Sistem Akses Pintu Menggunakan e-KTP Sebagai Kunci Elektronik Berbasis *Near Field Communication* Dimonitor Melalui Jaringan Komputer

Sarono Widodo[1], Ghassan Z.Sasmita[2], Lutfia N.Sari[3], Abu Hasan[4]

[1,2,3,4] *Teknik Telekomunkasi, Politeknik Negeri Semarang, Jl.Prof.Sudarto,S.H.Tembalang, Semarang, 50275*
E-mail: sarwede@gmail.com

Abstrak* — *Radio Frequency Indentification* (RFID)*card*, sidik jari, pendeteksi wajah atau tombol *key pad* telah banyak digunakan sebagai sistem pengaman pintu pada ruang kantor pribadi, kamar hotel, brankas dan lain sebagainya. Salah satu inovasi teknologi adalah memanfaatkan e-KTP sebagai kunci elektronik pembuka pintu. E-KTP termasuk dalam jenis *smartcard* yang berisi Nomor Induk Kependudukan (NIK) sebagai identitas tunggal setiap penduduk dan berlaku seumur hidup. Dengan memanfaatkan *Near Field Communication* (NFC) *shield* sebagai *reader e*-KTP (13.56 MHz) dan identifikasi sidik jari menggunakan FPM10a yang terhubung pada mikrokontroler Arduino Mega 2560 digunakan untuk mengontrol solenoid sebagai kunci elektronik . Setiap mikrokontroler didukung oleh *ethernet sield* yang memiliki alamat IP untuk dapat terhubung ke monitor *server* melalui jaringan komputer. Monitor *server* berisi *database* berfungsi untuk menyimpan data *user* dan riwayat *user* yang mengakses pintu. Pembacaan *Unique Identification* (UID) e-KTP oleh NFC efektif pada jarak maksimal 4 cm. Setiap user yang memiliki hak akses untuk membuka pintu harus mendaftarakan e-KTP dan sidik jari sehingga tercatat dalam sistem *database server*. Akses membuka pintu dilakukan dengan tahapan pembacaan UID dan identifikasi sidik jari pemilik yang terdaftar dalam *database* yang selanjutnya diolah oleh mikrokontroler untuk mengatifkan solenoid. Akses keluar dilakukan dengan menggunakan tombol exit. Dengan menggunakan sistem jaringan komputer akan memudahkan pemantauan seluruh aktivitas akses ke semua pintu secara *real time* hanya dengan monitor *server* tunggal. Penggunaan e-KTP sebagai kunci elektronik dan pengamanan dengan *fingerprint* secara teknis menjadikan sistem akses pintu tidak mudah untuk dibuka oleh orang lain.

***Kata Kunci* — *kunci elektronik, e-KTP, NFCshield, sidik jari, Arduino Mega 2560, monitor server*.**

I. PENDAHULUAN

Sesuai dengan fungsinya, pintu sangat dibutuhkan sebagai perantara atau media penghubung sehingga membutuhkan sistem keamanan yang baik untuk menghindari upaya pencurian.Sistem keamanan yang dipasang pada setiap pintu memiliki perbedaan, tergantung dari fungsi ruangan. Ruangan yang membutuhkan keamanan yang cukup ketat yang membatasi hak akses ruangan tersebut seperti ruangan direktur atau ruangan *server* yang tidak sembarang orang dapat memasuki ruangan tersebut. Salah satu cara membangun sistem keamanan ruangan yang baik yaitu mengganti jenis kunci pintu yang masih manual (kunci mekanik) dengan kunci elektronik seperti menggunakan kata sandi atau kode, remote control, sidik jari, *smartcard* atau dengan deteksi wajah.

Beberapa sistem akses untuk membuka pintu telah dibuat. Seperti sistem pengamanan rumah menggunakan teknologi identifikasi sidik jari menggunakan modul *fingerprint* FPM10a yang dilengkapi dengan tampilan LCD dan sistem *database* sebagai penyimpanan riwayat akses [1].

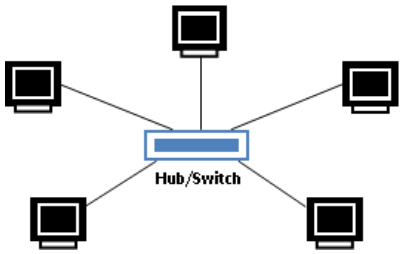
E-KTP termasuk dalam jenis kartu pintar (*smartcard*) yang dapat dimanfaatkan sebagai token akses dan berfungsi sebagai anak kunci elektronik. Dengan memanfaatkan teknologi mikrokontroler, *Near Field Communication* (NFC) *shield* sebagai pembaca e-KTP dan perangkat pembaca sidik jari sebagai pengidentifikasi pemilik e-KTP, maka secara elektronik pintu dapat diakses. Sistem akses menggunakan pembacaan e-KTP telah dibuat dengan memanfaatkan penyimpanan SD *card* untuk menyimpan UID e-KTP dan riwayat akses masuk. Sistem pengiriman data dan pencocokan UID e-KTP menggunakan komunikasi UART Xbee [2]. Sistem akses menggunakan e-KTP dan modul fingerprint FPM10a terus dikembangkan dengan menambahkan *server* sebagai pemantau aktivitas akses pintu. Sistem akses dengan Mikrokontroler yang terpasang pada pintu dilengkapi dengan *Ethernet shield* untuk terhubung langsung ke komputer *server* . Sistem monitoring yang dilakukan masih bersifat tunggal yaitu setiap perangkat pintu harus dilengkapi dengan komputer sebagai pemantau akses[3]. Penelitian ini mengembangkan model monitoring tunggal menjadi multi monitoring dengan sebuah monitor *server* melalui jaringan komputer. Setiap perangkat akses pintu yang terpasang pada pintu berfungsi sebagai *node*. Dibutuhkan sebuah perangkat *switch* yang berfungsi sebagai konsentrator dalam jaringan komputer.

II. LANDASAN TEORI

A. *Jaringan Komputer*

Jaringan komputer dalam skala terbatas disebut dengan *Local Area Network* (LAN) adalah suatu jaringan yang berisi sejumlah sistem komputer yang lokasinya terbatas di dalam suatu gedung atau kompleks. LAN merupakan jaringan komputer yang mendukung dalam sistem komunikasi data dan mampu untuk melakukan integrasi data, sehingga sistem koleksi data yang dilakukan secara manual atau *offline* tidak dibutuhkan lagi[4].

LAN mendukung *sharing* data dan sumber daya kepada setiap klien yang terhubung pada jaringan tersebut. Pada umumnya sebuah jaringan lokal memiliki sekurang-kurangnya sebuah *server* sebagai pusat data untuk melayani kebutuhan klien (*workstation*). Salah satu topologi yang digunakan dalam jaringan komputer adalah topologi *star* seperti ditunjukkan pada Gambar 1. Jaringan dengan topologi *star* didukung dengan teknologi *Ethernet*.



Gambar 1. Topologi *star*

B. *KTP Elektronik (e-KTP)*

KTP Elektronik adalah dokumen kependudukan dengan sistem keamanan / pengendalian administrasi ataupun teknologi informasi dalam sistem *database* kependudukan nasional. Setiap penduduk hanya memiliki satu KTP yang tercantum dalam Nomor Induk Kependudukan (NIK)[5].

Gambar 2. Contoh e-KTP dengan *contactless chip* di dalamnya

Teknologi Chip e-KTP berbasis mikroprosesor memiliki memori berkapasitas 8 kilo *byte*, dengan antar muka *contactless* dan memiliki metoda pengamanan data berupa autentikasi anti *cloning*, enkripsi data serta tanda tangan digital. Antar muka chip e-KTP memenuhi standar ISO 14443 A atau ISO 14443 B. Chip dapat dibaca oleh perangkat pembaca kartu (*card reader*) yang memiliki standar ISO 14443 A dan ISO 14443 B[6].

C. *Near Field Communication (NFC)*

Near Field Communication (NFC) merupakan salah satu teknologi komunikasi nirkabel terbaru popular adalah teknologi komunikasi nirkabel berdaya rendah yang memungkinkan perangkat elektronik untuk berkomunikasi pada jarak sangat dekat atau dengan menyentuhnya (*tap-in*). Komunikasi tersebut dapat dilakukan antara dua perangkat aktif atau dilakukan antara perangkat NFC dengan sebuah *tag* pasif.Kedua perangkat tidak boleh melebihi jarak 10 cm dan untuk komunikasi yang stabil kurang dari 4 cm. NFC adalah bagian dari *Radio Frequency Identification* (RFID) dengan lebih pendekjangkauan komunikasi untuk tujuan keamanan ([7],[8],[9]).

Protokol NFC atau disebut dengan *Near Field Communication Interface and Protocol* (NFCIP-1) mendefinisikan dua mode komunikasi (aktif dan pasif), skema modulasi, pengkodean bit, kecepatan transfer dan parameter lainnya yang diperlukan untuk komunikasi antar perangkat NFCIP-1. Anatar muka NFC beroperasi pada frekuensi 13,56 MHz dengan kecepatan transfer antar dua perangkat NFCIP-1 yaitu 106, 212 dan 424 kbps.

NFC beroperasi dalam tiga mode, yang masing-masing dapat digunakan untuk aplikasi yang berbeda. Ketiga mode tersebut adalah *reader/writer*, *peer-to-peer*, dan *card emulation*.Pada mode *reader/writer*, perangkat NFC dapat membaca data dari tag pasif atau memodifikasi isinya.Pertukaran data dapat dilakukan oleh perangkat NFC setelah dua perangkat terhubung dalam mode *peer-to-peer*.Mode*card emulation* memungkinkan perangkat NFC untuk bertindak sebagai *contactless smart card*.NFC Forum menetapkan empat format tag yang didasarkan pada standar *contactless smart card* ISO 14443 A / B dan Felica [10].

D. *RFID/NFC/PN532 Shield IC Card Expansion Boards*

RFID/NFC/PN532 shield adalah NFC *Shield*untuk Arduino ditunjukkan seperti pada Gambar 3. Eduino PN532 populer untuk penggunaan setiap RFID 13.56MHz atau aplikasi NFC. Eduino NFC menggunakan PN532 chip set untuk membaca dan menulis ke *tag*.Eduino NFC / RFID PN532 menangani komunikasi *contactless* pada frekuensi 13.56MHz dengan antena*stripline*dan didukung dengan 36-pin 0,1 " untuk dapat terpasang pada arduino [11].

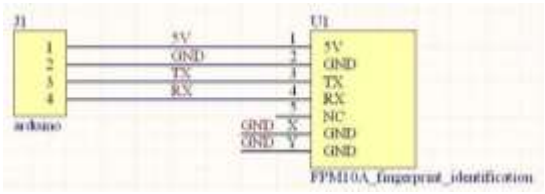
Gambar 3. RFID/NFC PN532*Shield*

E. *Modul Sensor Sidik Jari FPM10a*

Sensor sidik jari optik FPM10a pada Gambar 4 memiliki berbagai fungsi yaitu pendaftaran sidik jari hingga 162 sidik jari yang tersimpan ke dalam memori flash onboard dan pencocokan sidik jari [12].

Gambar 4. Modul sensor sidik jari FPM10a

Modul cukup dikoneksikan ke mikrokontroler menggunakan komunikasi serial (*serial port*) seperti ditunjukkan Gambar 5 atau sistem dengan TTL serial, dan mengirim paket data untuk mengambil foto, mendeteksi sidik jari [13].



Gambar 5. Skema hubungan FPM10A dengan Mikrokontroler

F. *Mikrokontroler Arduino Mega 2560*

Arduino Mega 2560 adalah *board* mikrokontroler berbasis ATmega2560 memiliki 54 pin digital input/output, 15 pin digunakan sebagai output PWM, 16 pin input analog, 4 UART (*serial port*), dilengkapi dengan *oscillator* 16 MHz, koneksi USB, jack catu daya eksternal, ICSP *header*, dan tombol reset. Untuk memulai menggunakan *board* Arduino cukup sederhana hanya dengan menghubungkan ke komputer dengan kabel USB. Bentuk fisik Arduino Mega 2560 ditunjukkan pada Gambar 6[14].

Gambar 6. Bentuk fisik Arduino/ Genuino Mega 2560

G. *Arduino Ethernet Shield*

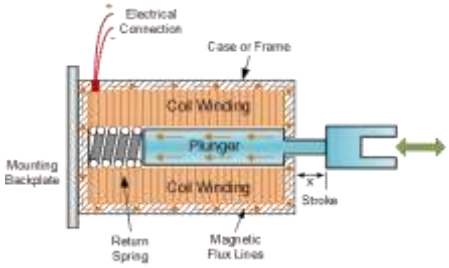
Arduino Ethernet Shield merupakan modul dengan *chip* Wiznet W5100 yang memungkinkan sebuah *board* Arduino untuk terhubung ke internet atau jaringan LAN/*Ethernet* (jaringan lain yang mendukung protokol TCP/IP atau UDP). Untuk menghubungkan *ethernet shield* dengan komputer, *hub/switch*, atau *router* menggunakan kabel *ethernet* standar (CAT5 atau CAT6 dengan konektor RJ45). *Ethernet Shield* yang dipasang pada *board* Arduino membutuhkan *input* tegangan 5V yang dapat diperoleh dari *board* Arduino, pin 5V. Spesifikasi *Ethernet Controller* yaitu *chip* Wiznet W5100 dengan *internal buffer* 16 kb, kecepatan koneksi 10/100 Mb. *Ethernet shield* ini terhubung dengan Arduino melalui *port* SPI. *Ethernet Shield* juga tersedia slot kartu micro-SD yang dapat digunakan untuk menyimpan file untuk melayani melalui jaringan. Hal ini kompatibel dengan semua *board* Arduino / Genuino. Bentuk fisik *Ethernet Shield* ditunjukkan pada Gambar 7 [15].

Gambar 7. Bentuk fisik *Ethernet Shield R3*

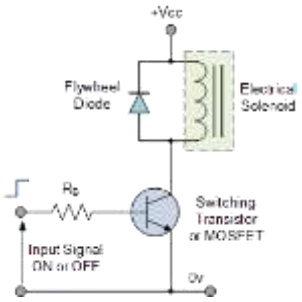
H. *Solenoid Door Lock*

Solenoid merupakan sebuah elektromagnetik yang dirancang khusus. Sebuah solenoid biasanya terdiri dari sebuah kumparan dan inti besi bergerak disebut angker. Solenoid yang murah biasanya digunakan terutama terbatas pada aplikasi *on-off* seperti menempel, mengunci, dan memicu [16]. Tipe lain dari aktuator elektromagnetik adalah solenoid linear, yaitu perangkat elektromagnetik yang mengubah energi listrik menjadi energi gerak. Energi gerak yang dihasilkan berupa mendorong atau menarik kekuatan mekanik.

Di dalam solenoid terdapat kawat melingkar (gulungan kumparan) pada inti besi. Ketika arus listrik melewati gulungan kumparan, maka terjadi medan magnet yang menghasilkan gerakan linier yang mendorong atau menarik piston/silinder yang terbuat dari besi yang disebut *plunger*. Solenoid linear memiliki prinsip dasar yang sama seperti relay elektromekanis dan juga dapat diaktifkan dan dikendalikan menggunakan transistor atau MOSFET[17]. Gambar 8 dan 9 menunjukkan konstruki solenoid linear dan contoh rangkaian pengendali.



Gambar 8. Konstruksi solenoid linear



Gambar 9. Contoh rangkaian pengendali solenid

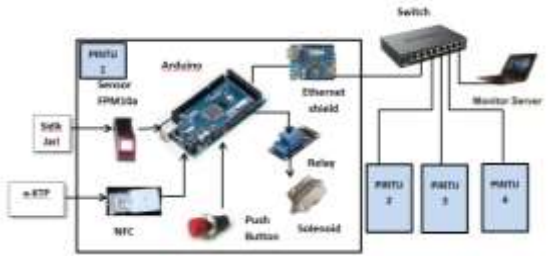
III. METODE PENELITIAN

Penelitian ini merupakan sebuah rancang bangun dengan tahapan penelitian sebagai berikut:

- Perancangan sistem
- Pembuatan sistem
- Pengujian sistem

A. *Perancangan Sistem*

Sistem ini dirancang untuk empat pintu yang berfungsi sebagai *node*dalam sistem jaringan komputer. Setiap pintu dilengkapi dengan sebuah NFC *shield*, modul sensor *fingerprint* FPM10a, Arduino Mega 2560, *Ethernet shield*, dan *solenoid door lock* terhubung ke server monitor menggunakan kabel *twisted pair* cat5e dan sebuah perangkat *switch*. Gambar 10 menunjukkan sistem rancangan *hardware*.



Gambar 10. Rancangan *hardware* sistem

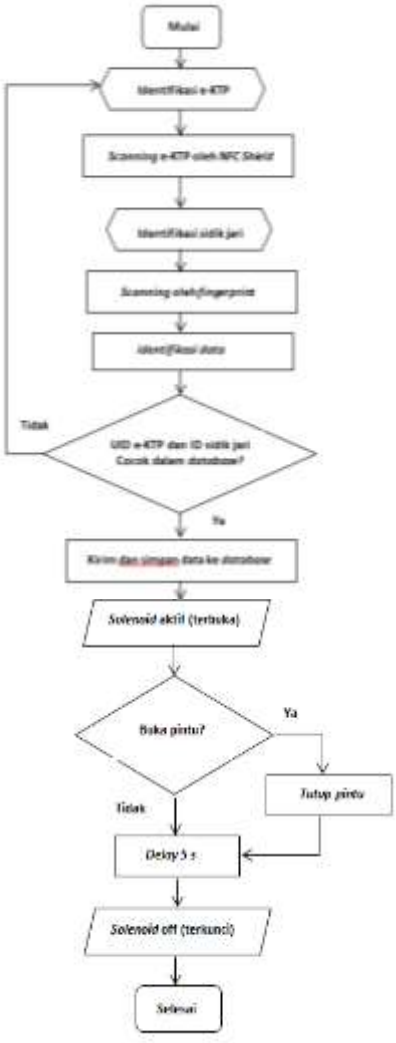
Perancangan *software* meliputi pembuatan *database* monitoring dan program arduino untuk mendeteksi e-KTP, alamat IP dari *Ethernet shield* dan sebagai fungsi pendataan/pendaftaran *user*.

Bagian *software* Arduino meliputi *Integrated Development Environment (IDE)* yang digunakan untuk penulisan program.IDE Arduino adalah *software* yang digunakan untuk membuat program pada mikrokontroler Arduino. *Software* Arduino yang akan digunakan adalah *driver* dan IDE. Bahasa pemrograman yang digunakan oleh IDE Arduino untuk membuat program adalah bahasa C++ dan Java yang telah dipermudah melalui *library*. Untuk membangun web dan *database* sistem akses dan monitoring dibutuhkan *software* XAMPP. XAMPP digunakan karena *open source* dan *software* ini memiliki kelebihan yang di dalamnya telah dilengkapi dengan program Apache HTTP Server, MySQL database, PHP, Perl ([18],[19]).

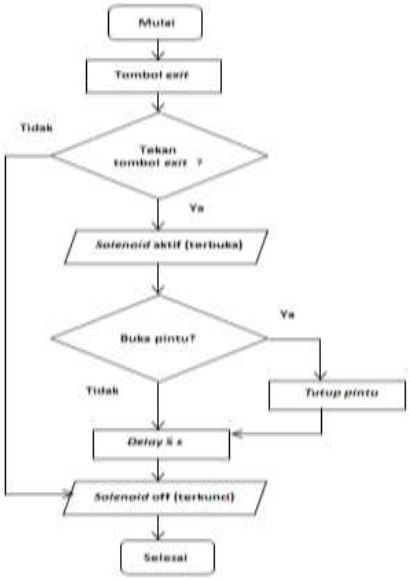
Rancangan alur operasi untuk akses masuk dan akses keluar dalam sistem ini seperti ditunjukkan pada Gambar 11 dan 12. Sistem jaringan pintu elektronik ini terbagi menjadi dua, yaitu akses masuk dan akses keluar.

Untuk akses masuk di identifikasi melalu *scanning* UID *e*-KTP dan identifikasi sidik jari. Untuk identifikasi *e*-KTP di lakukan oleh NFC *shield* sedangkan untuk identifikasi sidik jari di lakukan oleh modul sensor *fingerprint* FPM10a. Hasil identifikasi dari NFC *shield* dan juga modul sensor *fingerprint* FPM10a akan diolah Arduino Mega 2560 dan *output* untuk mengaktifkan *solenoid doorlock*.

Apabila pengakses pintu adalah salah satu dari daftar hak akses (pemilik e-KTP) yang terdapat dalam *database*, maka identifikasi akan diterima dan *solenoid* akan aktif dan kunci pada pintu akan terbuka. Hasil identifikasi yang yang berhasil akan tersimpan dalam sistem *database* riwayat akses melalui *Ethernet shield* dalam jaringan komputer. Untuk akses keluar hanya dengan menekan tombol *exit bottom* yang terpasang pada pilar pintu dalam.

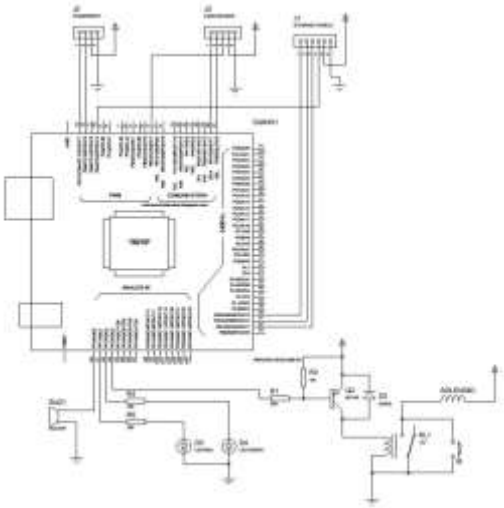


Gambar 11. Alur identifikasi masuk dan pengaktifan solenoid



Gambar 12. Alur akses keluar

Rancangan rangkaian *hardware* sistem seperti ditunjukkan pada Gambar 13. Rangkaian sistem akses kontrol pintu elektronik menggunakan sumber tegangan *power supply* 12 Volt 5 Ampere. *Board* Arduino terhubung dengan *Ethernet Shield* lewat pin 50,51,52 dan 10, sedangkan NFC *Shield* terhubung dengan *board* Arduino lewat pin SDA, SCL dan pin 2. Sensor *fingerprint* FPM10a, modul *relay*, LED, *buzzer*, tombol *Exit*, dan *solenoid* terhubung dengan Aduino menggunakan kabel *jumper*. *Ethernet Shield* terhubung dengan monitor *server* menggunakan kabel UTP *straight* melalui *switch*.



Gambar 13. Rancangan rangkaian *hardware* sistem

B. *Pembuatan Sistem*

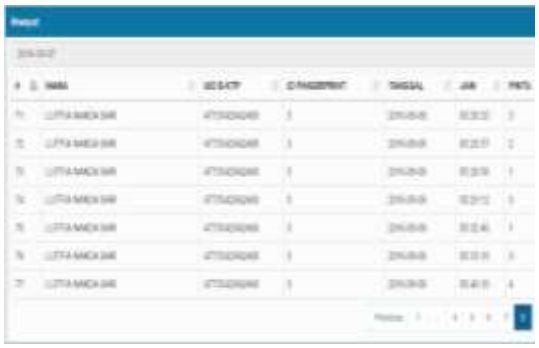
Pembuatan sistem meliputi *hardware* sistem, pintu peraga dan *software* aplikasi untuk identifikasi dan monitoring. Pembuatan rancang bangun pintu digunakan sebagai tempat pemasangan *hardware* sistem dan media pengujian sistem.Bahan yang digunakan dalam pembuatan rancang bangun pintu terbuat dari alumunium seperti ditunjukkan pada Gambar 14. Rancang bangun pintu sebagai peraga terdiri atas empat pintu tersambung yang masing-masing pintu berfungsi sebagai node dalam jaringan komputer. Setiap pintu dipasang *harware* sistem yang dapat terhubung pada jaringan komputer melalui sebuah *switch* dan kabel UTP. Kemasan *hardware* sistem seperti pada Gambar 15 menggunakan kotak plastik. Modul *fingerprint* diletakkan secara terpisah untuk memudahkan identifikasi sidik jari dan pendaftaran pengguna. Instalasi pengkabelan diletakkan di bagian dalam dari kusen alumunium pintu dan ditutup dengan alumunium. Penataan kabel dalam kerangka pintu agar instalasi pengkabelan menjadi rapi dan tidak mudah rusak atau mengganggu.

Gambar 14. Rancang bangun pintu sebagai peraga

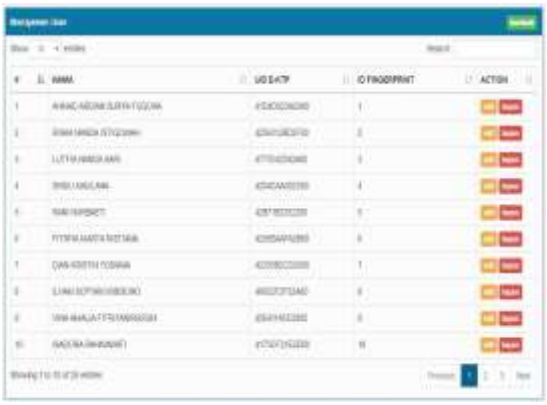
Gambar 15. Kemasan dan pemasangan *hardware* sistem

Diantara tampilan web dari sistem akses kontrol pintu elektronik ditunjukkan pada adalah "Riwayat user" dan "Data User" seperti ditunjukkan pada Gambar 16 dan 17. Riwayat *user* adalah halaman yang berfungsi untuk menampilkan data riwayat akses masuk oleh pengguna yang terdaftar dalam sistem *database*. Pada tampilan Riwayat user menampilkan nama, *Unique Identification* (UID) e-KTP, ID *fingerprint*, tanggal dan jam dari pengguna yang mengakses pintu.

Data *user* merupakan halaman yang berfungsi untuk menampilkan data yang memiliki hak akses masuk pintu elektronik. Tampilan "Data *User*" terdiri dari nama, UID (*Unique Identification*) E-KTP, ID *fingerprint*, dan *Action*. Di *Action* terdapat tombol *edit* untuk mengubah atau mengedit *user* dan hapus untuk menghapus *user*.



Gambar 16. Contoh Tampilan riwayat *user* pengakses pintu



Gambar 17. Data *User*

C. *Pengujian Sistem dan Pembahasan*

1) Pembacaan UID (Unique Identification) e-KTP oleh NFC Shield

Pengujian NFC*Shield* untuk pembacaan UID e-KTP dilakukan dengan cara mendekatkan *e*-KTP ke NFC *Shield* yang telah tersambung Arduino. Pengujian dan pengamatan dengan menggunakan laptop yang telah tersambung pada arduino. Pada pengujian pembacaan UID *e*-KTP ditandai dengan terbaca nomor UID eKTP pada *serial monitor* IDE Arduino.

Gambar 18. Pembacaan UID e-KTP menggunakan NFC *shield*

Hasil pengujian UID e-KTP telah berhasil terbaca dengan nomor '47735425A2A80' seperti ditunjukkan pada Gambar 18. Nomor ini bersifat uniq karena di setiap e-KTP hanya memiliki satu nomor. Dengan hasil pengujian ini menunjukkan bahwa penggunaan e-KTP sebagai kunci elektronik hanya dapat diberikan kepada pemilik hak akses pintu. Jika dalam suatu ruangan ditempati lebih dari satu orang maka setiap orang harus mendaftarkan e-KTP nya agar dapat teridentifikasi oleh *NFC shield.* Dengan terbacanya UID e-KTP maka *buzzer* berbunyi yang mengindikasikan bahwa *chip* dari *e*-KTP terdeteksi.

2) Pengukuran Jarak Baca NFC Shield Terhadap e-KTP

Pengukuran jarak baca NFC *Shield* terhadap e-KTP bertujuan untuk mengetahui jarak baca maksimal dari NFC *Shield* dalam mendeteksi e-KTP. Cara Mengukur jarak baca NFC *Shield* terhadap e-KTP menggunakan sebuah mistar seperti ditunjukkan pada Gambar 19. Hasil pengukuran ditunjukkan pada Tabel I.

Gambar 19. Pengukuran jarak baca e-KTP oleh NFC*Shield*

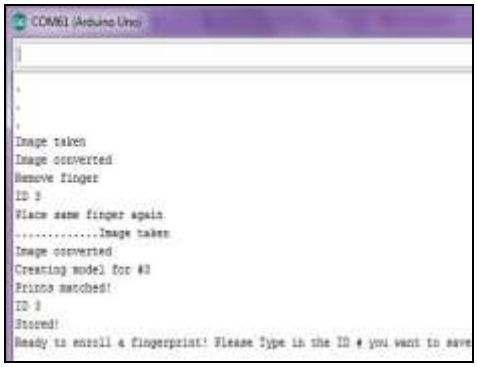
Table I
Hasilpengukuran Jarak Baca E-Ktp Oleh Nfc Shield

No	Jarak Baca (cm)	Keterangan
1	0	Terbaca
2	1	Terbaca
3	2	Terbaca
4	3	Terbaca
5	4	Terbaca
6	5	Tidak terbaca

Berdasarkan hasil pembacaan dari NFC *Shield* dalam mendeteksi *e*-KTP menunjukkan bahwa jarak optimum adalah 0cm sampai 4cm. Hal ini menunjukan bahwa akses pintu hanya dapat dilakukan ketika pemilik hak akses mendekatkan e-KTP nya pada kisaran jarak yang telah diujikan. Pada saat *e*-KTP di tag pada NFC *Shield buzzer* akan berbunyi yang menyatakan bahwa *e*-KTP terdeteksi oleh NFC *Shield*.

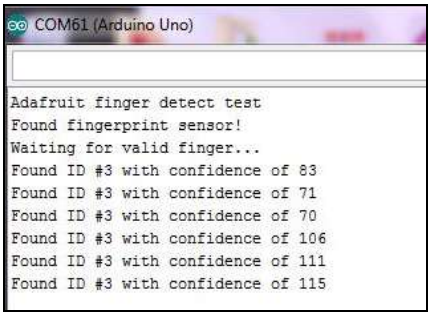
3) Proses Pendaftaran dan Pengujian Sidik Jari Dengan Sensor Fingerprint FPM10a

Proses pendaftaran (*enroll*) sidik jari bertujuan untuk menyimpan data sidik jari pada memori perangkat sensor *fingerprint* FPM10a. Proses pendaftaran sidik jari dilakukan dengan *scanning* sidik jari pada sensor *fingerprint* sebanyak dua kali. Hasil pendaftaran sidik jari dapat dilihat pada serial monitor IDE Arduino seperti ditunjukkan pada Gambar 20.



Gambar 20. Proses pendaftaran berhasil

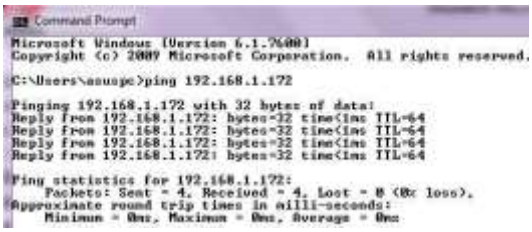
Setiap sidik jari yang didaftarkan akan tersimpan pada memori modul FPM10a. Proses pencocokan data sidik jari yang telah tersimpan dilakukan dengan proses *fingerprint* dan semua yang telah didaftar akan ditampilkan seperti pada Gambar 21.



Gambar 21. Proses pencocokan data sidik jari yang tersimpan

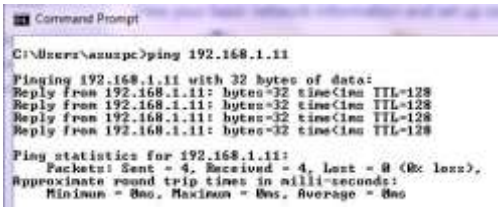
4) Pengujian Pengiriman Data Pada Sistem Jaringan Komputer

Pengujian pengiriman data yang dilakukan pada sistem jaringan komputer untuk memastikan bahwa *hardware* sistem (modul sistem kunci elektronik) telah terkoneksi ke jaringan komputer dan bekerja dengan baik. Setiap modul *hardware* sistem yang terasang pada setiap pintu berfungsi sebagai *node* dengan alamat IP yang berbeda. Empat modul akses pintu masing-masing denga alamat IP : 192.168.1.11 (pintu 1), IP : 192.168.1.12 (pintu 2), IP: 192.168.1.13 (pintu 3), IP: 192.168.1.14 (pintu 4), dan IP *server* : 192.168.1.172. Gambar 22 menunjukkan pengujian koneksi ke *server* yang berhasil dilakukan. Pengujian koneksi jaringan komputer ke *server* sebagai pusat *database* menjadi sangat penting karena semua proses yang dilakukan mulai dari identifikasi e-KTP dan sidik jari harus dapat terkirim dan tersimpn pada *database server* sebagai riwayat *user*.

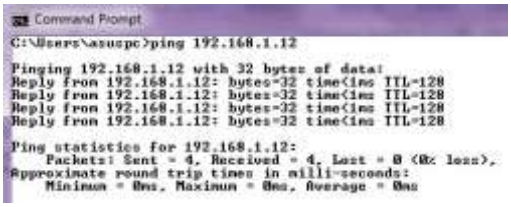


Gambar 22. Pengujian koneksi ke *server* berhasil dilakukan

Pengujian koneksi yang dilakukan pada setiap modul sistem kunci elektronik menyatakan bahwa mikrokontroler Arduino telah terkoneksi ke *server*. Gambar 23, 24, 25, dan 26 menunjukkan keberhasilan koneksi antara modul kunci elektronik pada pintu 1, 2, 3, dan 4 ke *server database*. Dengan keberhasilan koneksi antara *hardware* sistem akses pintu ke *server* , maka pengiriman data hasil scaning UID e-KTP dan identifikasi *fingerprint* dari setiap akses yang telah dilakukan dapat terkirim dan terekam ke dalam *server database*.

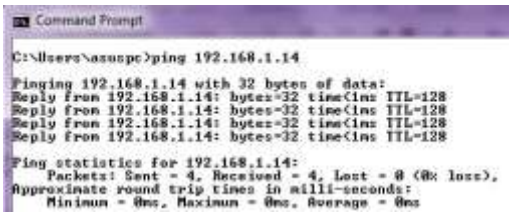


Gambar 23. Pengujian koneksi ke modul pintu 1



Gambar 24. Pengujian koneksi ke modul pintu 2

Gambar 25. Pengujian koneksi ke modul pintu 3



Gambar 26. Pengujian koneksi ke modul pintu 4

IV. KESIMPULAN

Berdasarkan hasil pengujian sistem maka dapat diambil kesimpulan sebagai berikut:

1. Penelitian ini berhasil dikembangkan dari model penelitian akses pintu tunggal menggunakan e-KTP.
2. Dengan menggunakan jaringan komputer tidak dibutuhkan lagi monitor server tersendiri untuk setiap akses pintu.
3. NFC dapat membaca UID e-KTP pada jarak optimum maksimal 4 Cm dan data dapat terkirim ke *server* jaringan.
4. Setiap mikrokontroler Arduino yang dilengkapi *Ethernet shield* pada setiap pintu dapat terhubung dengan baik ke *server database*.
5. Sistem akses pintu menggunakan e-KTP sebagai kunci elektronik sangat aman karena UID bersifat uniq dan hanya dimiliki oleh pemilik e-KTP.
6. Pengamanan dengan *fingerprint* untuk akses masuk dapat mengurangi penyalahgunaan penggunaan e-KTP oleh orang lain untuk mengakses/membuka pintu.
7. Sistem *database* dapat menyimpan riwayat *user* pengguna sehingga dapat diketahui seberapa banyak pintu tersebut telah diakses.

DAFTAR PUSTAKA

[1] Ardhi,Setya,"Perencanaan dan Pembuatan Sistem Pengaman Rumah Dengan Teknologi Pengenalan Sidik Jari", Sekolah Tinggi Teknik Surabaya,Surabaya,2011.

[2] Puasandi,Tadu,"Sistem Akses Kontrol Kunci Elektrik Memggunakan Pembacaan e-KTP ", Universitas Brawijaya Malang,Malang,2014.

[3] Dwi Prastiyo Utomo,"Rancang Bangun Sistem Akses Kontrol Pintu Elektronis Berbasis NFC (Near Field Communication) Menggunakan Pembacaan E-KTP dan Sidik Jari ", Politeknik Negeri Semarang,Semarang,2015.

[4] S Ganguly. COMPUTER NETWORKS. Available: http://www.unesco.org/education/aladin/paldin/pdf/course02/unit_08.pdf

[5] (2011) e-KTP Kartu Tanda Penduduk Elektronik. Available: http://www.e-ktp.com

[6] (2013) Press Release E-KTP Pusat Teknologi Informasi dan Komunikasi-BPPT. Available: http://www.bppt.go.id/berita/press-release/press-release-2013/1664-press-release-pusat-teknologi-informasi-dan-komunikasi-bppt?showall=1&limitstart=

[7] Nurbek Saparkhojayev, Aybek Nurtayev and Gulnaz Baimenshina, "Access Control and Management System Based on NFC-Technology by the Use of Smart Phones as Keys", Middle-East Journal of Scientific Research 21 (7),p.1130,2014.

[8] Rafid Karim, Haidara Al-Fakhri, "Smart Door Lock: A first prototype of a networked power lock controller with an NFC interface",Degree Project, School of Information and Communication Technology (ICT) KTH Royal Institute of Technology Stockholm, Sweden,2013.

[9] Doaa Abdel-Gaber Abdel-Aleem Ali, "Near-Field Communication Technology and Its Impact in Smart University and Digital Library: Comprehensive Study" , Journal of Library and Information Sciences, Vol. 3, No. 2, pp. 43-44, Dec. 2015.

[10] Tomi Aarnio, "Near Field Communication Using NFC to Unlock Doors", Master's Thesis, Degree Programme of Computer Science and Engineering, Aalto University School of Science, Nov. 2013.

[11] (2016) RFID/NFC/PN532 Shield IC Card Expansion Boards for Arduino with White Card FZ0089. Available: http://lapantech.com/jual-RFID-NFC-PN532-Shield-arduino-raspberry-surabaya

[12] (2016) FPM10A Optical Fingerprint reader Sensor Modules For Arduino Locks. Available: http://www.dhgate.com/product/fpm10a-optical-fingerprint-reader-sensor/388792568.html

[13] (2011) Tutorial of LinkSprite Optical Fingerprint Module for Ardino. Available : http://www.linksprite.com/article/shownews.php?lang=en&id=87

[14] (2016) Arduino MEGA 2560 & Genuino MEGA 2560-Overview. Available: https://www.arduino. cc/en/Main/ArduinoBoardMega2560

[15] (2016) Arduino Ethernet Shield-Overview and Description. Available: https://www.arduino. cc/en/Main/ Arduino EthernetShield

[16] Solenoid. Vailable: http://mechatronics. mech. northwestern. edu/design_ref/actuators/solenoids.html

[17] Linear Solenoid Actuator. Available:http://www. electronics- tutorials. ws/io/io_6.html

[18] Santoso, Hari, *Panduan Praktis Arduino Untuk Pemula*, Trenggalek: Elang Sakti, 2015.

[19] Dani Eko H, "Pembuatan Sistem Informasi Perpustakaan Berbasis Website Pada Sekolah Menengah Pertama Negeri 1 Donorejo Kabupaten Pacitan", IJINS-Indonesian Journal on Network and Security-Vol. 2 No 4 ,p.59,2014.