati pada gambar 6.

Gambar 6. RFID Tag

2.2.4 Keypad Shield

Keypad yang digunakan pada penelitian ini berfungsi untuk memasukkan password setelah RFID reader membaca kode dari *tag* yang ada. Password yang diinputkan oleh user nantinya akan dienkripsi pada mikrokontroller sebelum dikirimkan ke server untuk validasi. Keypad yang digunakan merupakan keypad matriks 3 x 4 yang terdiri dari angka dan karakter * serta karakter #. Keypad shield yang digunakan dapat diamati pada gambar 7.

Gambar 7. Keypad Shield

2.2.5 Motor DC 12 volt

Motor DC (Direct Current) seperti tampak pada gambar 8 disini digunakan sebagai penggerak pintu simulasi yang ada. Supply power yang digunakan sebesar 12 volt untuk dapat menggerakkan motor DC ini.

Gambar 8. Motor DC 12 Volt

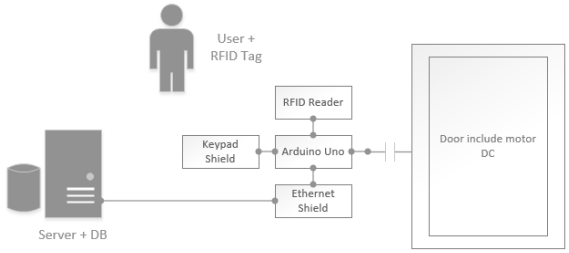
2.2.6 Kabel Jaringan UTP

Kabel jaringan yang digunakan adalah jenis *Unshielded Twisted Pair* (UTP) untuk menghubungkan mikrokontroller dengan komputer server agar dapat melakukan transaksi data. Data yang dikirim melalui kabel jaringan ini adalah data *username* dan *password* terenkripsi yang dihasilkan dari pembacaan kode tag RFID dan inputan *password* yang dilakukan melalui keypad shield. Gambar 9 adalah jenis kabel jaringan yang digunakan.

Gambar 9. Kabel UTP

III. PEMBAHASAN

Pada penelitian ini terdiri tahapan proses untuk mendapatkan hasil yang diinginkan. Secara umum skema tentang cara kerja perangkat digambarkan pada gambar 10 berikut.



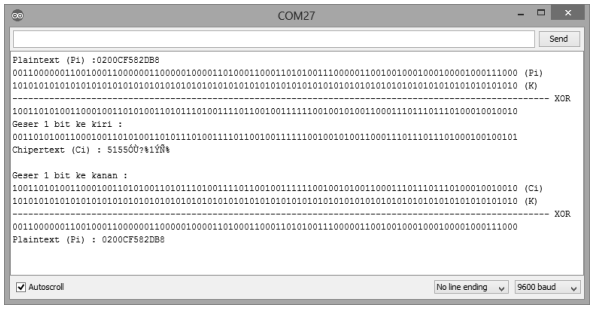
Gambar 10. Struktur Perangkat

Cara kerja alat, terlebih dahulu pengguna mendekatkan tag RFID yang dimiliki ke RFID reader yang ada. Kode yang dibaca oleh RFID reader yang berasal dari tag RFID yang digunakan kemudian akan menjadi *username*. *Password* diperoleh dari hasil inputan keypad shield setelah kode dari tag tersebut terbaca. *Username* dan *password* ini akan dienkripsi oleh mikrokontroller dan selanjutnya dikirmkan hasil enkripsi tersebut ke server untuk dilakukan pengecekan apakah *username* dan *password* tersebut terdaftar sebagai pengguna yang sah atau tidak.

Langkah selanjutnya adalah apabila data yang dikirim dari mikrokontroller telah diterima oleh server, selanjutnya akan dilakukan pencarian data tentang identitas pengguna apakah terdaftar atau tidak sebagai pengguna yang sah. Apabila pengguna terdaftar sebagai pengguna yang sah berdasarkan identitas kartu dan *password* yang dimasukkan, maka server akan mengirimkan data terenkripsi ke mikrokontroller berupa perintah untuk membuka pintu, pada saat yang bersamaan identitas pengguna tersebut akan direkam kedalam database sebagai *log* pengguna untuk keperluan analisa selanjutnya apabila diperlukan.

3.1 Implementasi Metode ECB

Berikut hasil implementasi metode ECB pada proses enkripsi kode yang dibaca pada kartu (tag) RFID, sekaligus proses dekripsi sehingga kode yang dienkripsi kembali ke teks asli semula. Hasil enkripsi ditampilkan menggunakan serial terminal software Arduino dan dapat diamati pada gambar 11.



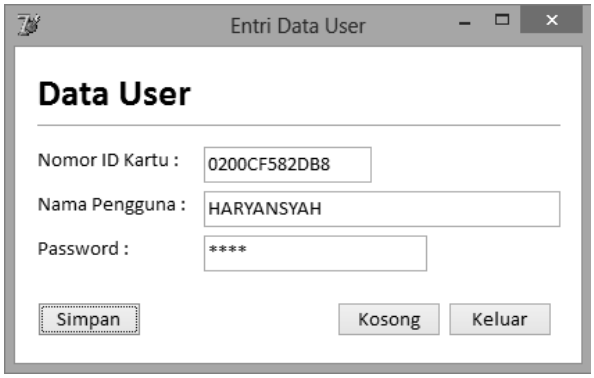
Gambar 11. Enkripsi Metode ECB

Pada gambar ? terlihat proses enkripsi dengan ID kartu 0200CF582DB8 dan setelah melalui proses enkripsi menggunakan metode ECB menghasilkan *chipertext* 5155ÓÙ?%1ÝÑ%. Begitu pula setelah mengalami proses dekripsi maka *chipertext* tersebut kembali ke teks asli atau *plaintext* semula.

Untuk *password* yang diinputkan nantinya juga akan diproses sama seperti enkripsi dan dekripsi ID kartu. Hasil enkripsi yang dihasilkan inilah nantinya akan dikirim ke server melalui kabel jaringan untuk divalidasi apakah terdaftar atau tidak untuk memberikan hak akses pintu yang ada.

Untuk dapat mengakses pintu, pengguna terlebih dahulu harus memeiliki kartu yang telah didaftarkan sebelumnya di komputer server. Pada komputer server terdapat aplikasi untuk menambahkan ID kartu untuk pengguna baru. Terdapat 3 (tiga) field penting yang dibutuhkan diantaranya nomor ID kartu (tag) yang dihasilkan dari pembacaan otomatis melalui RFID reader, nama pengguna dan *password* yang akan digunakan nantinya. Tampilan dapat diamati pada

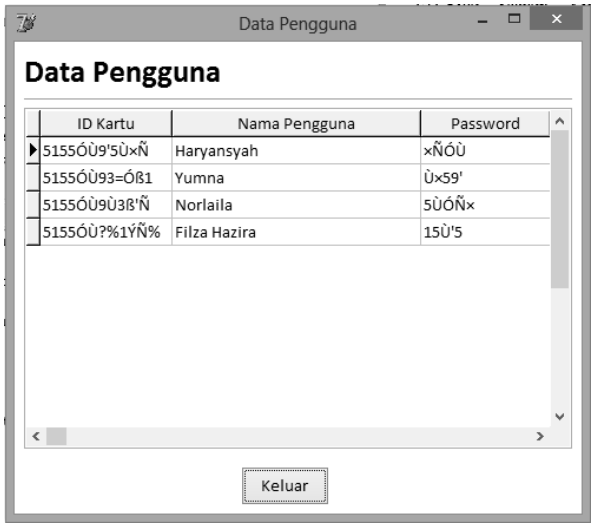
gambar 12 berikut.



Gambar 12. Entri Data User

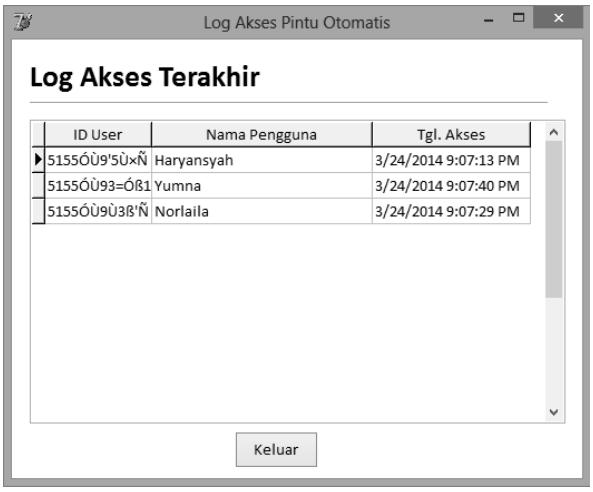
Data *user* yang diinputkan khusus untuk nomor ID kartu dan *password* pada form entri data user terlebih dahulu akan di enkripsi sebelum tersimpan kedalam database. Hal ini bertujuan agar tidak kerahasiaan data pengguna juga tetap terjaga terutama nomor ID Kartu dan *password*.

Data pengguna yang telah dienkripsi dan tersimpan dalam database dapat diamati melalui hasil pada gambar 13 berikut.



Gambar 13. Data User

Setiap pengguna yang mengakses (melewati) pintu akan secara otomatis tersimpan dalam database. Data akan disimpan dalam tabel log. Apabila terjadi sesuatu yang tidak diinginkan, maka data yang tersimpan dalam tabel log ini dapat dianalisa lebih lanjut. Data yang tersimpan pada tabel ini juga dienkripsi guna menjaga kerahasiaan data terutama ID kartu yang digunakan. Tampilan data pengguna yang mengakses pintu dapat diamati pada gambar 14 berikut.



Gambar 14. Log Akses Pintu

IV. KESIMPULAN

Keamanan pintu menggunakan kamera CCTV tidak dapat mencegah akses ke sebuah ruang dengan melewati sebuah pintu. Sistem keamanan pintu yang diterapkan pada penelitian ini selain berbasis Radio Frequency Identification (RFID) juga dilengkapi dengan *password* terenkripsi menggunakan metode Electronic Code Book (ECB) sehingga data pengguna dapat terjaga kerahasiannya. Setiap pengguna yang mengakses pintu akan terekam kedalam database sehingga data yang tersimpan dapat dianalisa lebih lanjut apabila diperlukan.

DAFTAR REFERENSI

[1] Dony Ariyus, Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi, Yogyakarta:Andi, 2008.

[2] Rifki Sadikin, Kriptografi untuk Keamanan Jaringan, Yogyakarta:Andi, 2012.

[3] Admin, "Kriptografi", wikipedia, [Online]. Tersedia: http://id.wikipedia.org/wiki/Kriptografi [Diakses 20 Maret 2014]

[4] Admin, "Arduino Uno", Arduino, [Online]. Tersedia: http://arduino.cc/en/Main/arduinoBoardUno [Diakses 20 Maret 2014]

[5] Admin, "Arduino Ethernet Shield", Arduino, [Online]. Tersedia: http://arduino.cc/en/Guide/ArduinoEthernetShield [Diakses 20 Maret 2014]

Biodata Penulis

Haryansyah, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika STMIK PPKIA Tarakanita Rahmawati, lulus tahun 2011. Saat ini sedang menempuh pendidikan Pasca Sarjana di Institut Sains Terapan Teknologi Surabaya (iSTTS). Saat ini menjadi Dosen di STMIK PPKIA Tarakanita Rahmawati