Smart Gate System untuk Akses Kontrol Keamanan Kampus

Smart Gate System for Acces of Campus Security *Control*

KHAIRUNNISA MANSUR

P2700215017

PROGRAM PASCASARJANA

UNIVERSITAS HASANUDDIN

MAKASSAR

2017

Smart Gate System untuk Akses Kontrol Keamanan Kampus

Tesis

Sebagai Salah Satu Syarat untuk Mencapai Gelar Master

Program Studi

Teknik Elektro

Kepada

SEKOLAH PASCASARJANA

UNIVERSITAS HASANUDDIN

MAKASSAR

2017

TESIS

***SMART GATE SYSTEM* UNTUK AKSES KONTROL KEAMANAN KAMPUS**

Disusun dan diajukan oleh

KHAIRUNNISA MANSUR
Nomor Pokok P2700215017

telah dipertahankan di depan Panitia Ujian Tesis
pada tanggal 28 September 2017
dan dinyatakan telah memenuhi syarat

Menyetujui
Komisi Penasehat,

Dr. Ir. Zulfajri B. Hasanuddin, M.Eng	**Dr. Eng. Wardi, S.T, M. Eng.**
Ketua	Anggota

Ketua Program Studi Teknik Elektro,	Dekan Fakultas Teknik Universitas Hasanuddin,
Dr. Ir. Zahir Zainuddin, M.Sc.	**Dr-Ing. Ir. Wahyu H. Piarah, MSME.**

PERNYATAAN KEASLIAN TESIS

Yang bertanda tangan di bawah ini :

Nama	: Khairunnisa Mansur
Nomor Mahasiswa	: P02700215017
Program Studi	: Teknik Elektro
Konsentrasi	: Telekomunikasi

Menyatakan dengan sebenarnya bahwa tesis yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilalian tulisan atau pemikiran orang lain. Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan tesis ini hasil karya orang lain, saya, bersedia menerima sanksi atas perbuatan tersebut.

Makassar, Oktober 2017

Yang Menyatakan

Khairunnisa Mansur

ABSTRAK

KHAIRUNNISA MANSUR. *Smart Gate System untuk Akses Kontrol Keamanan Kampus* (dibimbing oleh Zulfajri Basri Hasanuddin dan Wardi).

Penelitian ini bertujuan mengembangkan *smart gate system* sebagai akses kontrol keamanan dalam lingkungan kampus Fakultas Teknik Universitas Hasanuddin. Kartu NFC *smart card* digunakan sebagai identifikasi civitas akademik sebagai pengguna untuk proses otentikasi.

Penelitian terbagi atas dua perancangan, yakni perancangan *website* dan perancangan sistem *prototype smart gate*. Perancangan *website* dioperasikan oleh pengguna untuk mengisi *form* biodata dan administrator dalam melakukan registrasi kartu. Pada *smart card* ditulis *key* otentikasi dan informasi biodata pengguna yang telah dienkripsi. Perancangan sistem menggunakan pembaca *NFC PN532 NFC RFID module, mikrokontroller, NFC tag, sensor PING, motor servo, router*, dan *enthemet shield*. Identifikasi dilakukan pada *smart card* sekaligus kartu identitas. Pengguna yang ingin memasuki area kampus harus melewati *gate* dan melakukan proses identifikasi pada pembaca UID dan memasukkan kode tertentu ke dalam *smart card*. *Smart card* yang terdaftar akan membuka *gate*. Gerbang penghalang akan tertutup setelah pengguna melewati sensor. Riwayat akses akan ter-*update* pada server *database* melalui *local area nework* (*LAN*).

Hasil penelitian menunjukkan respon sistem dapat bekerja hingga jarak optimum 6 cm dengan respon sistem terhadap waktu pada jarak optimum 1.829 detik. Keamanan data dalam *smart card* dijaga enkripsi pada data informasi pengguna dan kunci otentikasi. *Website* dapat dioperasikan oleh administrator untuk registrasi pengguna dan monitoring pada riwayat akses masuk atau keluar kampus melalui *gate system*. Pengawasan keamanan akses kontrol dalam lingkungan kampus dapat dikontrol melalui *website*.

Kata kunci: akses kontrol, *smart gate*, *smart card*, kartu NFC, NFC PN 532

ABSTRACT

KHAIRUNNISA MANSUR. *Smart Gate System for Access of Campus Security Control* (*supervised* by **Zulfajri Basri Hasanuddin** and **Wardi**)

This research aims to develop a smart gate system as access of security control in campus environment in Engineering Faculty of Hasanuddin University. NFS smart card is used as the identification of the academicians as the user for the authentication process.

The research was divided into two designs, i.e. website design and design of smart gate prototype system. The design of the website run by the user to fill the biodata form and administrator to register the card. The authentication key and user information data that has been encrypted was written on the card. System design used NFC reader PN532 NFC RFID module, microcontoller, NFC tag, PING sensor, servo motor, router, and ethernet shield. Users who wish to visit the campus area must pass through the gate and perform the identification process on the smart card reader. The process of identification and authentication by reading smart card. Smart card that can be opened gate. The barrier gate is closed after the used passes the sensor. Open access will be updated on the server database via Local Area Nework (LAN).

The results show that the system response can work for the optimum distance of 6 cm with the system response to time at the optimum distance of 1828 seconds. The security data in the smart card is maintained encryption on user information data and authentication keys. Websites can be operated by administrators for user registration and monitor the access history of in and out of campus through the gate system. Control of access control security within the campus environment can be controlled through the website.

Keywords: access control, smart gate, smart card, NFC card, NFC PN 532.

KATA PENGANTAR

Puji dan syukur kehadirat Allah SWT atas Rahmat dan Karunia-Nya sehingga penulis dapat menyelesaikan tesis yang berjudul "*Smart Gate System* untuk Akses Kontrol Keamanan Kampus".

Tesis ini disusun guna memperoleh gelar Master Teknik pada Program Pascasarjana Teknik Elektro Universitas Hasanuddin Makassar. Melalui kesempatan yang sangat berharga ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu dalam penyelesaian Tesis ini, terutama kepada yang terkasih:

1. Keluarga, suami Farid Nahrir, Ayah Mansur Mangasing, Ibu ST.Syamsurida Akib, Bapak Mertua Nahrir Hamzah, Ibu Mertua Fatmawati, yang tak henti-hentinya memberikan semangat, tak lupa saudaraku Nurfauziah Mansur, Husnul Khatimah Mansur, Moh. Arief Mansur dan Nurul Amalia.
2. Bapak Dr. Ir. Zulfajri Basri Hasanuddin, M.Eng dan Ibu Dr. Eng. Wardi, S.,T., M. Eng. selaku Pembimbing I dan Pembimbing II atas kesabarannya memberikan bimbingan, bantuan dan arahan selama litian.

an-teman Teknik Elektro angkatan 2015 secara khusus kepada ka yang dekat dihati untuk semangat dan inspirasi.

4. Seluruh pihak yang telah membantu dalam penyelesaian Tesis ini dan tidak dapat disebutkan satu-persatu, terima kasih atas segala kebaikan kalian.

Penulis menyadari bahwa Tesis ini masih memiliki banyak kekurangan dan jauh dari kesempurnaan. Untuk itu melalui kata pengantar ini penulis sangat terbuka menerima kritik serta saran yang membangun sehingga secara bertahap penulis akan dapat memperbaikinya.

Namun demikian penulis sangat berharap kiranya Tesis ini dapat memberikan manfaat dan kontribusi yang besar untuk kepentingan bersama.

Makassar, Oktober 2017

Penulis

DAFTAR ISI

Halaman

DAFTAR TABEL

Nomor **Halaman**

DAFTAR GAMBAR

Nomor **Halaman**

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

A. Latar Belakang

Kebutuhan sistem keamanan diperlukan dalam berbagai aspek, salah satunya sistem keamanan akses kontrol di lingkungan kampus dengan *gate system.* Saat ini, *gate system* membutuhkan lebih banyak data identitas untuk mengidentifikasi kendaraan bermotor atau orang yang masuk ke dalam lingkungan terbatas. Kartu identitas atau *identification card* menjadi pendukung utama dalam *gate system* (Gardeman, 2015).

Smart Card memiliki kemampuan untuk menyimpan data identitas serta dapat diprogram pada sisi aplikasinya yang dapat digunakan untuk proses otentifikasi. *Radio Frequency Identification* merupakan teknologi untuk mengidentifikasi objek atau seseorang dengan menggunakan transmisi frekuensi radio pada 125 KHz, 13.6 MHz, atau 800-900MHz. Pengembangan dari teknologi RFID adalah NFC (*Near Field Communication*) bekerja pada frekuensi 13.56 MHz yang dapat digunakan pada aplikasi transportasi, identifikasi, dan *payment.* NFC dapat diintgrasikan pada sistem akses kontrol, *check-in* kontrol dan alarm keamanan. Teknologi NFC memenuhi standar komunikasi internasional miliki potensi untuk menjadi teknologi yang sangat kompetitif pada koneksi nirkabel jarak pendek (Wenxing, 2015).

Akses kontrol sistem secara sederhana didefenisikan sebagai teknik yang digunakan untuk mengendalikan perjalanan masuk atau keluar dari area seperti area perumahan, kantor dan lain-lain (Teh dkk, 2014). Akses kontrol adalah salah satu aplikasi kartu pintar yang paling banyak digunakan di kampus universitas. Manajemen akses control smart card di kampus universitas bertanggung jawab atas pengelolaan akses kontrol (Du dkk, 2015). Dalam lingkunagn kampus Fakultas Teknik Universitas Hasanuddin saat ini masih menggunakan sistem buka tutup *gate* oleh pihak keamanan kampus. Belum adanya proses identifikasi melalui kartu identitas memudahkan siapa saja dapat masuk kedalam lingkungan kampus. Pada penelitian ini *smart gate* dapat menjadi solusi untuk sistem keamanan akses kontrol.

Sistem akses kontrol berdasarkan RFID telah dikembangkan baik menggunakan *smart card* dan *smart phone*. Penelitian Kao Liu dan Huang Yang (2008), mengembangkan aplikasi system *computer client-end* dengan memanfaatkan kartu IC *contactless* dan reader berdasarkan RFID untuk pengendalian gerbang / *gate* kampus dengan proses identifikasi yang dibangun melalui *server-end* database dan Local Area Network (LAN) kampus. Proses pengiriman informasi antara *client* dan computer *server-end* menggunakan fungsi Hash satu arah untuk membangkitkan *message digest* (nilai yang juga dikenal sebagai kriptografi atau secure hash) juga opsi Advanced Encryption Standart untuk memperkuat proteksi rmasi pribadi dan secara keseluruhan keamanan sistem. Penelitian

Rosa Ma. *Et al.,* (2016) kontrol akses dengan sistem RFID untuk menentukan atau memberlakukan control akses dan pembatasan di area utama bangunan universitas yang seharusnya hanya bisa diakses oleh sekelompok kecil staf. Mekanisme akses kontrol dilakukan dengan mengevaluasi permintaan akses pada database. Permintaan yang memiliki otorisasi akan diizinkan dan ditolak apabila tidak memiliki otorisasi pada database. Topik penelitian akses control dalam lingungan kampus ini tetap potensial untuk dikembangkan karena masing-masing kampus ingin mengembangkan sistem sendiri, dan juga memiliki inovasi yang berbeda.

(Bouazzouni *et al.,*2016) mengajukan sebuah arsitektur untuk membangun sistem akses kontrol yang aman berbasis Trusted Execution Environtmen (TEE) dan Identity Based Encryption (IBE). TEE adalah kombinasi dari sebuah perangkat keras dan perangkat lunak dimana eksekusi sistemnya terbagi dalam dua lingkungan. Lingkungan pertama adalah Rich Execution Environtment (REE) atau Normal World Execution Environtment yang merupakan standar Operating System dari *smart phone* Android. Otentikasi dilakukan berdasarkan IBE dan TEE yang dipresentasikan dalam OP-TEE. Gruntz *et al.,*(2016) mengembangkan *smart phone* yang berdasarkan sistem akses kontrol secara fisik dimana akses poin tidak secara langsung terhubung ke sever pusat, tetapi lebih menggunakan konektivitas dari *smart phone* untuk dapat mengakses ...an akses online dari pengguna dengan menggunakan server ...usat. Otentikasi dari *smart phone* berdasar pada kunci kriptografi

publik. Hal tersebut membutuhkan kunci pribadi disimpan dalam suatu sistem pengamanan atau dalam TEE untuk menghindari pencurian identitas. Kedua penelitian ini memanfaatkan *smart phone* yang dilengkapi NFC untuk melakukan akses, sehingga apabila diterapkan dalam system akses kontrol setiap *user* atau pengguna diwajibkan memiliki *smart phone* yang dilengkapi NFC. Sebagai solusi dalam penelitian yang penulis ajukan dibutuhkan *smart card* NFC sebagai pengganti *smart phone.*

Sebagian besar sistem akses kontrol berbasis RFID rentan pada resiko serangan yang memungkinkan kloning dari tag / kartu untuk mendapatkan akses ke fasilitas akses control. Solusi untuk mengatasi resiko tersebut adalah dengan meningkatkan keamanan pada verifikasi dan otentikasi user. Penelitian Jacob *et al.,* (2015) menerapkan One-Time Password pada system kehadiran menggunakan NFC. One-Time Password dibuat secara otomatis dengan membangkitkan string karakter numerik atau alfanumerik pada otentikasi *user* untuk satu kali sesi transaksi menggunkan NFC *card.* Keamanan otentikasi dalam penelitian oleh penulis dilakukan dengan enkripsi metode Caesar Chiper dan Rotate Letter pada proses registrasi kartu untuk menjaga kerahasiaan data pribadi civitas akademik serta memasukkan *key in* dan *key out* pada *tag* / kartu.

Penelitian ini melakukan pengembangan perancangan penggunaan NFC *card* pada prototipe akses kontrol *gate system* dalam lingkungan Fakultas Teknik Universitas Hasanuddin. Akses keluar masuk cademika sebagai *user* dapat dikontrol melalui *gate system*. Kartu

identitas berupa NFC *card* berisi informasi biodata civitas akademika untuk proses identifikasi dan otentikasi. NFC card yang telah teregistrasi akan melakukan proses buka tutup *gate.* Sistem ini juga dilengkapi dengan website yang dioperasikan oleh administrator untuk mendaftarkan pengguna baru, mengedit identitas pengguna, memeriksa riwayat akses masuk atau keluar kampus.

Dengan adanya *smart gate syste*m dan *security building* menggunakan *smart card* yang diaplikasikan di Kampus Teknik Universitas Hasanuddin Gowa keamanan akses kontrol mahasiswa dan staf melalui kendaraan dan pintu dapat diproteksi. Kendaraan atau orang yang masuk harus melalui smart *gate system* untuk proses registrasi. Penelitian ini dilakukan untuk mendukung perwujudan *smart campus* sehingga dirancang dalam lingkup civitas akademika. Pada penelitian lebih lanjut pengguna kartu dapat menikmati berbagai fungsi lain dalam satu kartu yang sama.

B. Rumusan Masalah

Berdasarkan latar belakang maka rumusan masalah pada penelitian ini adalah:

1. Bagaimana kinerja penggunaan *smart card* sebagai kartu identitas pada *gate system* dan *security building*?
2. Bagaimana merancang website untuk otoritas akses kontrol?
3. Bagaimana merancanng *smart gate system* menggunakan mikrokontroller Arduino?

C. Tujuan Penelitian

Tujuan penelitian berdasarkan rumusan masalah yang telah dijabarkan antara lain:

1. Mengetahui kinerja implementasi dari penggunaan *smart card* sebagai kartu identitas untuk proses otentifikasi pada *gate system* dan security building.
2. Untuk merancang website bagi otoritas akses kontrol.
3. Merancanng *smart gate system* Mikrokontroller Arduino
4. Untuk manajemen proteksi akses kontrol civitas akademik yang masuk ke dalam lingkungan kampus.

D. Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dari penelitian *Smart Gate System* dan *security building* adalah:

1. Masyarakat, bermanfaat memberikan fasilitas teknologi berupa *smart gate system* dan *security building* yang dapat digunakan untuk proteksi keamanan lingkungan.
2. Bagi peneliti, peneliti ini berguna untuk menambah pengetahuan dan kemampuan/*skill* pada proses pembuatan aplikasi *smart card* pada *gate system* dan *security building*.

3. Bagi institusi pendidikan Magister Jurusan Teknik Elektro dapat digunakan sebagai referensi ilmiah dalam penelitian untuk pengembangan sistem akses kontrol

E.Batasan Masalah

Adapun batasan masalah penelitian ini antara lain:

Adapun batasan masalah pada penelitian ini, antara lain :

1. Penelitian dilakukan di kampus Universitas Hasanuddin Fakultas Teknik Gowa.
2. Sistem prototipe menggunakan PN532 NFC RFID module, sensor PING, dan ethernet shield.
3. Jenis kartu NFC *contactless* yang digunakan adalah Mifare Classic 1K.
4. Menggunakan http://localhost/gate/registrasi.php sebagai *hosting* yang dioperasikan pada sistem operasi windows.
5. Menggunakan *stopwatch* untuk perhitungan delay.
6. Pengambilan data dilakukan pada 10 sampel *smart card.*
7. Pengambilan data hanya dilakukan pada *smart card* yang memiliki akses di Kampus Fakultas Teknik Universitas Hasanuddin Gowa dan telah terdaftar pada *database.*

F.Sistematika Penulisan

Sistematika penulisan pada penelitian ini diuraikan sebagai berikut:

Bab I Pendahuluan

Bab I menjelaskan mengenai latar belakang masalah yang menjabarkan alasan dilakukannya penelitian; rumusan masalah; tujuan penelitian; manfaat penelitian; batasan masalah; dan sistematika penulisan.

Bab II Landasan Teori dan Kerangka Pemikiran

Bab II memaparkan landasan teori yang digunakan dalam penelitian, yang meliputi *Gate System* sebagai control akses, sistem RFID, teknologi smart card, NFC, Enkripsi *Caesar Chiper*, Enkripsi *Rotate Letter*, dan Arduino sebagai mikrokontroller dari sistem; penjabaran penelitian terkait dalam bentuk *roadmap* penelitian untuk melihat peluang penelitian dan jenis kebaruan yang diusulkan; serta kerangka pikir yang mendeskripsikan hubungan beberapa konsep dari penelitian ini berupa bagan sehingga lebih mudah untuk dipahami.

Bab III Metodologi Penelitian

Tahapan penelitian, waktu dan lokasi penelitian, alat dan bahan, jenis penelitian, sumber data, perancangan sistem, deskripsi sistem, skenario sistem, serta metode analisis kinerja sistem yang telah dirancang, diuraikan pada Bab III.

Hasil dan Pembahasan

ab IV menjabarkan hasil penelitian dalam bentuk tabel dan grafik mbahasan hasil penelitian.

Bab V Kesimpulan dan Saran

Kesimpulan yang merujuk pada rumusan masalah dan saran pengembangan penelitian disusun pada Bab V.

BAB II

TINJAUAN PUSTAKA

A. Landasan Teori

1. *Gate System*

Gate system menjadi standar dasar keamanan yang membutuhkan lebih banyak data untuk mengidentifikasi kendaraan atau orang yang masuk dalam suatu lingkungan (Gardeman, 2015). Pada perkembangannya *radio frequency* digunakan sebagai *trasnpounder.* Identifikasi dasar menggunakan kartu menjadi keandalan sistem. *Gate system* diproduksi menggunakan teknolgi magnetic *striped cards* dan *proximity cards* untuk proses identifikasi yang lebih cepat dimana sistem akan terbuka otomatis apabila data yang teridentifikasi telah teregister.

2. *Smart Card*

Smart card adalah sistem penyimpanan data elektronik, dengan kapasitas komputasi tambahan (kartu mikroprosesor) yang dimasukkan ke dalam kartu plastik seukuran sebuah kartu kredit. Salah satu keunggulan utama *smart card* adalah data yang tersimpan di dalamnya terlindungi dari akses dan manipulasi yang tidak diinginkan. Transfer data antara pembaca u berlangsung menggunakan antarmuka serial bidirectional (port I ini dimungkinkan untuk membedakan antara dua tipe dasar *smart*

card berdasarkan fungsionalitas internal yaitu *card memory* dan *microprocessor card*.

Ada tiga jenis chip yang berbeda yang dapat dikaitkan dengan *smart card, yaitu* :

a) *Memory-Only integrated circuit chip cards.* Memory-Only card merupakan *strip* magnetik elektronik dan memberikan keamanan lebih baik dari pada kartu strip magnetik. Kelebihan yang dimiliki jika dibandingkan kartu strip magnetik adalah memiliki kapasitas data yang lebih tinggi (sampai 16 Kbits dibandingkan dengan 80 byte per track); dan perangkat baca tulis jauh lebih murah. Kartu chip *memory-only* tidak mengandung logika atau melakukan perhitungan, melainkan hanya menyimpan data. Kartu chip memori yang dilindungi serial memiliki fitur keamanan yang tidak ditemukan dalam kartu chip memory-only.

b) *Wired logic integrated circuit chip cards.* Kartu chip berbasis logika menyediakan enkripsi dan akses otentik ke memori dan isinya. Kartu ini menyediakan sistem file statis yang mendukung banyak aplikasi dengan akses terenkripsi opsional ke konten memori. Sistem file dan command hanya dapat diubah dengan mendesain ulang logika sirkuit terpadu. Kartu chip logika terintegrasi termasuk contactless seperti I-Class atau MIFARE.

ure microcontroller integrated circuit chip cards. Kartu okontroler mengandung mikrokontroler, sistem operasi, dan

memori baca/tulis yang bisa diupdate berkali-kali. Kartu chip mikrokontroler yang aman berisi dan mengeksekusi logika dan perhitungan dan menyimpan data sesuai dengan sistem operasinya. Oleh karena kapasitas penyimpanannya yang terbatas dan tingkat keamanan yang rendah, kartu chip tidak sesuai dengan kartu multi-aplikasi atau multi-tujuan.

a. Kartu *contact* dan contactless

Ada dua tipe utama dari interface kartu chip-kontak dan contactless. Istilah "kontak" dan "contactless" menggambarkan sarana dimana daya listrik dipasok ke ICC dan dengan mana data dipindahkan dari ICC ke perangkat antarmuka. Kartu mungkin menawarkan antarmuka kontak dan penghubung tanpa kontak dengan menggunakan dua chip terpisah (hybrid) atau dengan menggunakan chip dual-interface.

1) *Contact smart card.* Memerlukan penyisipan ke pembaca *smart card* dengan koneksi langsung ke mikromodul konduktif di permukaan kartu.
2) *Smart card contactless* hanya berada di dekat pembaca (umumnya dalam jarak 10 sentimeter) agar pertukaran data berlangsung. Pertukaran data contactless terjadi melalui gelombang frekuensi radio (RF). Perangkat yang memfasilitasi komunikasi antara kartu dan pembaca adalah antena RF internal baik untuk kartu maupun pembaca. *Smart card* dengan kontak harus sesuai dengan standar ISO 7816 an yang tanpa kontak belum sepenuhnya distandarisasi (sebagian, SO 14443).

Sejauh pendekatan teknologi dan produk industri, jenis produk yang digunakan dalam dinyatakan dalam tiga bagian, antara lain:

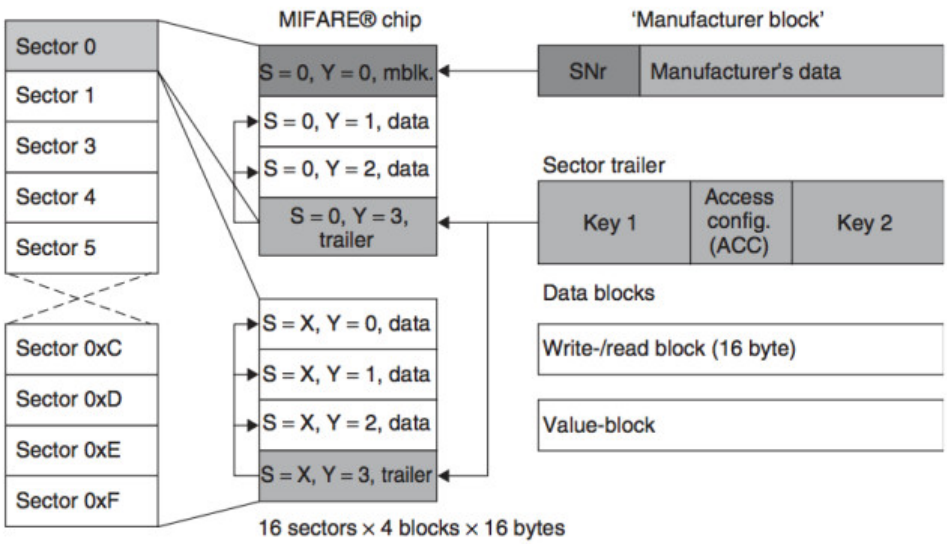
1) Kartu tipe A seperti kartu Philips mifare (contoh: London, Madrid, Helsinki)
2) Kartu tipe B seperti Innovatron Calypso (mis: Paris, Lisbon, Brussels)
3) Standar ketiga yang diwakili oleh kartu Sony Felica terutama digunakan di negara-negara Asia (misalnya: Hong Kong, Singapura).

Tipe A dan Tipe B sesuai dengan spesifikasi yang ditentukan dalam standar ISO 14443. Sebagian besar *smart card contactless* yang diimplementasikan dalam transportasi umum sesuai dengan standar ISO 14443. Kartu *contactless* berbasis standar dapat dengan aman mengotentikasi identitas seseorang, menentukan tingkat akses yang sesuai, dan mengakui pemegang kartu ke fasilitas, semua dari data yang tersimpan di kartu. ISO 14443 telah dirancang secara khusus untuk berfungsi dengan buruk di luar jangkauan 10 sentimeter.

b. Keamanan *smart card* jenis MIFARE

Memori transponder MIFARE® terbagi menjadi 16 segmen independen, dikenal sebagai sektor. Setiap sektor dilindungi dari akses yang tidak sah oleh dua kunci rahasia yang berbeda. Hak akses yang berbeda dapat dialokasikan ke masing-masing dua kunci dalam daftar akses sendiri (konfigurasi). Dengan demikian, 16 aplikasi independen yang gi satu sama lain oleh kunci rahasia dapat dimuat ke transponder, itunjukkan pada gambar 1. Tak satu pun aplikasi bisa dibaca tanpa

kunci rahasia, bahkan untuk pengecekan atau identifikasi. Jadi, tidak mungkin menentukan aplikasi apa yang tersimpan di transponder.



Gambar 1. Konfigurasi memory pada Mifare (Finkenzeller, 2010).

3. *Near Field Communication* (NFC)

Near Field Communication (NFC) bukanlah sistem RFID, namun merupakan komunikasi data *interface* nirkabel antara perangkat, mirip dengan Inframerah atau Bluetooth yang terkenal. Namun, NFC memiliki beberapa karakteristik yang menarik sehubungan dengan sistem RFID. Transmisi data antara dua *interface* NFC menggunakan frekuensi tinggi pada rentang frekuensi 13,56 MHz. Teknologi ini memungkinkan pengiriman data secara elektronik hingga jarak 10 cm. Komunikasi NFC dibedakan antara dua mode operasional yang berbeda, mode terbuka (aktif) dan mode tertutup (pasif)

1.) NFC Terbuka (aktif)

Untuk mentransmisikan data antara dua *interface* NFC dalam mode aktif, pada awalnya salah satu *interface* NFC mengaktifkan pemancar dan dengan demikian bekerja sebagai inisiator NFC. Arus frekuensi tinggi yang mengalir di antena menginduksi medan magnet *H* yang menyebar di sekitar antena Loop. Bagian dari medan magnet yang diinduksi bergerak melalui loop antena dari *interface* NFC lainnya yang terletak di dekatnya. kemudian tegangan *U* diinduksi pada loop antena dideteksi penerima *interface* NFC lainnya. Jika *interface* NFC menerima sinyal dan yang sesuai perintah inisiator NFC, *interface* NFC ini secara otomatis menerima sinyal yang dipancarkan target NFC.

Untuk transmisi data antara *interface* NFC menggunakan modulasi ASK, mirip dengan transmisi data antara RFID *reader* dan transponder. Namun, perbedaan antara target NFC dalam mode aktif dan RFID transponder terdiri dari medan magnet bolak-balk yang harus memasok transponder dengan daya untuk mengoperasikan *microchip*. Berbeda dengan hal tersebut, perangkat elektronik yang berisi *interface* NFC memasok *interface-nya* dengan *power*.

Arah transmisi dibalik agar bisa mengirim data dari target NFC ke inisiator NFC. Ini berarti target NFC mengaktifkan pemancar dan inisiator NFC beralih ke mode penerimaan kedua *interface* NFC secara bergantian

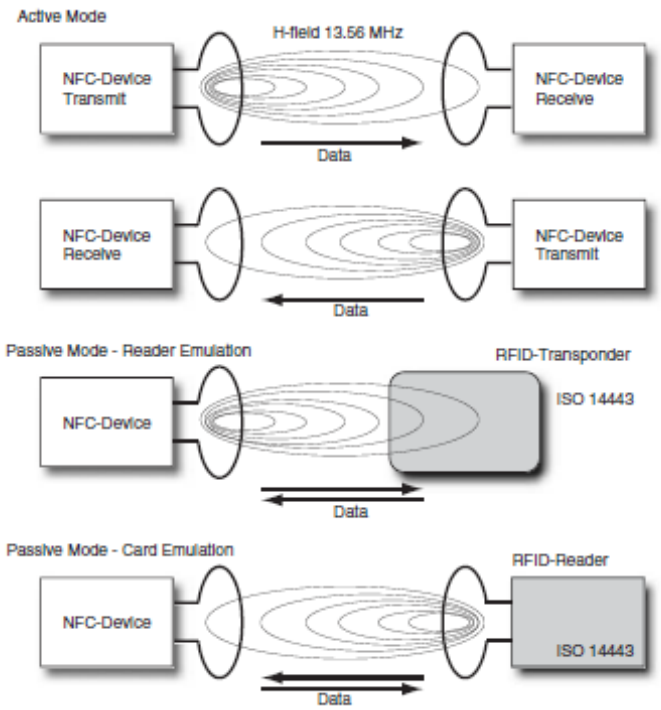
uksi medan magnet dimana data dikirim dari pemancar ke

a saja.

2.) NFC Tertutup (pasif)

Dalam mode pasif inisiator NFC juga menginduksi medan magnet untuk mentransmisikan data ke target NFC. Daerah amplitude dimodulasi sesuai dengan *pulse* data untuk ditransmisikan. Namun, setelah mentransmisikan blok data, daerahnya tidak terganggu, tapi terus dipancarkan dengan cara tidak dimodulasi. Target NFC mampu mengirimkan data ke inisiator NFC dengan menghasilkan modulasi beban. Metode modulasi beban juga diketahui dari sistem RFID.

Jika antarmuka NFC terletak dekat dengan pembaca RFID yang kompatibel (mis., Menurut ISO / IEC 14443), pembaca NFC juga bisa berkomunikasi dengan pembaca. *Interface* NFC menerima target NFC dan bisa mentransmisikan data ke pembaca menggunakan modulasi beban.



Gambar 2. Operasi NFC Mode Terbuka dan Mode Tertutup (Finkenzeller, 2010)

4. Enkripsi Caesar Chiper

Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (plaintext) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Pada Caesar cipher, tiap huruf disubtitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah pergeseran huruf (yaitu 3). Susunan alphabet setelah digeser sejauh 3 huruf membentuk sebuah table substitusi sebagai berikut:

Alfabet Biasa: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Alfabet Sandi: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya.

Penggunaan dari Caesar cipher ini dapat dimodifikasi dengan mengubah jumlah gesaran (bukan hanya 3) dan juga arah geseran. Jadi kita dapat menggunakan Caesar cipher dengan geser 7 ke kiri, misalnya. Hal ini dilakukan untuk lebih menyulitkan orang yang ingin menyadap pesan sebab dia harus mencoba semua kombinasi (26 kemungkinan geser) to dkk, 2012).

5. ISO/IEC 14443

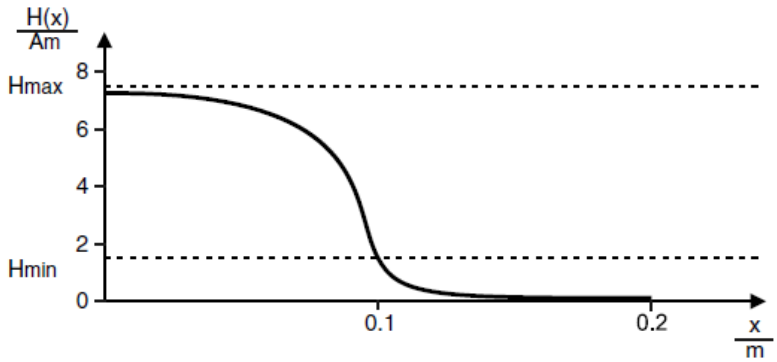
ISO 14443 menjelaskan sifat dan mode pengoperasian contactless kartu pintar dengan kisaran sekitar 10 cm. Standar ISO / IEC 14 443 terdiri dari bebrapa bagian yaitu karakteristik fisik, kekuatan frekuensi radio dan antarmuka sinyal, inisialisasi dan anticollision, serta protokol transmisi.

1) Karakteristik Fisik

Standar ISO / IEC 14 443, kartu identifikasi menjelaskan sifat dan mode pengoperasian kartu cerdas tanpa kontak dengan jarak sekitar 10 cm. Jumlah energi yang dapat ditransfer dalam rentang ini cukup untuk menyalakan mikroprosesor. Agar kartu jenis ini digunakan dengan infrastruktur yang ada untuk kartu tipe kontak, mereka sering memiliki kontak selain komponen kopling untuk operasi tanpa kontak, sehingga bisa digunakan dengan atau tanpa kontak sesuai keinginan. Jenis kartu ini disebut *dual-interface c*ard atau *combicard.*

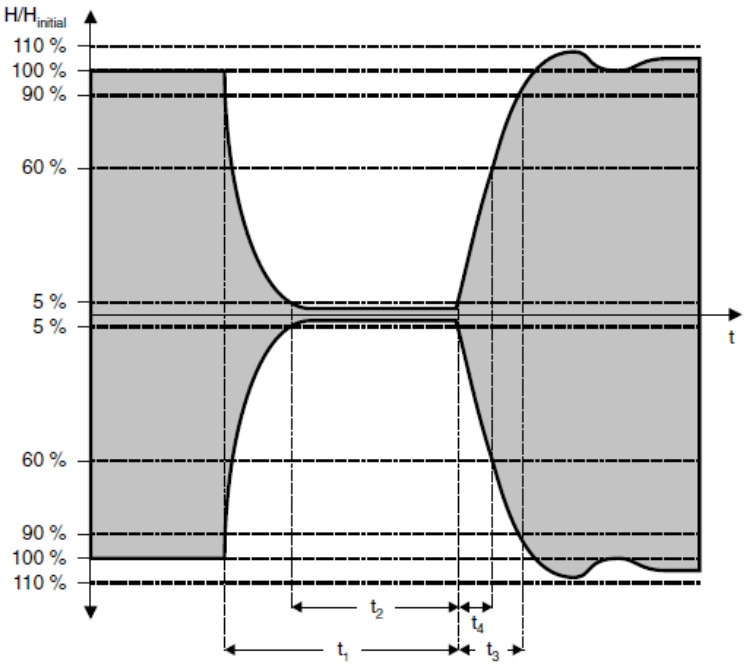
2) Kekuatan frekuensi radio dan antarmuka sinyal

Kartu *proximity* bekerja pada prinsip kopling induktif. Daya operasi dan data keduanya ditransfer menggunakan medan magnet bolak-balik yang dihasilkan oleh terminal kartu. Dalam ISO/IEC 14443 standar, terminal kartu disebut *proximity coupling device* (PCD). Demi dari keterbacaan, dalam uraian berikut istilah 'terminal' dan 'PCD' yang lebih umum digunakan secara bergantian.



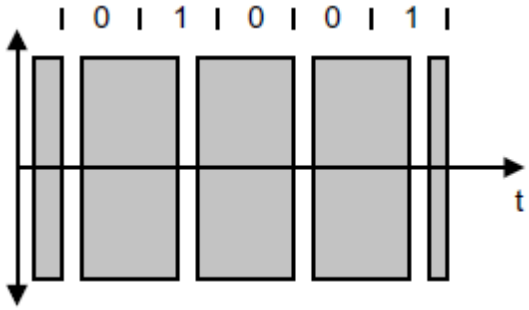
Gambar 3. Tipe karakteristik medan magnet dari sebuah terminal untuk kartu proximity (PCD)

Frekuensi transmisi PCD diatur ke fC = 13, 56 MHz ± 7 kHz, dengan medan magnetH dari kecepatan 1.5 A / m dan paling 7,5 A / m (efektif). Kekuatan khas Medan versus jarak. Peta jarak jauh (PICC). Dengan kurva gaya yang pada Gambar 3 dan kekuatan aktivasi PICC yang diasumsikan sebesar 1,5 W / m, kita menghasilkan pengaturan sekitar 10 cm.



Gambar 4. Spesifikasi dari blanking interval (gap) sesuai ISO / IEC 14433- 2

Maksimal durasi celah dibatasi sampai 3 μs untuk menyela pasokan energi ke kartu sesingkat mungkin. Disini 2,0 μs ≤ t1 ≤ 3,0 μs; 0,5 μs ≤ t2 ≤ t1 jika t1> 2,5 μs, atau 0,7 μs ≤ t2 ≤ t1 jika t1 ≤ 2,5 μs; dan 0 μs ≤ t4 ≤ 0,4 μs. Dengan kartu type A, transmisi data berlangsung di kedua arah pada tingkat fC / 128 bit (≈106 kbit / s). Modulasi amplitudo digital (100% ASK) dengan modified Miller coding digunakan untuk data beralih jarak jauh (gap) berada terbatas pada 3 μs. Interval blanking yang relatif pendek ini mempermudah penyediaan energi ke kartu. Spesifikasi pasti panjang interval blanking dan kenaikannya dan karakteristik peluruhan tahan pada Gambar 4. selama interval t4, yang berarti setelah magnetis telah mencapai 5% dari $H_{INITIAL}$ dan sebelum melebihi 60% dari $H_{INITIAL}$. Overshoot harus terbatas pada $H_{INITIAL}$ ± 10%.



Gambar 5. Pengkodean sedikit berurutan dikirim dari terminal ke kartu untuk komunikasi Tipe-A antarmuka dengan 100% ASK dan dimodifikasi Miller coding pada 106 kbit / s. Angka itu menunjukkan voltase di terminal udara

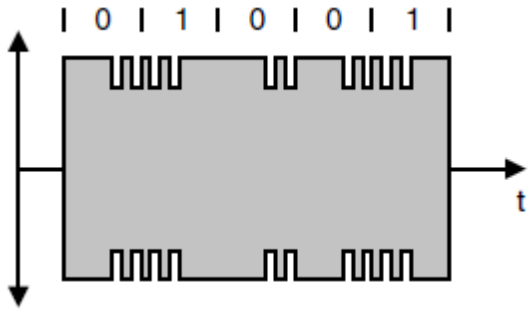
Contoh pengkodean urutan bit menggunakan pengkodean Miller yang dimodifikasi dalam Gambar 5. Aturan pengkodean berikut berlaku di sini:

- logika 1: interval blanking setelah setengah interval bit
- logika 0: tidak ada blanking, dengan nada sebagai berikut:
- Jika ada dua atau lebih logika 0 negara berturut-turut, ada interval blanking pada awal interval bit
- Jika bit pertama dari frame protokol adalah 0, itu penuh oleh interval blanking pada interval interval awal
- memulai sebuah pesan: interval blanking pada awal interval sedikit
- akhir sebuah pesan: logika 0 diikuti oleh satu bit tanpa interval blanking
- tidak ada data: tidak ada interval blanking untuk durasi minimal dua bit.

Kecepatan bit untuk transmisi data dari kartu ke terminal juga fC / 128 (≈106 kbit / s). Modulasi beban dengan subcarrier digunakan, yang berarti subcarrier dihasilkan oleh *switching* beban di dalam kartu. Frekuensi *subcarrier* ditentukan menjadi fS = fC / 16 (≈847 kHz). Subcarrier dimodulasi dengan mengganti dan menghidupkan subcarrier (on-off keying, atau OOK) menggunakan coding Manchester. Contoh pengkodean urutan bit ditunjukkan pada gambar 6. Pengkodeannya didefinisikan sebagai berikut:

ogika 1: kopian dimodulasi oleh subcarrier selama paruh pertama
nterval bit

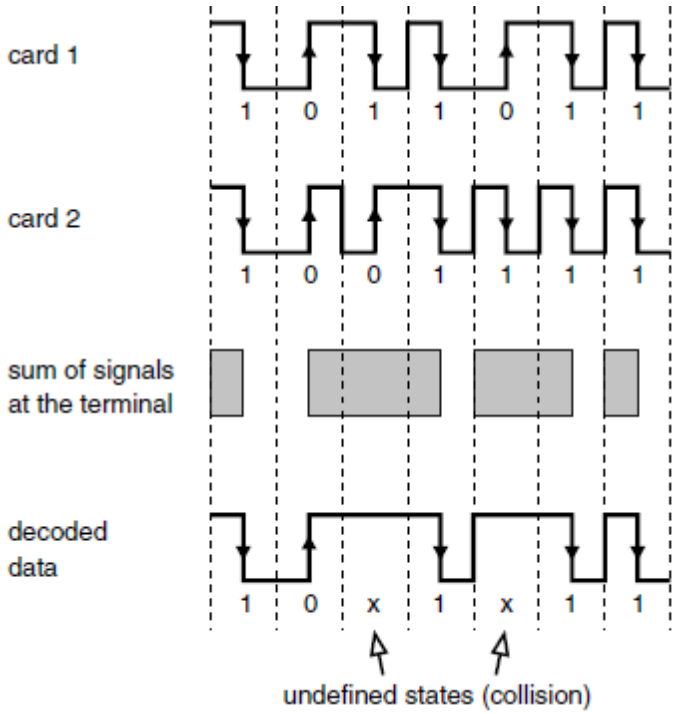
- logika 0: kopling dimodulasi oleh subcarrier selama paruh kedua interval bit
- memulai sebuah pesan: terbodulasi oleh subcarrier selama paruh pertama interval bit
- akhir pesan: tidak dimodulasi untuk interval satu bit
- tidak ada data: tidak ada modulasi subcarrier.



Gambar 6. Modulasi beban untuk transmisi data dari kartu ke terminal menggunakan subcarrier pada frekuensi fC / 16 (≈847 kHz) dan Manchester coding dengan bit rate 106 kbit / s dan OOK. angka menunjukkan voltase pada kumparan kartu

3) Inisialisasi dan anticollision

Algoritma pencarian biner dinamis digunakan untuk menginisialisasi dan memilih kartu Tipe-A. Dengan metode ini, maka perlu agar terminal bisa mengenali *collision* data pada tingkat bitnya. Seperti yang dijelaskan di bawah, pengkodean Manchester yang digunakan di sini t deteksi bitwise *collision* (lihat Gambar 7). Namun, ini uhkan semua kartu dalam jangkauan kerja terminal untuk smisikan data mereka serentak.

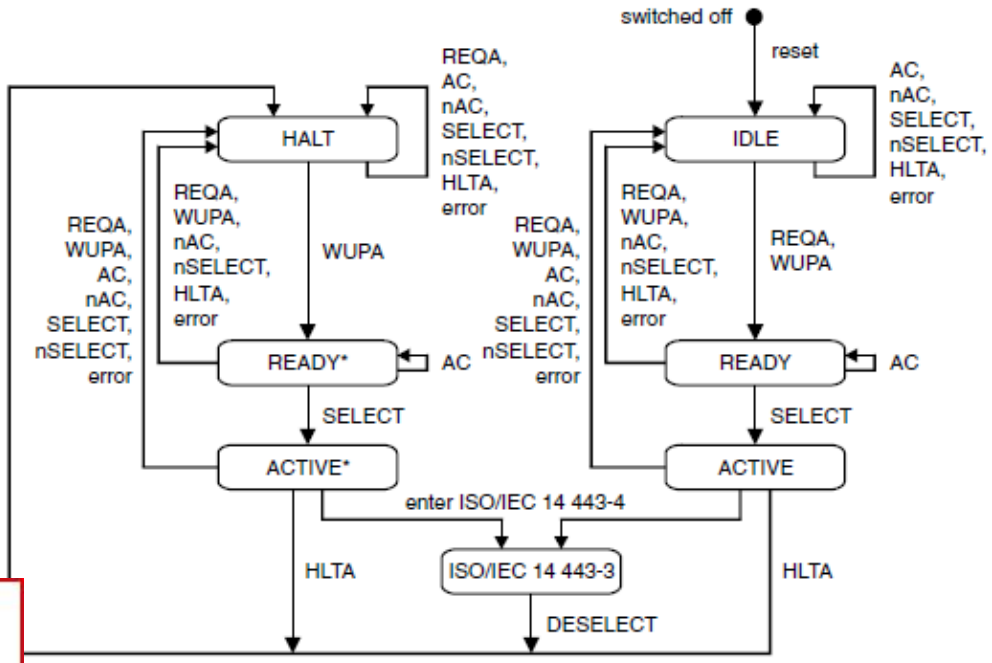


Gambar 7. collision dua bit sequence dengan pengkodean Manchester (Tipe A).

Dengan gangguan bebas transmisi, carrier selalu dimodulasi oleh subcarrier selama hanya satu setengah dari setiap interval bit. Jika Bit yang berbeda ditumpangkan, modulasi hadir untuk seluruh durasi interval bit, memungkinkan terminal untuk mendeteksi collision. Jika kartu kedekatan masuk ke bidang terminal, mikroprosesor di kartu diberikan dengan daya, dan setelah reset power-on masuk ke status Idle. Dalam keadaan ini, kartu hanya diizinkan untuk merespons perintah REQA (Request Type-A) atau a Perintah WUPA (Wake-up Type-A). Semua perintah lain dikirimkan oleh terminal untuk berkomunikasi dengan kartu Tipe-A atau Type-B lainnya yang sudah ada dalam pekerjaan jangkauan terminal harus diabaikan agar ngganggu komunikasi ini. Diagram keadaan yang ditunjukkan pada

Gambar 8. menunjukkan semua kemungkinan keadaan yang dapat diasumsikan oleh kartu Tipe-A selama fase inisialisasi dan *anticollision*. Seperti telah disebutkan, kartu masuk ke status Idle setelah reset power-on. Standar mengharuskan kartu masuk ke status Idle dalam waktu 5 ms setelah menerima daya operasi yang memadai dari lapangan terminal Dalam status Idle, kartu tersebut menunggu perintah lebih lanjut. Ini berubah menjadi siap saat mengenali aREQAorWUPAcommand, namun mengabaikan semua perintah lainnya.

Untuk memastikan tingkat keandalan yang tinggi untuk mengenali perintah REQA dan WUPA, perintah ditransfer menggunakan bingkai pendek khusus. Semua perintah lainnya kecuali anticollision perintah ditransmisikan menggunakan frame standar. Bingkai khusus disebut *anticollision* berorientasi bit frame didefinisikan untuk perintah *anticollision*.



8. Diagram keadaan PICC Tipe-A selama fase inisialisasi dan *anticollision*

4) Protocol transmisi data

Bagian 4 dari ISO / IEC 14443 menjelaskan protokol transmisi half-duplex block yang dapat digunakan saat PICC berada dalam status Active. Protokol ini berada di luar cakupan aplikasi ini; Namun, pengkodean byte perintah ditunjukkan pada Tabel 1 dan Tabel 2 untuk referensi

Tabel 1. Tipe B *Commands*

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Command Name	Hexadecimal
1	1	0	0	CID	0	1	0	DESELECT S-Block	$C2/CA
1	1	1	1	CID	0	1	0	WTX S-Block	$F2/FA
0	0	0	chain	CID	NAD	0	Block	I-Block	$0x/1x

Tabel 2. Tipe B *Response*

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Command Name	Hexadecimal
1	0	1	ACK	CID	0	1	Block	R-Block ACK	$Ax
1	0	1	NAK	CID	0	1	Block	R-Block NAK	$Bx

6. Mikrokontroller Berbasis Board Arduino Uno

Arduino Uno adalah *board* atau papan mikrokontroler berdasarkan ATmega328. Arduino memiliki 14 pin input / output digital (6 dapat digunakan sebagai output PWM), 6 input analog, resonator keramik 16 MHz, koneksi USB, colokan listrik, header ICSP, dan tombol reset dan berisi segalanya yang diiperlukan untuk mendukung mikrokontroler. gantinya, fitur Atmega16U2 (Atmega8U2 sampai versi R2) m sebagai USB-to-serial.

Revisi 2 dari papan Uno memiliki sebuah resistor yang menarik garis 8U2 HWB ke ground, sehingga memudahkan untuk dimasukkan ke dalam mode DFU. Revisi 3 papan memiliki fitur baru berikut;

1. 1.0 pin out: tambahkan pin SDA dan SCL yang berada di dekat pin AREF dan dua pin baru lainnya yang ditempatkan di dekat pin RESET, IOREF yang memungkinkan *shield* untuk menyesuaikan voltase yang diberikan dari *board*. Di masa depan, perisai akan kompatibel baik dengan *board* yang menggunakan AVR, yang beroperasi dengan 5V dan dengan Arduino Due yang beroperasi dengan 3.3V.
2. Rangkaian RESET yang lebih kuat.
3. Atmega 16U2 menggantikan 8U2.

Gambar 9. Arduiono Uno R3 (datasheets)

B. Penelitian Terkait

Penelitian mengenai akses kontrol dengan memanfaatkan *smart card* unruk identifikasi dan otentikasi telah dilakukan sebelumnya. Dalam penelitian selanjutnya oleh penulis, dilakukan inovasi dari penelitian sebelumnya. Diharapkan penelitian ini akan memberikan hasil yang baik dari penelitian sebelumnya. Beberapa penelitian terkait yang membahas mengenai *smart card* dan *gate system* adalah berikut:

1. Penelitian Kao Liu dan Huang Yang (2008), " Design and Implementation of Campus Gate Control System Basen on RFID" mengembangkan pengendalian gerbang / *gate* kampus dengan proses identifikasi yang dibangun melalui *server-end* database dan Local Area Network (LAN) kampus. Proses pengiriman informasi antara *client* dan computer *server-end* menggunakan fungsi Hash satu arah untuk membangkitkan *message digest* (nilai yang juga dikenal sebagai kriptografi atau secure hash) juga mengadopsi Advanced Encryption Standart (SDA) untuk memperkuat proteksi dari informasi pribadi dan secara keseluruhan keamanan sistem.
2. Penelitian Rosa Ma. *et al.,* (2016) "Design and Implementation of a System Access Control by RFID" kontrol akses dengan sistem RFID untuk menentukan atau memberlakukan control akses dan embatasan di area utama bangunan universitas yang seharusnya anya bisa diakses oleh sekelompok kecil staf. Mekanisme akses ontrol dilakukan dengan mengevaluasi permintaan akses pada

database. Permintaan yang memiliki otorisasi akan diizinkan dan ditolak apabila tidak memiliki otorisasi pada database. Program dikembangkan dengan menggunakan MATLAB.

3. Bouazzouni *et al.,*(2016) *“* Trusted Acces Control System for Smart Campus” mengajukan sebuah arsitektur untuk membangun sistem akses kontrol yang aman berbasis Trusted Execution Environtmen (TEE) dan Identity Based Encryption (IBE). TEE adalah kombinasi dari sebuah perangkat keras dan perangkat lunak dimana eksekusi sistemnya terbagi dalam dua lingkungan. Lingkungan pertama adalah Rich Execution Environtment (REE) atau Normal World Execution Environtment yang merupakan standar Operating System dari *smart phone* Android. Otentikasi dilakukan berdasarkan IBE dan TEE yang dipresentasikan dalam OP-TEE.
4. Gruntz *et al.,*(2016) *“* MOONAC: a mobile on-/offline NFC- based physical access control syst em”mengembangkan *smart phone* yang berdasarkan sistem akses kontrol secara fisik dimana akses poin tidak secara langsung terhubung ke sever pusat, tetapi lebih menggunakan konektivitas dari *smart phone* untuk dapat mengakses permintaan akses online dari pengguna dengan menggunakan server akses pusat. Otentikasi dari *smart phone* berdasar pada kunci kriptografi publik. Hal tersebut membutuhkan kunci pribadi disimpan alam suatu sistem pengamanan atau dalam TEE untuk enghindari pencurian identitas.

5. Penelitian Jacob *et al.,* (2015) " Mobile Attendance using Near Field Communication and One Time Password" menerapkan One-Time Password pada system kehadiran menggunakan NFC. One-Time Password dibuat secara otomatis dengan membangkitkan string karakter numerik atau alfanumerik pada otentikasi *user* untuk satu kali sesi transaksi menggunkan NFC *card.*

Penelitian Bouazzouni *et al., (2*016) dan Gruntz *et al.,*(2016) memanfaatkan *smart phone* yang dilengkapi NFC untuk melakukan akses, sehingga apabila diterapkan dalam system akses kontrol setiap *user* atau pengguna diwajibkan memiliki *smart phone* yang dilengkapi NFC. Sebagai solusi dalam penelitian yang penulis ajukan dibutuhkan *smart card* NFC sebagai pengganti *smart phone.*

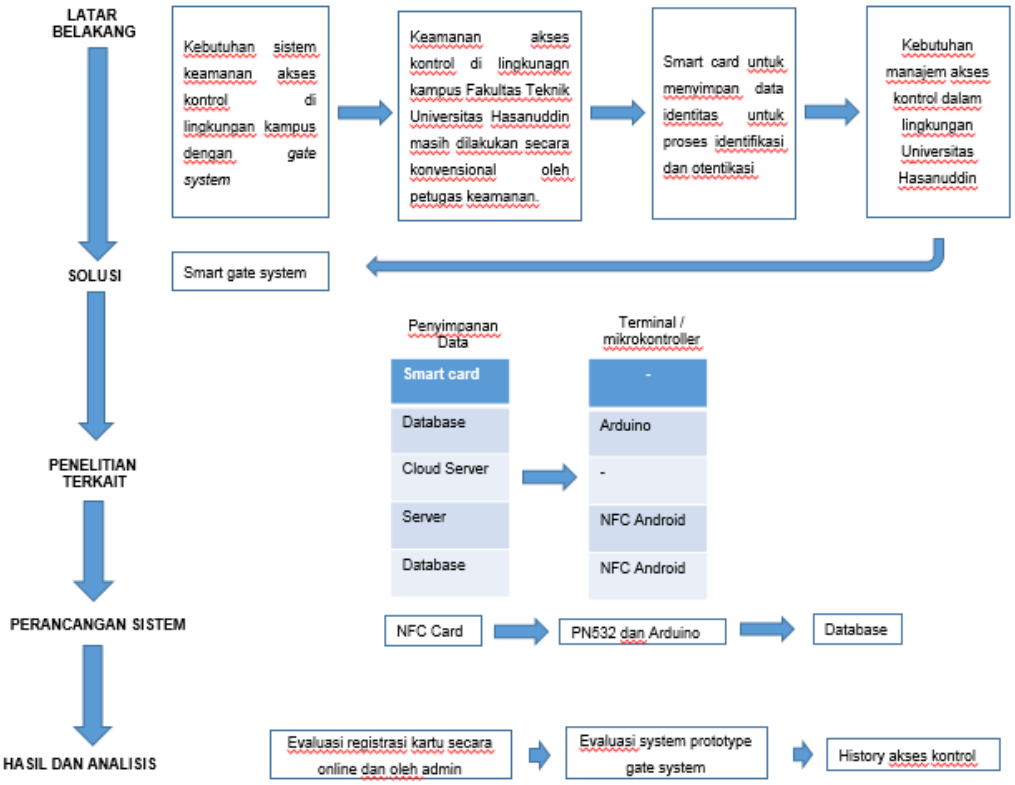
Penelitian Kao Liu dan Huang Yang (2008) Rosa Ma. *Et al.,* (2016) sistem akses kontrol berbasis RFID rentan pada resiko serangan yang memungkinkan kloning dari tag / kartu untuk mendapatkan akses ke fasilitas akses control. Solusi untuk mengatasi resiko tersebut adalah dengan meningkatkan keamanan pada verifikasi dan otentikasi user. Dengan mengambil konsep dari One Time Pasword pada NFC *card*, penelitian yang diusulkan juga menerapkan hal serupa dengan memasukkan kode berupa "key" ke dalam kartu.

Tabel 3. *Roadmap* penelitian terkait akses kontrol

Penelitian	Identifikasi	Penyimpanan identititas	Terminal/ Mikrokontroller	Data transfer
Penelitian Kao Liu dan Huang Yang (2008)	RFID TAG	Smart card	-	LAN
Rosa Ma. *et al.,* (2016)	RFID TAG	Database	Arduino	-
Bouazzouni *et al.,*(2016)	NFC Smartphone	Cloud Server	-	-
Gruntz *et al.,*(2016)	NFC Smartphone	Server	NFC Android	-
Jacob *et al.,* (2015)	NFC TAG	Database	NFC Android	Intranet
Khairunnisa M. (2017)	NFC TAG	Smart card	Arduino	LAN

C. Kerangka Pikir

Adapun untuk kerangka pikir penelitian ini ditunjukkan pada blok diagram sebagai berikut :



Gambar 10. Kerangka pikir

Kerangka pikir penelitian disajikan dalam bagan penelitian seperti yang ditunjukkan pada gambar 10. Penjelasan mengenai setiap bagan kerangka pikir penelitian yaitu:

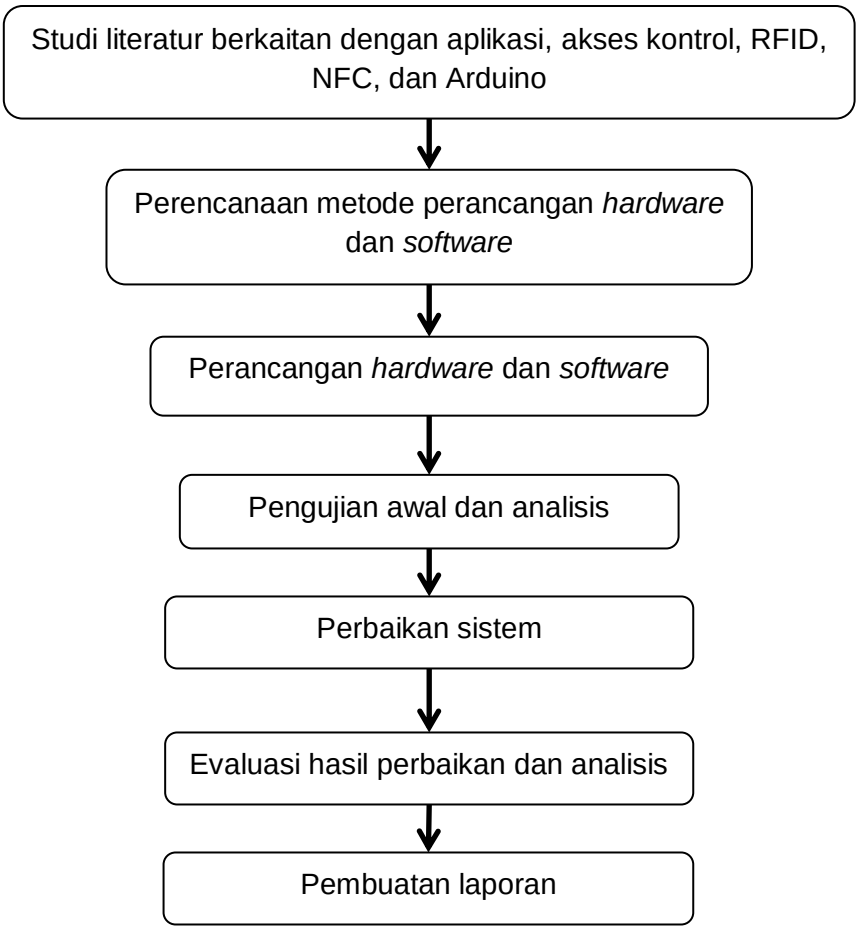
1. Latar belakang. Berisi tentang alur yang mendasari penelitian ini mengenai akses kontrol keamanan menggunakan identitas *smart card* gai untuk otentikasi.

2. Solusi. Masalah pada latar belakang diberikan solusi sebagai inti sari penelitian ini dan sebagai penelitian awal yang akan dikembangkan selanjutnya.
3. Penelitian terkait. Berisi tentang rincian penyimpanan data, dan unit terminal pada penelitian terkait.
4. Perancangan sistem. Perancangan sistem tiket elektronik merupakan pengembangan dari penelitian terkait.
5. Hasil dan analisis berupa evaluasi pada registrasi kartu, evaluasi sistem prototipe dan evaluasi pada web berupa *history* akses kontrol.

BAB III
METODE PENELITIAN

A. Tahapan Penelitian

Penelitian ini merupakan pengembangan dari penelitian-penelitian yang telah ada sebelumnya. Adapun tahapan-tahapan yang akan dilakukan diuraikan pada bagan berikut:



Gambar 11. Tahapan penelitian

Berdasarkan tahapan penelitian pada gambar 11, tahapan-tahapan dalam penelitian ini adalah sebagai berikut:

1. Studi literatur yang dilakukan terkait pada akses kontrol RFID, NFC, Enkripsi dan Arduino beserta bahasa pemrograman pendukungnya. Pada bagian ini dilakukan pula pengkajian literatur untuk membandingkan penelitian ini dengan penelitian terdahulu sehingga terbentuk pola roadmap penelitian.
2. Perencaan metode perancangan *hardware* dan *software* merupakan tahapan yang termasuk di dalamnya langkah menyusun rencana penelitian yang meliputi perancangan prototipe *smart gate*, perancangan akses data smart card, dan perancangan web server. Penelitian ini termasuk dalam jenis pendekatan yang bersifat pengembangan dari metode yang telah ada, yang disebut *discovery approach*.
3. Setelah membuat perencanaan, selanjutnya melakukan perancangan Hardware dan Software yang sesuai dengan tahapan perencanaan metode.
4. Pengujian awal dan analisis yaitu melakukan uji coba dalam skala terbatas. Pada perencanaan awal, sistem dirancang secara *online*. Dalam melakukan identifikasi, terminal membutuhkan koneksi internet untuk mengambil data dari server. Analisis awal yang diperoleh adalah ampuan terminal mengakses data dipengaruhi oleh kecepatan

jaringan internet. Hal-hal yang disebutkan merupakan sebuah keterbatasan yang membutuhkan perbaikan.

5. Perbaikan sistem adalah perbaikan terhadap produk awal yang dihasilkan berdasarkan hasil uji coba awal. Perbaikan ini dilakukan di semua sisi yakni pada sisi prototipe, server, *smart card* dan pemrograman yang berkaitan.
6. Evaluasi hasil perbaikan dan analisis merupakan uji validasi terhadap model operasional yang telah dihasilkan untuk mengetahui keakuratan dan sensitivitas sistem. Selain itu dilakukan juga proses analisis terhadap parameter-parameter terkait.
7. Pembuatan laporan merupakan tahapan untuk menulis keseluruhan proses penelitian yang telah dilakukan, berupa laporan tesis dan artikel jurnal yang akan dipublikasikan.

B. Waktu dan Lokasi Penelitian

Waktu Penelitian dilaksanakan selama delapan bulan dimulai pada bulan November 2016 sampai Juni 2017. Penelitian dilakukan di Laboratorium Antena, Departemen Teknik Elektro, Universitas Hasanuddin.

C. Alat dan bahan

Instrumen yang digunakan pada penelitian ini terbagi atas hardware dan software.

1. *Hardware*:
   a) NFC *Reader* PN532
   b) Mifare classic 1K
   c) Arduino Uno R3
   d) Ethernet Shield
   e) Sensor Ping HC SR-04
   f) Motor servo
   g) Router
   h) Komputer dengan *processor* Intel Core i5-3317U (1.7 GHz), windows 7 64-bit operating system.
   i) Kabel *jumper*
   j) Maket *gate*
2. *Software*:
   a) Aplikasi pemrograman Arduino IDE
   b) Aplikasi pemrograman Java Script
   c) PHP 5
   d) XAMPP control panel V3.2.1
   plikasi pemrograman MySQL
   plikasi pemerograman Visual Basic 2010

D. Jenis Penelitian

Jenis penelitian ini merupakan penelitian eksperimental yang bersifat aplikatif sehingga dari ruang lingkup masalah dilakukan pengkajian dengan metode studi pustaka (*library research*) dan studi lapangan (*field research*) dilanjutkan dengan perancangan perangkat dan pembuatan aplikasi.

E. Sumber Data

Data yang digunakan merupakan data input uji coba terhadap *smart card* yang diujikan dalam sistem. Data ini akan digunakan untuk menguji kinerja sistem yang telah dirancang kemudian akan divalidasi untuk melihat tingkat keberhasilan sistem dan perangkat dalam melakukan pembayaran.

F. Perancangan Sistem

Penelitian terbagi atas beberapa tahapan perancangan, antara lain: perancangan basis data, perancangan website, perancangan sistem akses data kartu, perancangan prototipe.

1. Perancangan Basis Data

Perancangan basis data merupakan proses untuk menentukan jenis data yang dibutuhkan sebagai dukungan sistem penyimpanan data. e tersimpan dalam bentuk tabel terpisah sebagai penampung i basis data. Tabel tersebut diantaranya; tabel pengguna

(db_siswa) digunakan sebagai penyimpan data pengguna; tabel admin (db_admin) sebagai penyimpan data admin; (db_history) untuk menyimpan riwayat akses masuk dan keluar gate.

Program basis data yang digunakan adalah MySQL. Semua perintah dimasukkan melalui *command prompt* karena tidak memiliki antarmuka visual. Salah satu pembuatan tabel ditunjukkan pada perintah berikut:

```
no_siswa int(3) NOT NULL AUTO_INCREMENT PRIMARY KEY,
nim varchar(15) NOT NULL,
nama varchar(60) NOT NULL,
jurusan varchar(60) NOT NULL,
status varchar(100) NOT NULL,
jurusan varchar(100) NOT NULL,
alamat varchar(100) NOT NULL,
no_telp varchar(13) NOT NULL,
uid varchar(8) NOT NULL);

CREATE TABLE siswa(
```

Dari perintah tersebut dihasilkan sebuah tabel yang ditunjukkan pada gambar 12.

Gambar 12. Tabel basis data pengguna

2. Perancangan Website

Tujuan perancangan website pada penelitian ini adalah sebagai untuk melayani pengguna kartu, dimana secara khusus akan ikan oleh seorang administrator. Basis data yang telah dibuat

merupakan media penyimpanan data yang diperlukan untuk membuat website lebih dinamis sehingga memungkinkan data yang ada dapat dimonitoring. Selanjutnya, website akan dikoneksikan dengan basis data dengan perintah berikut:

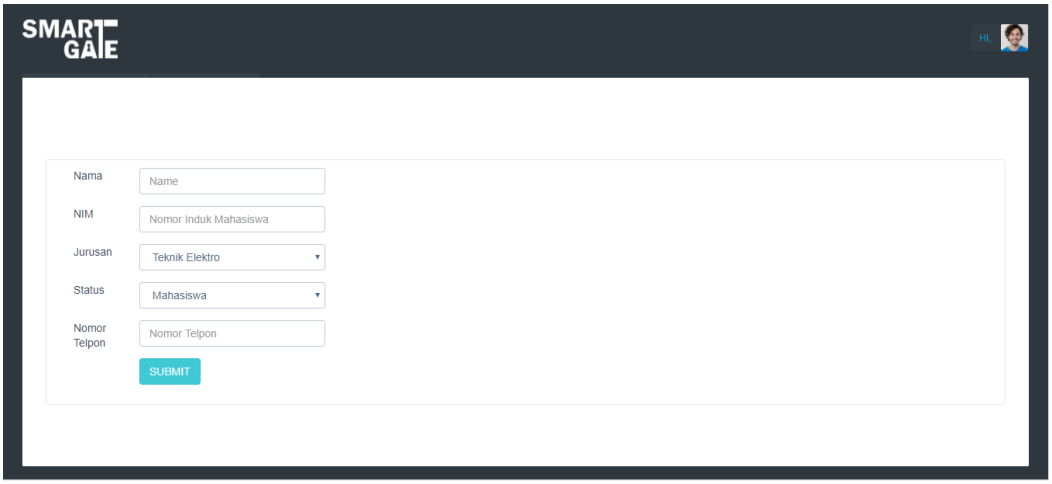
```php
<?php
$myHost = "localhost";
$myUser = "root";
$myPasw = "";
$myDbs = "siswadb";

$koneksiDbs = mysql_connect($myHost, $myUser, $myPasw)or die ("Gagal Koneksi..!").mysql_error();
mysql_select_db($myDbs)or die ("Database $myDbs tidak ada".mysql_error());
?>
```

Terdapat perancangan beberapa form yang akan digunakan untuk menginput, menampilkan, dan mengedit data di dalam database tersebut.

Pada basis data tabel db_admin data-data yang dibutuhkan adalah, NIM, nama, jurusan, nomor telepon. Semua fied harus terisi pada saat registrasi. Ketika data yang dibutuhkan sudah lengkap dan benar, data akan ditambahkan ke dalam basis data. Dari rincian tersebut, ditulis perintah sebagai berikut:

```
                <div class="row">
                    <div class="col-md-12">

                        <!-- Begin: life time stats -->
                        <div class="portlet light portlet-fit portlet-datatable bordered">

                            <div class="portlet-body">
                                <div class="table-container">
                                                <form class="login-form" action="auth1.php" method="post">

                                                <div class="form-group">
                                                <span class="col-md-1 control-label">Nama</span>
                                                    <!--ie8, ie9 does not support html5 placeholder, so we just show field title for that-->
                                                    <label class="control-label visible-ie8 visible-ie9">Nama</label>
                                                    <input class="form-control input-inline input-medium" type="text" autocomplete="off"
placeholder="Name" name="nama"/>
                                                </div>

                                                <div class="form-group">
                                                <span class="col-md-1 control-label">NIM</span>
                                                    <!--ie8, ie9 does not support html5 placeholder, so we just show field title for that-->
                                                    <label class="control-label visible-ie8 visible-ie9">NIM</label>
                                                    <input class="form-control input-inline input-medium" type="text" autocomplete="off"
placeholder="Nomor Induk Mahasiswa" name="nim"/>
                                                </div>
```

Dari perintah tersebut, dihasilkan tabel yang ditunjukkan pada gambar 13.



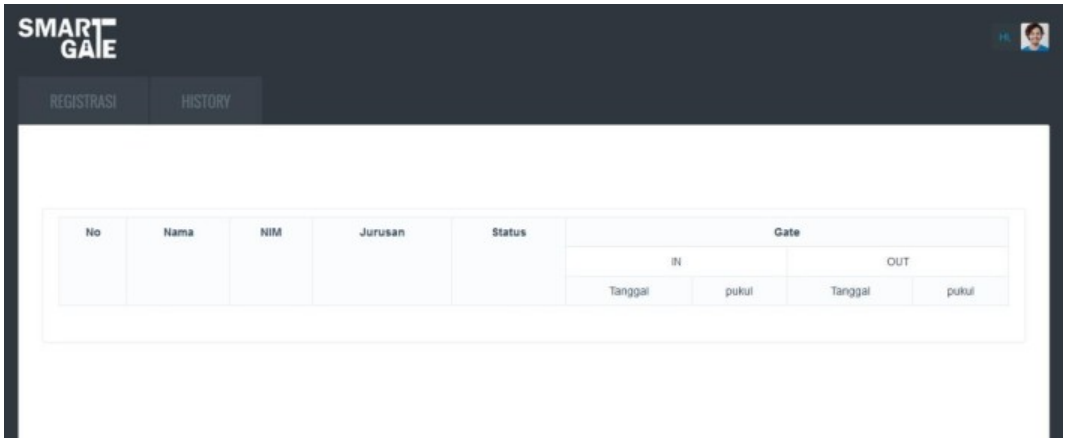
Gambar 13. Form registrasi

Pada form data pengguna, data user yang ada ditampilkan pada tabel basis data. Data akan disimpin dalam database server untuk proses selanjutnya.

i. Form *History* Akses Masuk dan Keluar *Gate*

Adapun form riwayat *history* adalah riwayat akses keluar dan masuk. Perintah untuk pengecekan history ditunjukkan sebagai berikut:

```
                                <div class="table-container">
                                    <table class="table table-striped table-bordered" style="width:100%">
                                        <tr>
                                          <th rowspan="3">No</th>
                                          <th rowspan="3">Nama</th>
                                          <th rowspan="3">NIM</th>
                                          <th rowspan="3">Jurusan</th>
                                          <th rowspan="3">Status</th>
                                          <th colspan="4">Gate</th>

                                        </tr>
                                        <tr>
                                          <td colspan="2">IN</td>
                                          <td colspan="2">OUT</td>
                                        </tr>
                                        <tr>
                                          <td>Tanggal</td>
                                          <td>pukul</td>
                                          <td>Tanggal</td>
                                          <td>pukul</td>
                                        </tr>
                                        <?php
                                        include "koneksidb2.php";
                                        $sql = "SELECT history.*, siswa.nama,siswa.jurusan,siswa.nim,siswa.status FROM history,siswa WHERE
siswa.uid=history.uid ORDER BY history.no";
```



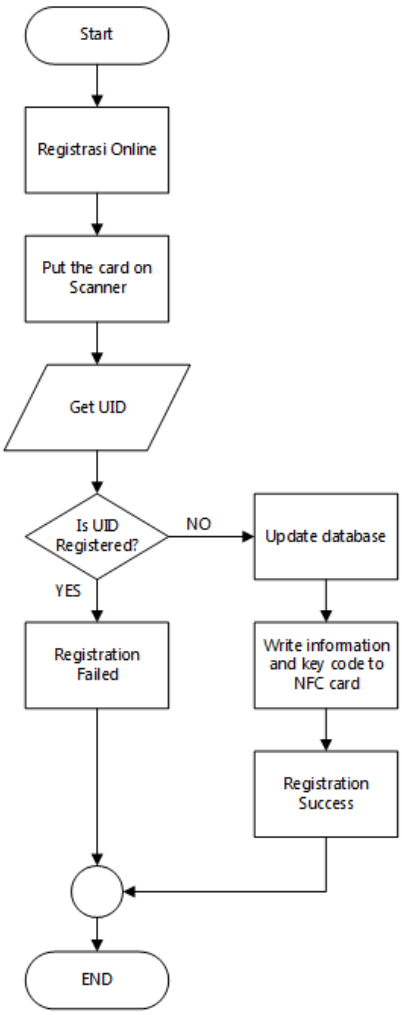
Gambar 14. Form riwayat akses kontrol

3. Registrasi Kartu

Penelitian ini mengarah pada perwujudan *smart campus* sehingga dirancang dalam lingkup civitas akademika. *Smart card* yang dirancang memuat informasi identitas pengguna antara lain nama, NIM, jurusan, status, nomor telepon, dan alamat. Secara khusus, jabatan yang dimaksud adalah mahasiswa, staf, karyawan, dan dosen. Dengan adanya informasi identitas pengguna, maka pihak kampus dapat mengatur siapa saja yang memiliki hak untuk memanfaatkan suatu sarana dan prasarana yang ada.

Proses registrasi nantinya dilakukan secara online melalui website yang telah disediakan dan data informasi akan tesimpan dalam database server. Informasi yang diunggah berupa biodata nama, nomor identitas, dan nomor telepon serta informasi penting lainnya. Pihak administrasi kampus yang berwenang dalam hak akses system (admin) melakukan update Dentifier (UID) NFC dan penulisan informasi biodata kedalam NFC ata informasi yang ditulikan ke dalam NFC card telah melalui

enkripsi. Enkripsi dilakukan dengan metode *Caesar Chiper* dan metode *Rotate Letter.* Untuk memberikan keamanan akses control masuk dan keluar dituliskan kode rahasia “key in” untuk akses masuk dan “key out” untuk akses keluar pada NFC tag.



Gambar 15. Flowchart Algoritma Registrasi Kartu

dministrator melakukan validasi data user yang telah terdaftar. data dinyatakan valid, NFC tag didekatkan pada reader untuk scan a kartu. Setelah didapatkan UID dilakukan proses registrasi oleh

administrator. Pada tahap registrasi pertama dilakukan update UID user ke database server kemudian proses *write* informasi dan *key* pada kartu. NFC PN532 digunakan sebagai *reader* dan *writer* informasi biodata pada NFC tag sesuai ISO 144443A. Parameter yang digunakan untuk penulisan pada kartu adalah alamat memori tempat pengumpulan data, data yang ditransmisikan, dan kunci otentikasi berupa “key”. Jenis NFC card yang digunakan adalah Mifare Classic 1 K ISO/IEC 14443A yang terdiri dari 16 sektor yang dilindungi oleh dua kunci yang berbeda (key A dan Key B). setiap sektor terdiri dari 3 blok data dan 1 blok trailer dimana tiap blok berisi 16 byte.

Perintah untuk registrasi kartu oleh administrator ditunjukkan sebagai berikut:

```
Private Sub uid_TextChanged(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles uid.TextChanged
    Timer1.Enabled = False
End Sub

Private Sub registrasibtn_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles registrasibtn.Click
    Dim update As String
    update = "update siswa set uid = '" & uid.Text & "' WHERE nim = '" & nim.Text & "' "
    CMD = New OdbcCommand(update, Conn)
    CMD.ExecuteNonQuery()

    txtEnc.Text = EncryptDecrypt(txtserial.Text, txtKey.Text, True)
    textToReverse = txtEnc.Text
    Letters = textToReverse.ToCharArray()
    Array.Reverse(Letters)
    Dim ReversedText As New String(Letters, 0, Letters.Length)
    txtResult.Text = "!" + ReversedText

    SerialPort1.Write(txtResult.Text)
    Timer1.Enabled = True

    MsgBox("Data UID berhasil di daftar")
End Sub
```

Gambar 16. Form Registrasi oleh Administrator

4. Proses Enkripsi Melalui *Visual Basic*

Proses baca / tulis informasi pada smart card akan dikonfigurasi dimana blok data dapat dibaca dengan menggunakan *software* yang telah dirancang dengan menggunakan aplikasi Visual Basic (VB) 2010. Proses penulisan data pada NFC *tag* melalui komunikasi serial dimana data informasi digabungkan menjadi 1 line informasi yang telah melalui tahapan enkripsi kemudian akan dialokasikan dalam bentuk *array* kedalam blok data yang telah ditentukan dalam penelitian ini yakni blok data 9,10,11 dan 13 dengan total data 64 Byte. Pada tahap pengisian informasi pada NFC *tag* dilakukan dua pihak yakni mahasiswa dan pihak administrasi kampus.

Tahap pertama mahasiswa melakukan pengisian biodata secara *online* dan data tersebut akan tersimpan dalam database yang dapat oleh pihak administrasi kampus sebagai pihak yang melakukan i dan penulisan data pada NFC *tag*. Proses penulisan data pada g melalui beberapa tahap yakni verifikasi data pada database,

enkripsi data dan penulisan data ke NFC *tag*. Verifikasi data yakni proses dimana pihak administrasi kampus melakukan pencarian Nomor Induk Mahasiswa (NIM) pada aplikasi VB yang telah dirancang dan dikoneksikan pada *server database* apabila NIM telah terdaftar maka secara otomatis aplikasi VB akan menampilkan informasi yang telah diisi oleh pihak mahasiswa. Informasi yang diperoleh dari database kemudian akan dilakukan proses enkripsi untuk memberikan sistem keamanan informasi pada *tag* sehingga pihak lain tidak dapat melakukan pembacaan blok data tanpa menggunakan apikasi VB dan mengetahui sistem enkripsinya.

Data mahasiswa dilindungi dengan melalui 2 (dua) tahap enkripsi. Enkripsi pertama dilakukan dengan metode Caesar Chiper, metode enkripsi ini berbasis sistem pergerseran dimana huruf/karakter asli akan digantikan dengan karakter lain dan merujuk pada *key* yang telah ditentukan dengan formula enkripsi sebagai $E_n(x) = (x + n)$ dimana, $E_n(x)$ = Hasil enkripsi, X = Karakter asli N = *Key.* Sebagai contoh proses Caesar chipper yakni informasi asli KHAIRUNNISA akan dilakukkan menggunakan Caesar Chiper dengan key 24 maka informasi asli akan melalui proses enkripsi ditunjukkan pada Tabel 4.

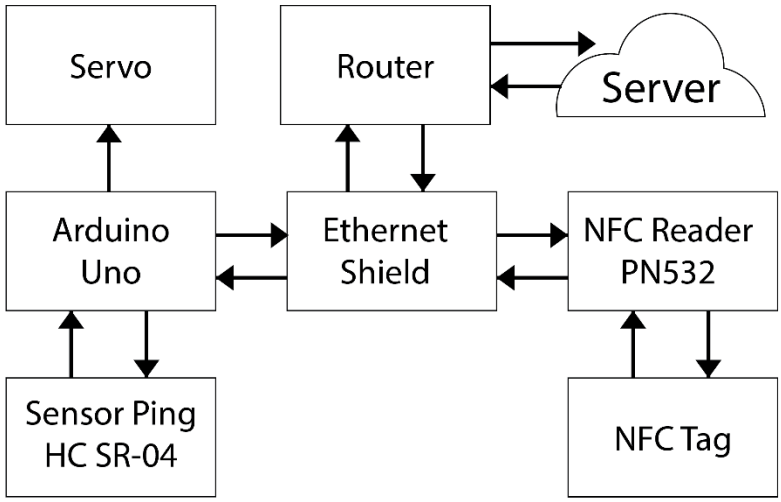
Tabel 4. Enkripsi caesar chiper

Informasi	Key	Hasil Enkripsi
K	2	M
H	4	L
A	2	C
I	4	M
R	2	T
U	4	Y
N	2	P
N	4	R
I	2	K
S	4	W
A	2	C

Setelah melalui tahap enkripsi awal Caesar Chiper maka untuk memastikan informasi mahasiswa lebih aman maka dilakukan enkripsi tahap kedua dengan metode *rotate letter* dimana urutan karakter pada informasi dibalik secara utuh. Informasi yang mengalami enkripsi Caesar Chiper yakni MLCMTYPRKWC akan dirotasi menjadi CWKRPYTMCLM dan informasi inilah yang akan diwrite pada NFC *tag* melalui komunikasi serial dari *desktop* ke NFC *reader / write* PN532.

5. Perancang Prototipe *Gate System*

Dalam sistem ini, prototipe Gate System terhubung ke server dan terdiri atas hardware dan software.



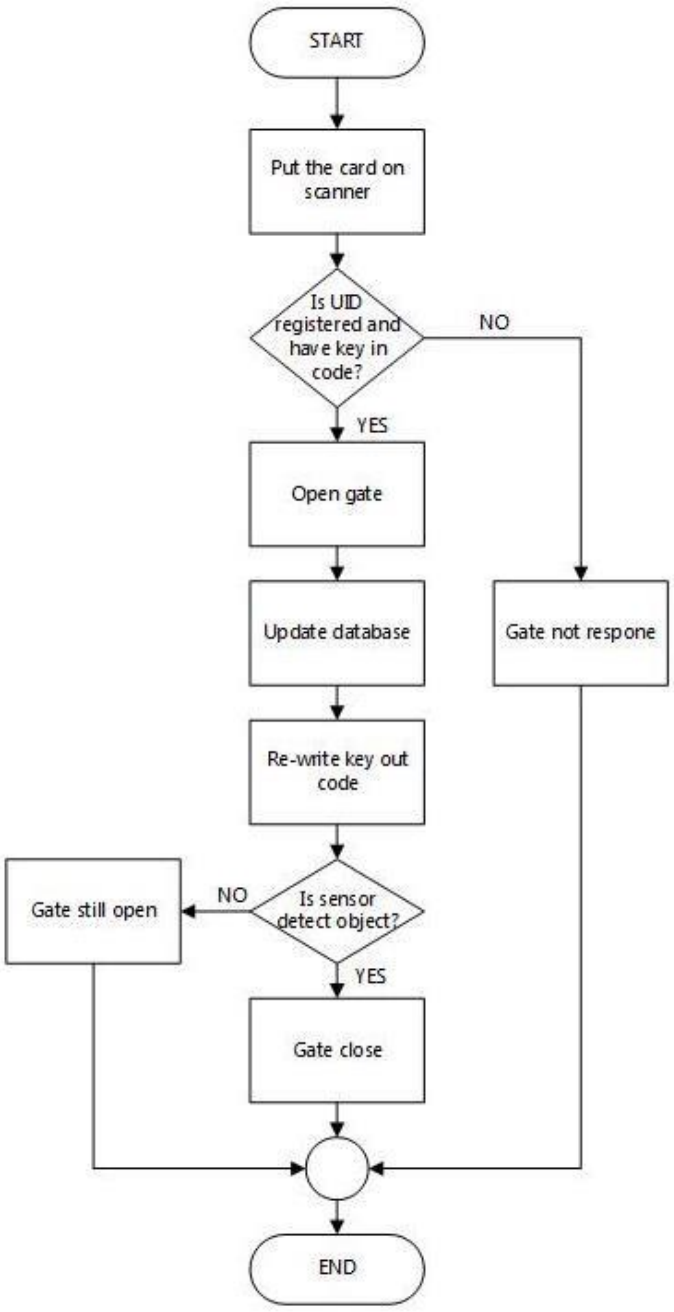
Gambar 17. Gambar Rancangan Sistem

Prototype smart gate terdiri dari PN532 NFC RFID module, mikrokontroller, NFC tag, sensor PING, motor servo, router, dan ethernet shield. Bagian lain pendukung dari smart gate access control adalah server. Server menyimpan semua data user dan riwayat akses masuk dan keluar gate. Pada prototype yang dirancang server menggunakan *localhost*.

Proses akses masuk atau keluar gate dimulai dengan mendekatkan tag pada reader untuk proses scanning/pembacaan kartu. NFC tag yang telah terregistrasi akan diidentifikasi sebagai user yang berhak untuk untuk mendapatkan akses masuk atau keluar gate. Apabila UID terdaftar dan key otentikasi telah terverifikasi maka gate akan terbuka dan riwayat user akan terupdate pada database server. Gate akan tertutup setelah sensor PING mendeteksi objek yang ada di depannya.

Pada NFC tag akan dituliskan kembali key otentikasi untuk
an kembali pada saat scanning kartu akses keluar gate. NFC tag

hanya dapat digunakan satu kali pemakaian untuk akses masuk dalam waktu bersamaan karena adanya re-write key otentikasi pada kartu. Untuk akses keluar dilakukan dengan cara yang sama.



mbar 18. Gambar Flowchart Sistem Prototipe *Smart Gate*

G. Skenario implementasi sistem

1. Sisi Pengguna

a. Pengguna melakukan pendaftaran dengan mengisi form biodata.

b. Setelah proses registrasi selesai, admin akan mengupdate informasi pada data base. Setelah data ditemukan, admin akan melakukan penulisan informasi pada kartu. Dan mengupdate UID dari pengguna kartu. Selanjutnya kartu diberikan kepada pengguna.

c. Pengguna menempelkan atau mendekatkan kartu pada perangkat prototipe. Kartu yang telah teregistrasi akan diidentifikasi sebagai user yang berhak mendapatkan akses. Setelah *gate* terbuka, informasi user akan masuk dalam riwayat akses kontrol. Setelah user melalui sensor, maka *gate* akan tertutup kembali.

2. Sisi Pengelolah

Server dimanfaatkan oleh pengelolah untuk mengetahui riwayat akses kontrol pada *gate* melalui website. Dengan demikian manajemen akses control civitas akadeimik dapat dipantau.

H. Pengujian Eksperimental

Pengujian untuk mengevaluasi performansi sistem dilakukan berbeda- beda disesuaikan dengan setiap sistem yang akan diuji secara eksperimental. Evaluasi pertama adalah registrasi user secara online dan n informasi pada kartu. Evaluasi selanjutnya adalah respon ı pada prototipe *smart gate.*

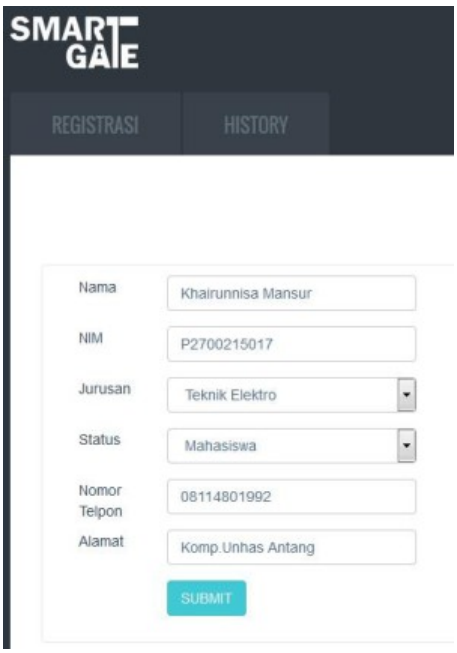
BAB IV

HASIL DAN PEMBAHASAN

Hasil perancangan akan disajikan dalam tiga bagian antara lain hasil evaluasi web dan registrasi, dan hasil evaluasi *prototype smart gate*.

1. Evaluasi Web dan Registrasi

Pertama, memastikan bahwa seorang pengguna dapat melakukan pendaftaran di administrator. Dengan identitas yang lengkap, user berhasil melakukan pendaftaran. Identitas tersimpan pada database server dan juga tersimpan dalam kartu. Gambar 19 menunjukkan user telah berhasil melakukan submit informasi.



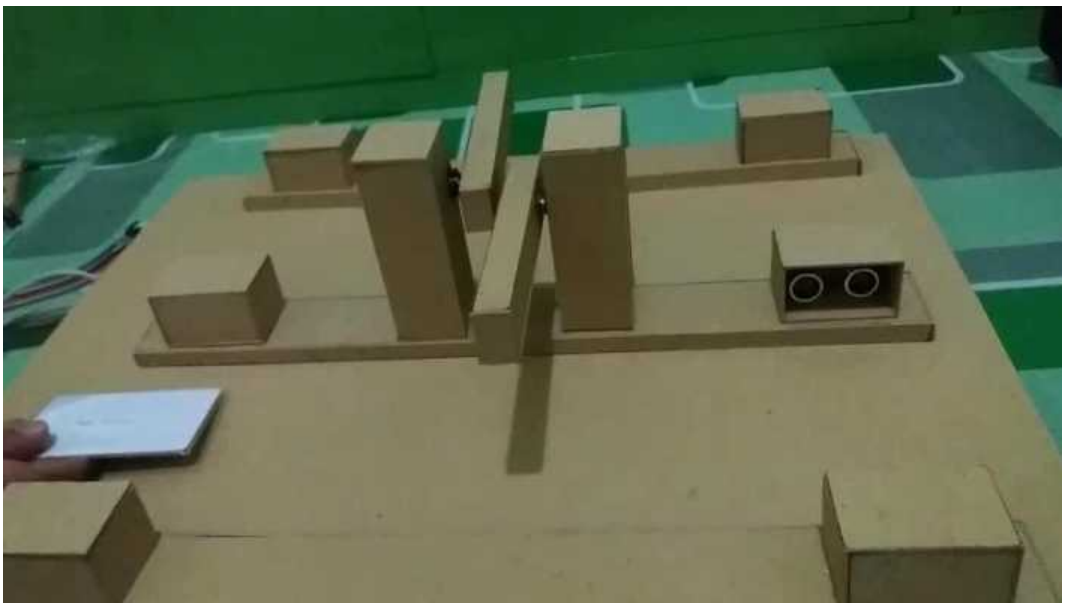
Gambar 19. Proses Input Data oleh User

Data user berhasil di submit dan akan tersimpan dalam database server. Proses selanjutnya adalah registrasi kartu oleh admin untuk memasukkan data informasi dan UID user dan memasukkan key untuk masuk atau keluar *gate*. Pada data informasi dilakukan enkripsi Caesar Chiper dan Rotate Letter, sehingga kerahasiaan informasi pengguna dapat terjaga. Gambar 20 memperlihatkan registrasi kartu oleh admin.

Gambar 20. Proses Reistrasi Kartu oleh Admin

2. Evaluasi Prototipe *Smart Gate*

Implementasi NFC pada smart gate akses kontrol telah berhasil dikembangkan dengan menggunakan mikrokontroller dan NFC tag Mifare classic IK. Gambar 21 mengggambarkan prototype system,

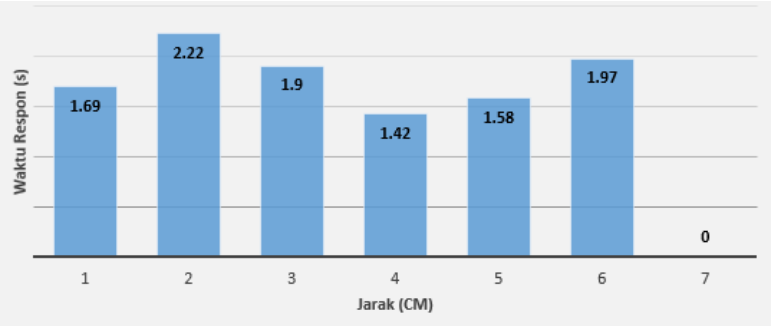


Gambar 21. Prototipe Smart Gate Acces Control

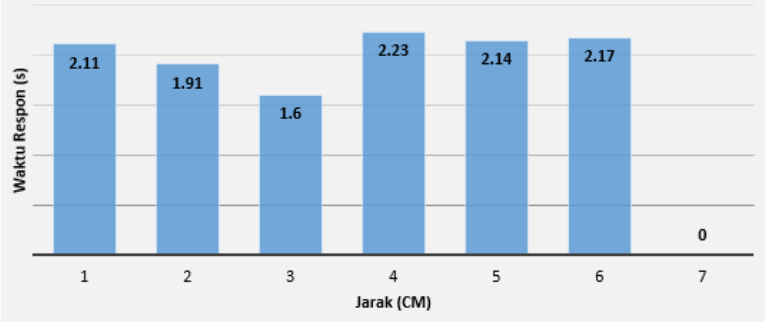
System akan bekerja apabila NFC tag sebagai Identitas didekatkan pada reader, apabila kartu user telah tergistrasi gate akan terbuka. Gate akan tertutup kembli apabila user telah melewati sensor. Jarak jangkau NFC tag yang diuji 1 cm dan 7 cm. pengujian dilakukan dengan 10 kartu secara acak.

Tabel 5. Hasil pengukuran respon waktu sistem pada kartu (gate terbuka)

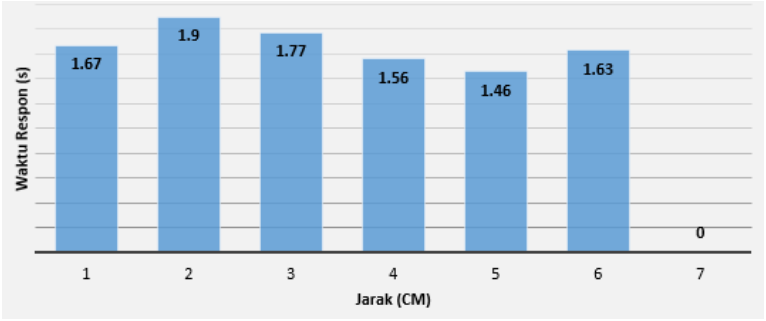
	Jarak (Cm)							Kartu
	1	2	3	4	5	6	7	
Waktu Respon (detik)	1.69	2.22	1.9	1.42	1.58	1.97	-	1
	2.11	1.91	1.6	2.23	2.14	2.17	-	2
	1.67	1.9	1.77	1.56	1.46	1.63	-	3
	1.76	1.85	2.11	1.93	2.16	1.83	-	4
	1.95	1.7	1.88	2.2	1.67	1.88	-	5
	2.18	1.97	1.76	1.66	2.1	1.67	-	6
	1.88	1.66	2.26	1.49	1.58	1.73	-	7
	1.58	1.74	1.61	2.12	1.76	1.86	-	8
	1.75	1.89	1.92	1.88	1.61	1.89	-	9
	2.07	1.91	1.93	1.68	1.72	1.66	-	10



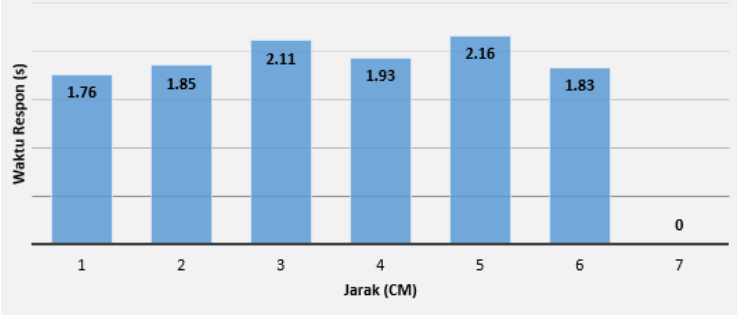
Gambar 22. Waktu respon kartu 1 terhadap jarak



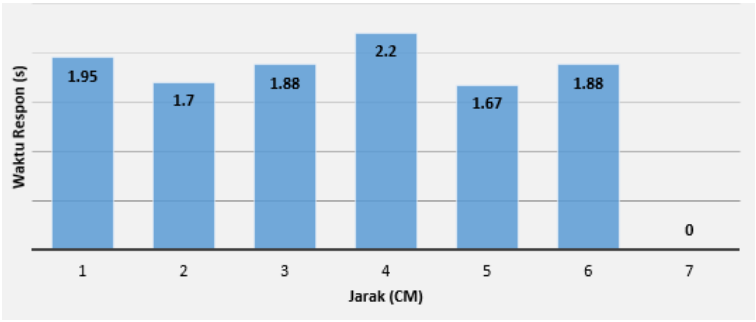
Gambar 23. Waktu respon kartu 2 terhadap jarak



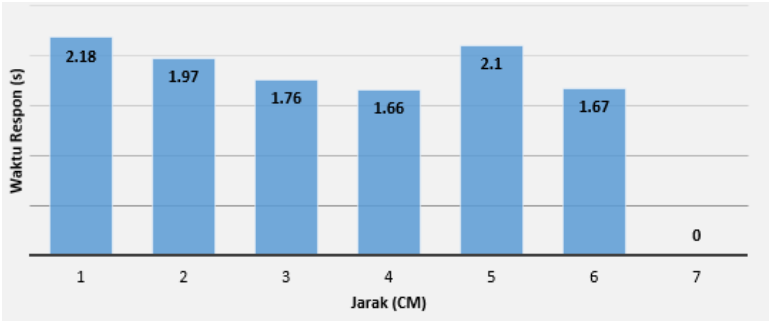
Gambar 24. Waktu respon kartu 3 terhadap jarak



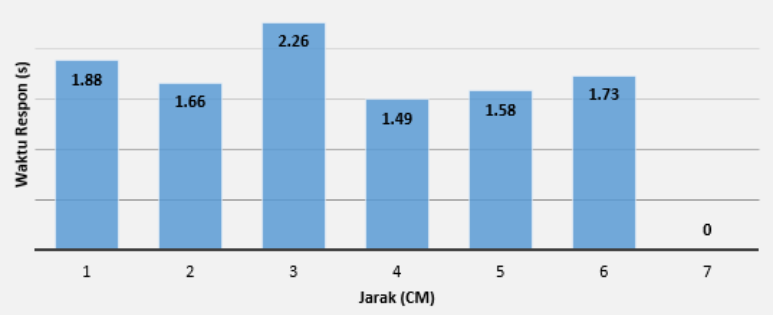
Gambar 25. Waktu respon kartu 4 terhadap jarak



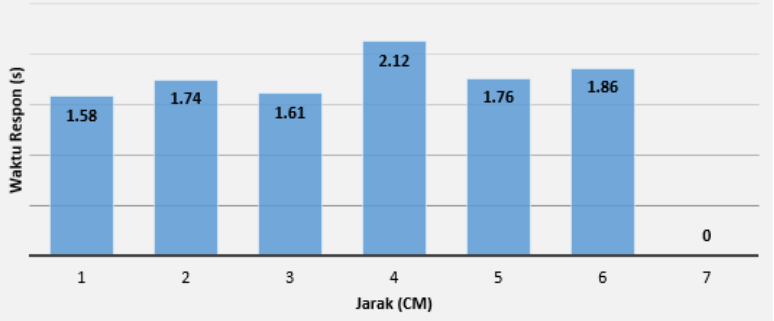
Gambar 26. Waktu respon kartu 5 terhadap jarak



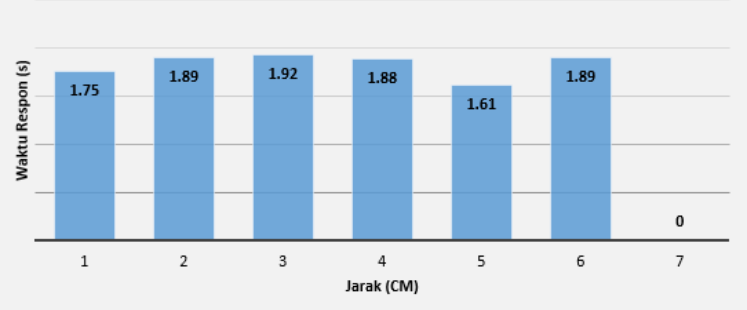
Gambar 27. Waktu respon kartu 6 terhadap jarak



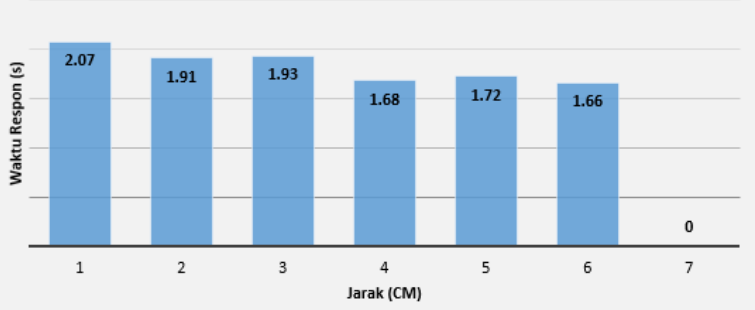
Gambar 28. Waktu respon kartu 7 terhadap jarak



Gambar 29. Waktu respon kartu 8 terhadap jarak



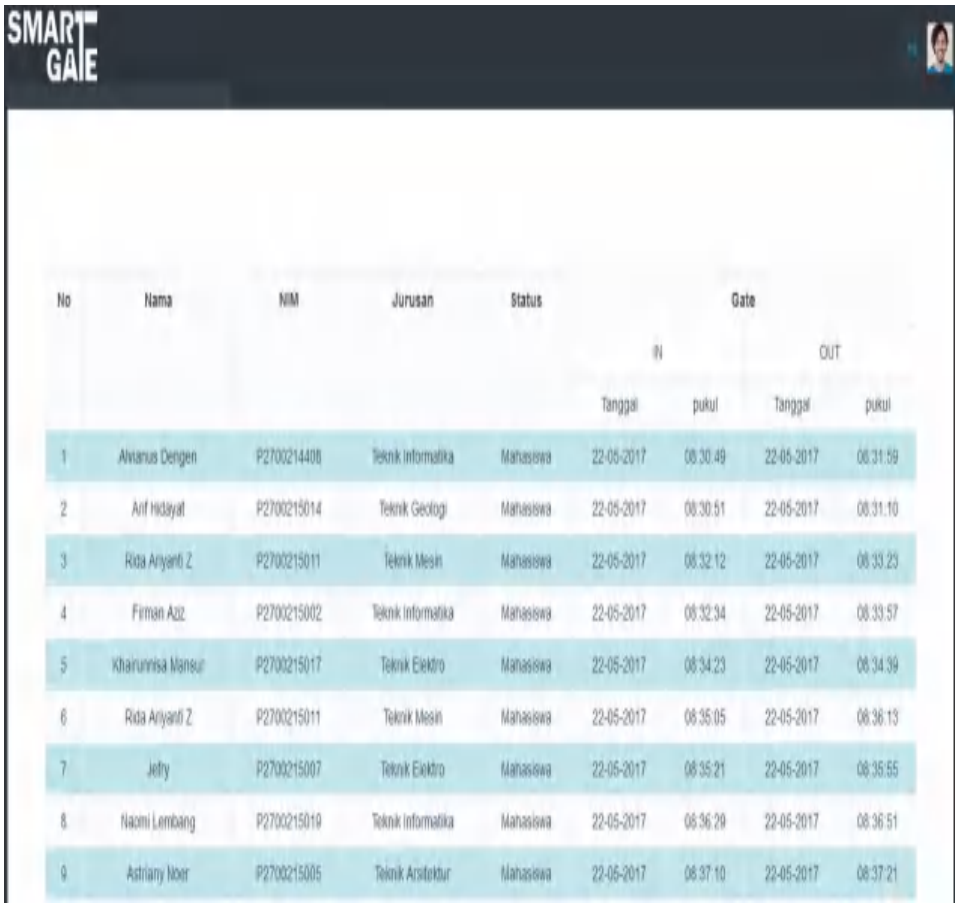
Gambar 30. Waktu respon kartu 9 terhadap jarak



Gambar 31. Waktu respon kartu 10 terhadap jarak

Gambar 32. Rata-rata waktu respon sistem terhadap jarak kartu (gate terbuka)

Respon sistem diharapkan bekerja pada jarak hingga 10 cm. Pada penelitian ini sistem dapat merespon kartu pada jarak berada 1 cm sampai 6 cm dengan respon sistem terhadap waktu pada jarak optimum 1,829 detik. Sistem melakukan proses otentikasi pada kartu saat scan kartu hingga *gate* terbuka. Hal ini menunjukkan sistem bekerja dengan mengeksekusi seluruh algoritma otentikasi. Riwayat akses masuk dan keluar gate di update pada data base dapat dilihat pada gambar 33. Kartu yang masuk hanya dapat digunakan satu kali akses. Dengan adanya riwayat akses maka keamanan akses kontrol dalam lingkungan kampus dapat kontrol.



No	Nama	NIM	Jurusan	Status	Gate			
					IN		OUT	
					Tanggal	pukul	Tanggal	pukul
1	Alvianus Dengen	P2700214408	Teknik Informatika	Mahasiswa	22-05-2017	08:30:49	22-05-2017	08:31:59
2	Arif Hidayat	P2700215014	Teknik Geologi	Mahasiswa	22-05-2017	08:30:51	22-05-2017	08:31:10
3	Rida Ariyanti Z	P2700215011	Teknik Mesin	Mahasiswa	22-05-2017	08:32:12	22-05-2017	08:33:23
4	Firman Aziz	P2700215002	Teknik Informatika	Mahasiswa	22-05-2017	08:32:34	22-05-2017	08:33:57
5	Khairunnisa Mansur	P2700215017	Teknik Elektro	Mahasiswa	22-05-2017	08:34:23	22-05-2017	08:34:39
6	Rida Ariyanti Z	P2700215011	Teknik Mesin	Mahasiswa	22-05-2017	08:35:05	22-05-2017	08:36:13
7	Jefry	P2700215007	Teknik Elektro	Mahasiswa	22-05-2017	08:35:21	22-05-2017	08:35:55
8	Naomi Lembang	P2700215019	Teknik Informatika	Mahasiswa	22-05-2017	08:36:29	22-05-2017	08:36:51
9	Astriany Noer	P2700215005	Teknik Arsitektur	Mahasiswa	22-05-2017	08:37:10	22-05-2017	08:37:21

Gambar 33. Riwayat Akses Kontrol

KESIMPULAN DAN SARAN

A. Kesimpulan

1. Akses kontrol dilakukan menggunakan NFC *card* yang telah teregistrasi. Metode yang digunakan adalah memanfaatkan UID dan key yang ditulis dan dalam kartu untuk proses otentikasi. Data informasi pribadi disimpan dengan aman dengan melakukan enkripsi pada saat registrasi kartu oleh administrator.
2. Perancangan website dapat dioperasikan oleh pengguna untuk mengisi form biodata dan administrator dalam melakukan registrasi kartu. Hasil membuktikan bahwa sistem bekerja dengan baik.
3. Respon sistem dapat bekerja hingga jarak optimum 6 cm dengan respon system terhadap waktu pada jarak optimum 1,829 detik
4. Riwayat akses masuk dan keluar *gate* di update pada database. Dengan adanya riwayat akses maka keamanan akses kontrol dalam lingkungan kampus dapat kontrol.

B. Saran

Untuk kelanjutan penelitian perbaikan dengan menggunakan spesifikasi hardware yang lebih baik. Spesifikasi *reader* / *writer* yang lebih canggih akan meningkatkan respon sistem lebih cepat. Penggunaan smart ngan kapasitas memori yang lebih besar akan memuat lebih banyak si.

DAFTAR PUSTAKA

Benyo, B. 2007. Near Field Communication Technology: Contactless Applications in Mobile Environment. *Magyar Kutatók 8. Nemzetközi Szimpóziuma 8th International Symposium of Hungarian Researchers on Computational Intelligence and Informatics,* 2007. 178-188.

Bouazzouni, M. A. *et al.* Trusted Access Control System for Smart Campus. *Proceedings Internationa*l IEEE *Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress*. 2016. 1006-1012

Du, Z. dan Yeming Tang. 2014 Web-based multi-level smart card access control system on university campus. *Proceedings of* IEEE *International Conference Software Engineering and Service Science*, 2014. 1015-1018.

Finkenzeller, K. 2010. *RFID Handbook: Fundamentals and applications in contactless smart cards, radio frequency identification*. 3th edition. Whiley. 2010.

Gerdeman, J. 2015. RFID Changing Gates. 2016 IEEE Potentials Magazine. Vol (34) Vol. 40-42.

Gruntz, D. *et al.* 2016. MOONACS: a mobile on-/offline NFC-based physical access control system. International Journal of Pervasive Computing and Communications Vol. 12 No. 1 2016. 2-22.

https://www.farnell.com/datasheets/1682209.pdf diakses 28 Juli 2017 14.00

Jacob, J. *et al.* 2015. Mobile Attendance using Near Field Communication. International Conference on Green Computing and Internet of Things (ICGCloT) 2015. 1298 - 1303.

Kao Liu, T. dan Chung-Huang Yang. 2008. Design and Implementation of Campus Gate Control System Based on RFID. Proceedings IEEE Asia-Pacific Services Computing Conference, 2008. 1406 - 1411.

Product data sheet, “MF1S50yyX_V1,” ©NXP Semiconductors N.V., 2014.

Seftyanto, D. dkk. 2012. Peran Algoritma Caesar Chiper dalam Membangun Karakter Akan Kesadaran Informasi. *Prosiding Seminar Nasional Matematika dan Pendidikan Matematika dengan tema ontribusi Pendidikan Matematika dan Matematika dalam embangun Karakter Guru dan Siswa. 2012*

ng-Long. *et al.* 2014. NFC Smart Phone based Access Control ystem. *Proceedings of the* IEEE *Conference on Open System, COS 2013. 13-17.*

Wenxing, O. et al. 2015. Implementation of Smart Shopping System Based on NFC Technology. *Proceedings of 7th International Conference Measuring Technology and Mechatronics Aotomation*, 2015. 553-555

Woo-Garcia, Rosa Ma. U. H. Lomeli-Dorantes, F.Lopez-Huerta, “Design and Implementation of a System Access Control by RFID”, International Conference Engineering Summit, II Cumbre Internacional de las Ingenierias (IE-Summit), April 2016.

LAMPIRAN

1. Listing Program Registrasi Kartu

```
#include <Wire.h>
#include <PN532_I2C.h>
#include "PN532.h"
#include <NfcAdapter.h>

PN532_I2C pn532_i2c(Wire);
PN532 nfc(pn532_i2c);
uint8_t written = 0;

void setup(void) {
  Serial.begin(9600);
  Serial.println("Hello!");

  nfc.begin();

  uint32_t versiondata = nfc.getFirmwareVersion();
  if (! versiondata) {
    Serial.print("Didn't find PN53x board");
    while (1); // halt
  }
  // Got ok data, print it out!
  Serial.print("Found chip PN5"); Serial.println((versiondata >> 24) & 0xFF, HEX);
  Serial.print("Firmware ver. "); Serial.print((versiondata >> 16) & 0xFF, DEC);
  Serial.print('.'); Serial.println((versiondata >> 8) & 0xFF, DEC);

  // configure board to read RFID tags
  nfc.SAMConfig();

  Serial.println("Waiting for an ISO14443A Card ...");
}

void loop(void)
{
 uint8_t success;                          // Flag to check if there was an error with the PN532
  uint8_t uid[] = { 0, 0, 0, 0, 0, 0, 0 };  // Buffer to store the returned UID
  uint8_t uidLength;                        // Length of the UID (4 or 7 bytes depending on ISO14443A card
type)
  uint8_t currentpage;                      // Counter to keep track of which page we're on
  bool authenticated = false;               // Flag to indicate if the sector is authenticated
  uint8_t data[4];                          // Array to store page data during reads


  uint8_t datablock[16];
  uint8_t blockn;
  // Wait for an ISO14443A type cards (Mifare, etc.).  When one is found
  // 'uid' will be populated with the UID, and uidLength will indicate
  d is 4 bytes (Mifare Classic) or 7 bytes (Mifare Ultralight)
  = nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A, uid, &uidLength);


  keya[6] = { 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF };
  ama;
```

```
    uint8_t writeBuffer1[65];
   while(Serial.available()){
  nama.toCharArray(writeBuffer1, 65);
  nama = Serial.readString() ;

   }

//---------------------------------scan uid
if(nama=="read"){
 if (success) {
   Serial.print("");
   for (uint8_t i = 0; i < uidLength; i++) {
     Serial.print(uid[i], HEX);

   }
   Serial.println("");
}
else {
 Serial.println("NFC Tag Not Found");
}
}
//-------------------



   if (nama[0]=='!')
   {

 if (success) {
   // Display some basic information about the card
```

2.Listing Program Akses Masuk Gate

```
#include <SPI.h>
#include <Ethernet.h>
#include <Wire.h>
#include <PN532_I2C.h>
#include "PN532.h"
#include <NfcAdapter.h>
#include <Servo.h>

PN532_I2C pn532_i2c(Wire);
PN532 nfc(pn532_i2c);
uint8_t written = 0;

#define LED 3
#define TRIGGER_PIN  8
#define ECHO_PIN     7
#define MAX_DISTANCE 200
```



```
= {0xDE, 0xAD, 0xBE, 0xEF, 0xFE, 0xED };

ip(192,168,27,103);
```

```
int input;
char server[] = "192.168.27.102";
int x = 0;
char dataStr[12];
char c;
int d;
String e;
int trig= 8;
int echo= 7;
long durasi, jarak;

EthernetClient client;
Servo myservo;
int pos = 70;

String uidsiswa;
String message;
String html;


void setup(void) {
  Serial.begin(9600);
  Serial.println("Looking for PN532...");

  nfc.begin();
  pinMode(LED,OUTPUT);
  myservo.attach(9);
  myservo.write(pos);
  pinMode(trig, OUTPUT);
  pinMode(echo, INPUT);

  uint32_t versiondata = nfc.getFirmwareVersion();
  if (! versiondata) {
    Serial.print("Didn't find PN53x board");
    while (1); // halt
  }
  Serial.print("Found chip PN5"); Serial.println((versiondata>>24) & 0xFF, HEX);
  Serial.print("Firmware ver. "); Serial.print((versiondata>>16) & 0xFF, DEC);
  Serial.print('.'); Serial.println((versiondata>>8) & 0xFF, DEC);
  nfc.SAMConfig();

   if (Ethernet.begin(mac) == 0) {
    Serial.println("Failed to configure Ethernet using DHCP");
    // try to congifure using IP address instead of DHCP:
    Ethernet.begin(mac, ip);
    delay(1000);}
                connect(server, 80)){
                rintln("connected");}
```

```
    uint8_t success;
    uint8_t uid[] = { 0, 0, 0, 0, 0, 0, 0 };  // Buffer to store the returned UID
    uint8_t uidLength;                        // Length of the UID (4 or 7 bytes depending on ISO14443A
card type)
    uint8_t i;
    success = nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A, uid, &uidLength);

    if (success) {
    // Display some basic information about the card
    Serial.println("Found an ISO14443A card");
    Serial.print("  UID Length: ");Serial.print(uidLength, DEC);Serial.println(" bytes");
    Serial.print("  UID Value: ");
    nfc.PrintHex(uid, uidLength);
    Serial.println("");

    //bacadatanfc();//scanning data dalam nfc

     uint8_t datalog[16];
     uint8_t keya[6] = { 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF };
     if (nfc.mifareclassic_AuthenticateBlock(uid, uidLength, 13, 0, keya))
       {
         //read memory block 0x08
         nfc.mifareclassic_ReadDataBlock(13, datalog);
         d = datalog[0];
         Serial.print("Kode Data blok13 adalah:  "); Serial.println(d);
       }

    if (client.connect(server, 80)){
    Serial.println("connected");
    //scanning datauid dalam database

    client.print("POST /cari.php?");
    client.print("search=");
    i=0;
    client.print(uid[i], HEX);
      i++;

    client.print(uid[i], HEX);
         i++;

    client.print(uid[i], HEX);
         i++;

    client.print(uid[i], HEX);

    ntln(" HTTP/1.1");
    ntln("Host: 192.168.27.102");
    ntln("Connection: close");
    ntln();
    ntln();
    0);
```

```
}

papua:
if (client.available()) {
c = client.read();
html = html + String(c);
Serial.print(c);
if ( c == '>')
 {int k = html.length();
  e = html.substring(k-2,k-1);
  Serial.print("Data yg Masuk adalah : ");
  Serial.println(e); client.stop(); }
else
  {
   goto papua;
  }

}

if ( e == "1" )
{
  if ( d == 0x00)
 {
   Serial.println("Autentikasi Data Berhasil Silahkan Masuk");
   //masukkan data kondisi masuk kedalam nfc
   uint8_t writeBuffer[16] = {0x02};
   nfc.mifareclassic_WriteDataBlock(13,writeBuffer);
   // buka gerbang
   pos = 180;
   myservo.write(pos);
   delay(1000);
   ulang:
     //============================ PING ========================//
    digitalWrite(trig, LOW);
    delayMicroseconds(8);
    digitalWrite(trig, HIGH);
    delayMicroseconds(8);
    digitalWrite(trig, LOW);
    delayMicroseconds(8);

    durasi= pulseIn(echo, HIGH);  // menerima suara ultrasonic
    jarak= (durasi/2) / 29.1;
    Serial.println(jarak);
    delay(200);
   //==========================================================//

jarak < 4 && jarak >=1)
{
 //tutup gerbang
 pos = 70;
 myservo.write(pos);
 Serial.println("Gerbang Tertutup");
```

2. Listing Program Akses Keluar Gate

```
#include <SPI.h>
#include <Ethernet.h>
#include <Wire.h>
#include <PN532_I2C.h>
#include "PN532.h"
#include <NfcAdapter.h>
#include <Servo.h>

PN532_I2C pn532_i2c(Wire);
PN532 nfc(pn532_i2c);
uint8_t written = 0;

#define LED 3
#define TRIGGER_PIN  8
#define ECHO_PIN     7
#define MAX_DISTANCE 200


byte mac[] = {0xDE, 0xAD, 0xBE, 0xEF, 0xFE, 0xED };


IPAddress ip(192,168,27,105);

int input;
char server[] = "192.168.27.102";
int x = 0;
char dataStr[12];
char c;
int d;
String e;
int trig= 8;
int echo= 7;
long durasi, jarak;

EthernetClient client;
Servo myservo;
int pos = 27;

String uidsiswa;
String message;
String html;


void setup(void) {
  Serial.begin(9600);
  Serial.println("Looking for PN532...");
  nfc.begin();
  pinMode(LED,OUTPUT);
  myservo.attach(9);
```

```
  myservo.write(pos);
  pinMode(trig, OUTPUT);
  pinMode(echo, INPUT);

  uint32_t versiondata = nfc.getFirmwareVersion();
  if (! versiondata) {
    Serial.print("Didn't find PN53x board");
    while (1); // halt
  }
  Serial.print("Found chip PN5"); Serial.println((versiondata>>24) & 0xFF, HEX);
  Serial.print("Firmware ver. "); Serial.print((versiondata>>16) & 0xFF, DEC);
  Serial.print('.'); Serial.println((versiondata>>8) & 0xFF, DEC);
  nfc.SAMConfig();

   if (Ethernet.begin(mac) == 0) {
    Serial.println("Failed to configure Ethernet using DHCP");
    // try to congifure using IP address instead of DHCP:
    Ethernet.begin(mac, ip);
    delay(1000);}
  //if (client.connect(server, 80)){
   //Serial.println("connected");}

}

void loop(){

    uint8_t success;
    uint8_t uid[] = { 0, 0, 0, 0, 0, 0, 0 };  // Buffer to store the returned UID
    uint8_t uidLength;                        // Length of the UID (4 or 7 bytes depending on ISO14443A
card type)
    uint8_t i;
    success = nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A, uid, &uidLength);

    if (success) {
    // Display some basic information about the card
    Serial.println("Found an ISO14443A card");
    Serial.print("  UID Length: ");Serial.print(uidLength, DEC);Serial.println(" bytes");
    Serial.print("  UID Value: ");
    nfc.PrintHex(uid, uidLength);
    Serial.println("");

    //bacadatanfc();//scanning data dalam nfc

     uint8_t datalog[16];
     uint8_t keya[6] = { 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF };
     if (nfc.mifareclassic_AuthenticateBlock(uid, uidLength, 13, 0, keya))

                d memory block 0x08
               ifareclassic_ReadDataBlock(13, datalog);
               latalog[0];
               l.print("Kode Data blok13 adalah:  "); Serial.println(d);
```

```
 if (client.connect(server, 80)){
Serial.println("connected");
 //scanning datauid dalam database

 client.print("POST /cari.php?");
 client.print("search=");
 i=0;
 client.print(uid[i], HEX);
   i++;

 client.print(uid[i], HEX);
       i++;

 client.print(uid[i], HEX);
       i++;

 client.print(uid[i], HEX);

 client.println(" HTTP/1.1");
 client.println("Host: 192.168.27.102");
 client.println("Connection: close");
 client.println();
 client.println();
 delay(500);
 }

 papua:
 if (client.available()) {
 c = client.read();
 html = html + String(c);
 Serial.print(c);
 if ( c == '>')
  {int k = html.length();
   e = html.substring(k-2,k-1);
   Serial.print("Data yg Masuk adalah : ");
   Serial.println(e); client.stop(); }
 else
   {
    goto papua;
   }

 }

 if ( e == "1" )
 {
                 = 0x02)

                 println("Autentikasi Data Berhasil Selamat Jalan");
                 kkan data kondisi masuk kedalam nfc
                  writeBuffer[16] = {0x00};
                 areclassic_WriteDataBlock(13,writeBuffer);
```

```
// buka gerbang
pos = 108;
myservo.write(pos);
delay(1000);
ulang:
  //============================ PING ========================//
 digitalWrite(trig, LOW);
 delayMicroseconds(8);
 digitalWrite(trig, HIGH);
 delayMicroseconds(8);
 digitalWrite(trig, LOW);
 delayMicroseconds(8);

 durasi= pulseIn(echo, HIGH);  // menerima suara ultrasonic
 jarak= (durasi/2) / 29.1;
 Serial.println(jarak);
 delay(500);
//=========================================================//

     if ( jarak < 4 && jarak >=1)
        {
          //tutup gerbang
          pos = 27;
          myservo.write(pos);

          Serial.println("Gerbang Tertutup");
         }
```